

Instalación de GFI MailSecurity

Introducción

Este capítulo explica el procedimiento para instalar y configurar GFI MailSecurity. Puede instalar GFI MailSecurity directamente en su servidor de correo o puede escoger instalarlo en un equipo diferente configurado como servidor de retransmisión/gateway. Cuando se instala en un equipo diferente, primero debe configurar el equipo para retransmitir el correo entrante y saliente a sus servidor de correo antes de instalar este software de seguridad de correo.

Para poder funcionar correctamente, GFI MailSecurity necesita acceder a la lista completa de todos sus usuarios de correo y sus correspondientes direcciones de correo. Esto es necesario para poder generar las reglas de supervisión de correo que filtrarán el correo entrante y saliente. GFI MailSecurity puede definir la lista de usuarios de correo de dos formas: Ya sea consultando su Directorio Activo (requiere instalar este software en **modo Directorio Activo**) o importando la lista de su servidor SMTP (requiere instalar este software en **modo SMTP**). El modo a utilizarse depende enteramente de su configuración de red y del equipo en el cual será instalado este software de seguridad de correo. Puede escoger el modo de acceso requerido durante la instalación de GFI MailSecurity.

Instalar GFI MailSecurity en su servidor de correo

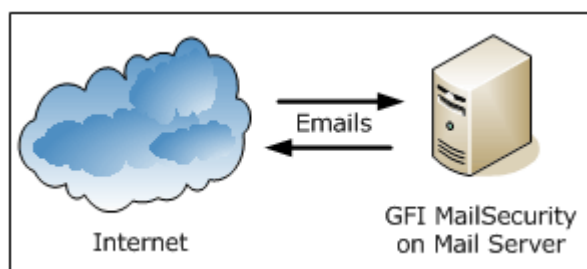


Figure 1 - Instalar GFI MailSecurity en su servidor de correo

Puede instalar GFI MailSecurity directamente en su servidor de correo, sin necesitar de ninguna configuración adicional. Además también puede escoger cualquier de los dos modos de instalación (es decir, modo Directorio Activo o modo SMTP) para definir cómo recuperará GFI MailSecurity la lista de usuarios ya que su servidor de correo tendrá acceso a ambos Directorio Activo así como a la lista de usuarios SMTP que está contenida en el propio servidor de correo.

Instalar GFI MailSecurity en su servidor de retransmisión de correo

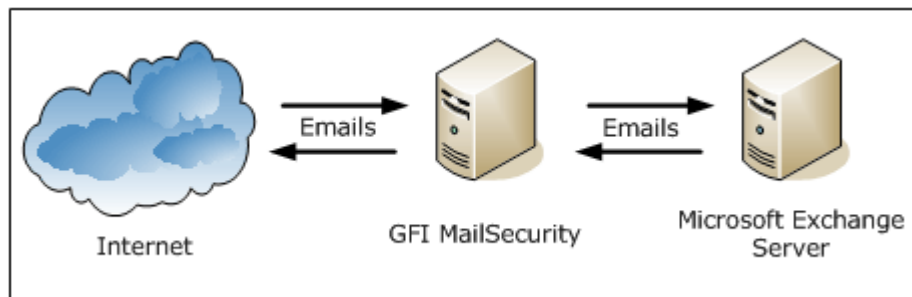


Figure 2 - Instalar GFI MailSecurity en su servidor gateway/retransmisor de correo

Cuando instale en un equipo diferente (es decir, en un servidor que no es su servidor de correo), primero debe configurar ese equipo para que actúe como gateway (también conocido como servidor “host inteligente” o “retransmisor de correo”) de todo su correo. Esto significa que todo el correo entrante debe pasar a través de este equipo para ser analizado antes de ser retransmitido al servidor de correo para su distribución (es decir, debe ser el primero en recibir todo el correo destinado a su servidor de correo). Lo mismo se aplica para el correo saliente: El servidor de correo debe retransmitir el correo saliente al equipo gateway para ser analizado antes de entregarse a los destinatarios externos vía Internet (es decir, debe ser la última 'parada' para el correo destinado a Internet). De esta forma, GFI MailSecurity chequea todo su correo entrante y saliente antes de que este sea entregado a los destinatarios.

OBSERVACION 1: Debe instalar GFI MailSecurity en modo SMTP Gateway si está utilizando Lotus Notes u otro servidor SMTP/POP3.

OBSERVACION 2: Si está utilizando una red Windows NT, el equipo que utiliza GFI MailSecurity se puede separar de su red Windows NT – GFI MailSecurity no requiere Directorio Activo cuando se instala en modo SMTP.

Instalando GFI MailSecurity frente a su cortafuegos

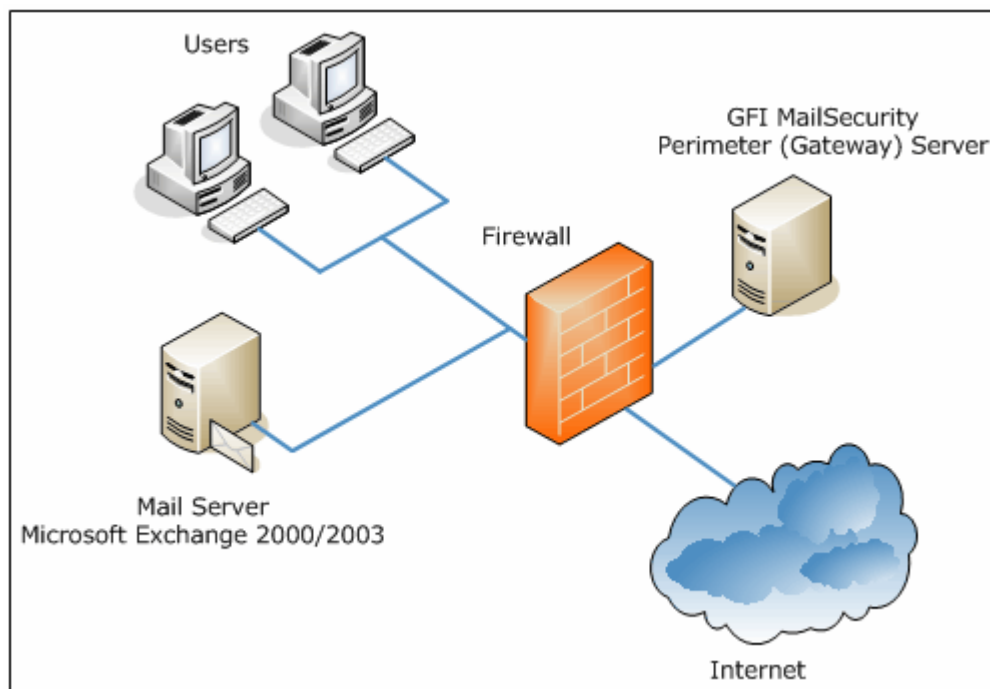


Figura 3 – Instalar GFI MailSecurity es un equipo separado de una DMZ

Si utiliza un cortafuegos Windows 2000/2003 como Microsoft ISA Server, una buena forma de implementar GFI MailSecurity es instalarlo en un equipo aparte delante de su cortafuegos o en el propio cortafuegos. Esto permite mantener su servidor de correo corporativo detrás del cortafuegos. GFI MailSecurity actuará como un host inteligente/servidor retransmisor de correo en el perímetro de la red (también conocido como DMZ – zona desmilitarizada).

Cuando GFI MailSecurity no está instalado en su servidor de correo:

- Puede realizar el mantenimiento de su servidor de Correo, mientras continúa recibiendo correo de Internet.
- Menores recursos son utilizados en su servidor de correo.
- Tolerancia a fallos adicional – si ocurre cualquier cosa en su servidor de correo, todavía podrá recibir el correo. Este correo se encola en el equipo GFI MailSecurity.

NOTA: GFI MailSecurity no necesita un equipo dedicado cuando no está instalado en el servidor de correo. Usted puede, por ejemplo, instalar GFI MailSecurity en su cortafuegos (es decir, en su ISA Server) o en equipos corriendo otras aplicaciones tales como GFI MailEssentials.

Instalar GFI MailSecurity en un Cluster Activo/Pasivo

Para instalar GFI MailSecurity en un cluster Activo/Pasivo debe instalar GFI MailSecurity en cada nodo.

NOTA: Aunque puede instalar GFI MailSecurity en un cluster Activo/Pasivo, tenga en mente que aún necesitará configurar y administrar un instalación de GFI MailSecurity por nodo. Las opciones de configuración y correos en cuarentena no están compartidos entre nodos.

En cada nodo tiene que hacer lo siguiente:

- Instalar GFI MailSecurity en el disco duro local del nodo.
NOTA: No instale GFI MailSecurity en la unidad compartida.
- Instale el directorio virtual WWW de GFI MailSecurity en el **Sitio Web Predeterminado** del nodo.
- Si está instalando en un cluster IIS, asegúrese de enlazar GFI MailSecurity en la instancia de Servidor Virtual SMTP **Clusterizada**.

El siguientes pasos muestran cómo instalar GFI MailSecurity en un entorno Cluster Activo/Pasivo típico. Para este escenario, se asume que el cluster, llamado **MAILCLUSTER**, está formado por dos nodos, llamados **Nodo1** y **Nodo2**.

1. Utilizando la consola **Administración del Cluster** hace activo el **Nodo1**.

2. Instale GFI MailSecurity en el disco duro local del **Nodo2** según se describe en la sección 'Instalar GFI MailSecurity' de este capítulo. Cuando llegue al paso **IIS Setup** de la instalación, seleccione **Sitio Web Predeterminado** para albergar el directorio virtual WWW de GFI MailSecurity.

3. Cuando la instalación de GFI MailSecurity en **Nodo2** haya finalizado, usted debe poder acceder a la configuración de **Nodo2** utilizando la siguiente URL: <http://Nodo2/MailSecurity/>

4. Utilizando la consola **Administración del Cluster** hace activo el **Nodo2**.

5. Instale GFI MailSecurity en el disco duro local del **Nodo1** según se describe en la sección 'Instalar GFI MailSecurity' de este capítulo. Cuando llegue al paso **IIS Setup** de la instalación, seleccione **Sitio Web Predeterminado** para albergar el directorio virtual WWW de GFI MailSecurity.

6. Cuando la instalación de GFI MailSecurity en **Nodo1** haya finalizado, usted debe poder acceder a la configuración de **Nodo1** utilizando la siguiente URL: <http://Nodo1/MailSecurity/>

7. Para acceder a la configuración del producto del nodo activo en cada momento utilice la siguiente URL: <http://MAILCLUSTER/MailSecurity/>.

8. La instalación de GFI MailSecurity en un cluster Activo/Pasivo está ahora completa.

NOTA: Si en una instalación cluster Microsoft Exchange Server 2003 no está instalado Service Pack 2 para Microsoft Exchange Server 2003, los sitios Web Internet information Server que estén alojados en el cluster no se iniciarán automáticamente cuando un servidor virtual Exchange Server 2003 falle en un nodo cluster. Más información sobre este asunto se puede encontrar en [Microsoft Knowledge Base Article 885440](#).

Debido a lo anterior, la configuración de GFI MailSecurity podría no estar disponible a continuación de una caída o de mover un Servidor Virtual Exchange de un nodo del cluster al otro.

Por lo tanto es recomendable instalar Service Pack 2 para Exchange Server 2003. Directrices sobre cómo instalar service packs de Exchange Server 2003 en un entorno cluster Exchange Server se pueden encontrar en [Microsoft Knowledge Base Article 867624](#).

Para desinstalar GFI MailSecurity del entorno de cluster **MAILCLUSTER** delineado anteriormente, siga estos pasos:

1. Utilizando la consola **Administración del Cluster** hace activo el **Nodo1**.
2. Desinstale GFI MailSecurity del **Nodo2**.
3. Utilizando la consola **Administración del Cluster** hace activo el **Nodo2**.
4. Desinstale GFI MailSecurity del **Nodo1**.
5. La desinstalación de GFI MailSecurity de un cluster Activo/Pasivo está ahora completa.

Instalar GFI MailSecurity en un Cluster Activo/Activo

Actualmente no se soporta la instalación de GFI MailSecurity en un cluster Activo/Activo.

¿Qué modo de instalación debo usar?

Modo Directorio Activo

Cuando está instalado en modo Directorio Activo, GFI MailSecurity crea reglas basadas en usuarios, tales como reglas de Análisis de Adjuntos y Análisis de Contenido, en base a la lista de usuarios disponible en el Directorio Activo. Esto significa que el equipo que ejecuta GFI MailSecurity debe estar detrás de su cortafuegos y debe tener acceso al Directorio Activo que contiene todos sus usuarios de correo (es decir, el equipo debe ser parte del dominio del Directorio Activo). Puede instalar GFI MailSecurity en modo Directorio Activo directamente en su servidor de correo así como sobre cualquier otro equipo del dominio que esté configurado como servidor de retransmisión de correo en su dominio.

Modo SMTP

En modo SMTP, GFI MailSecurity creará reglas basadas en usuarios, tales como reglas de Análisis de Adjuntos y Análisis de contenido, en base a la lista de usuarios/direcciones de correo disponibles en su servidor de correo. Esto significa que usted debe instalar GFI MailSecurity en modo SMTP si su equipo no tiene acceso al Directorio Activo que contiene todos sus usuarios de correo. Esto incluye equipos que no son parte de su dominio Directorio Activo (es decir, equipo que no son del dominio) así como equipos en una DMZ. Sin embargo, todavía puede instalar GFI MailSecurity en modo SMTP en su servidor de correo así como sobre cualquier otro equipo que tenga acceso al Directorio Activo que contenga todos los usuarios (de correo).

NOTA: Ambos modos de instalación tiene las mismas características y funciones. La única diferencia entre los modos de instalación Directorio Activo y SMTP es la forma en que GFI MailSecurity

accede/recoge la lista de usuarios de correo para la generación de sus reglas de análisis y notificaciones.

Requerimientos del sistema

Para instalar GFI MailSecurity usted necesita:

- Windows 2000 Profesional/Server/Advanced Server (Service Pack 1 o superior) o Windows 2003 Server/Advanced Server o Windows XP.

NOTA: Como Windows XP tiene algunas limitaciones de velocidad, instalar GFI MailSecurity en un equipo Windows XP puede afectar su rendimiento.

- Microsoft Exchange Server 2000 (SP1), 2003, 4, 5 ó 5.5, Lotus Notes 4.5 y superior, o cualquier servidor de correo SMTP/POP3
- Cuando utilice Small Business Server, asegúrese de haber instalado Service Pack 2 para Exchange Server 2000 y Service Pack 1 para Exchange Server 2003.
- Microsoft .Net framework 1.1 / 2.0
- MSMQ – Microsoft Messaging Queuing Service.
- Internet Information Services (IIS) – Servicio SMTP y servicio World Wide Web.
- Microsoft Data Access Components (MDAC) 2.8

IMPORTANTE: Desactive el análisis de los directorios de GFI MailSecurity en su software anti-virus. Los productos anti-virus son conocidos por interferir con el funcionamiento normal así como por ralentizar cualquier software que requiera acceso a archivos. De hecho Microsoft no recomienda ejecutar software anti-virus basado en sistemas de archivos en el servidor de correo. Para más información sobre [enrutamiento](http://kbase.gfi.com/showarticle.asp?id=KBID001559) visite, <http://kbase.gfi.com/showarticle.asp?id=KBID001559>.

IMPORTANTE: Los directorios de GFI MailSecurity nunca deben ser copiados utilizando software de copia de seguridad.

Requerimientos hardware:

Los requerimientos hardware de GFI MailSecurity son:

- Pentium 4 (o equivalente) - 2Ghz
- 512MB RAM
- 1,5 GB de espacio físico en disco

Preparación para instalar GFI MailSecurity en su servidor de retransmisión de correo

Para poder instalar GFI MailSecurity en un equipo retransmisor/gateway de correo, debe estar utilizando el servicio SMTP IIS y el servicio World Wide Web. El equipo también debe estar configurado como retransmisor SMTP para su servidor de correo. Esto significa que el registro MX de su dominio debe estar apuntando al equipo gateway. Esta sección describe cómo puede configurar su retransmisor de correo e instalar GFI MailSecurity. Para más

información, por favor visite <http://support.microsoft.com/support/kb/articles/Q293/8/00.ASP>.

Instalar y configurar los servicios IIS SMTP y World Wide Web

GFI MailSecurity usa el servicio SMTP de Windows 2000/XP/2003 como su servidor SMTP. Sin embargo, primero debe configurar este servicio como servidor de retransmisión de correo para permitir a GFI MailSecurity analizar todo el correo entrante y saliente antes de que llegue a su servidor de correo.

Acerca de los servicios IIS SMTP y World Wide Web de Windows 2000/2003

El servicio SMTP es parte de IIS, que es parte de Windows 2000/2003/XP. Se utiliza como el agente de transferencia de mensajes de Microsoft Exchange Server, y ha sido diseñado para manejar grandes tráficoos de correo.

El servicio World Wide Web también es parte de IIS. Utiliza el protocolo HTTP para manejar las solicitudes web de clientes en una red TCP/IP.

El servicio IIS SMTP y el servicio World Wide Web están incluidos en cada distribución Windows 2000/2003/XP.

Para instalar y configurar el servicio IIS SMTP como servidor de retransmisión de correo, usted debe:

Paso 1: Verifique la Instalación de los Servicios SMTP y World Wide Web

1. Go to **Inicio** ► **Panel de Control**. Haga doble clic sobre **Agregar o Quitar Programas** y a continuación haga clic sobre **Agregar o Quitar Componentes de Windows**.
2. Desde el diálogo en pantalla, localice y haga clic sobre **Componentes de Internet Information Services (IIS)**, a continuación sobre el botón **Detalles**.
3. Asegúrese que las casilla **Servicio SMTP** y **Servicio World Wide Web** estén seleccionados. Si no, seleccione estas casillas y haga clic en **Aceptar**. Esto debe iniciar la instalación de los servicios seleccionados. Siga las instrucciones en pantalla y espere hasta que finalice la instalación.

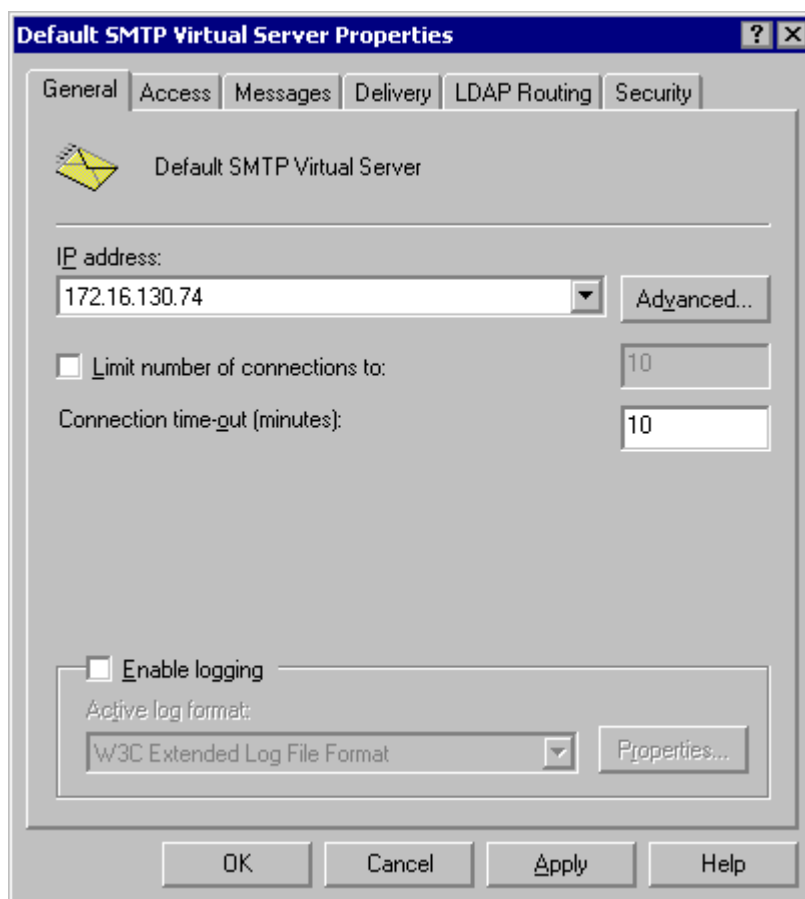


Imagen 2 – Asigne una dirección IP al servidor de retransmisión de correo

Paso 2: Especifique un nombre del servidor de retransmisión de correo y asigne una IP

1. Go to **Inicio ▶ Programas ▶ Herramientas Administrativas** y haga clic sobre **Administración de Internet Information Services (IIS)**.
2. Expanda el nodo del nombre del servidor, haga clic con el botón derecho sobre el nodo **Servidor Virtual SMTP Predeterminado** y seleccione **Propiedades** desde el menú contextual.
3. Asigne una dirección IP al servidor de retransmisión SMTP y haga clic sobre el botón **Aplicar** para aceptar los cambios y salir.

Paso 3: Configure el servicio SMTP para retransmitir el correo a su servidor de correo

Ahora debe configurar el servicio SMTP para retransmitir los mensajes entrantes a su servidor de correo.

Comience por crear un dominio local en IIS para enrutar correo:

1. Go to **Inicio ▶ Programas ▶ Herramientas Administrativas** y haga clic sobre **Administración de Internet Information Services (IIS)**.
2. Expanda el nodo del nombre del servidor, y a continuación expanda el Servidor SMTP Virtual Predeterminado. Por defecto, debe tener un dominio Local (Predeterminado) con el nombre de dominio totalmente cualificado del servidor.

3. Configure el dominio para la retransmisión de mensajes entrantes como sigue:

a) Haga clic con el botón derecho sobre el nodo Dominios y vaya a **Nuevo ▶ Dominio**.

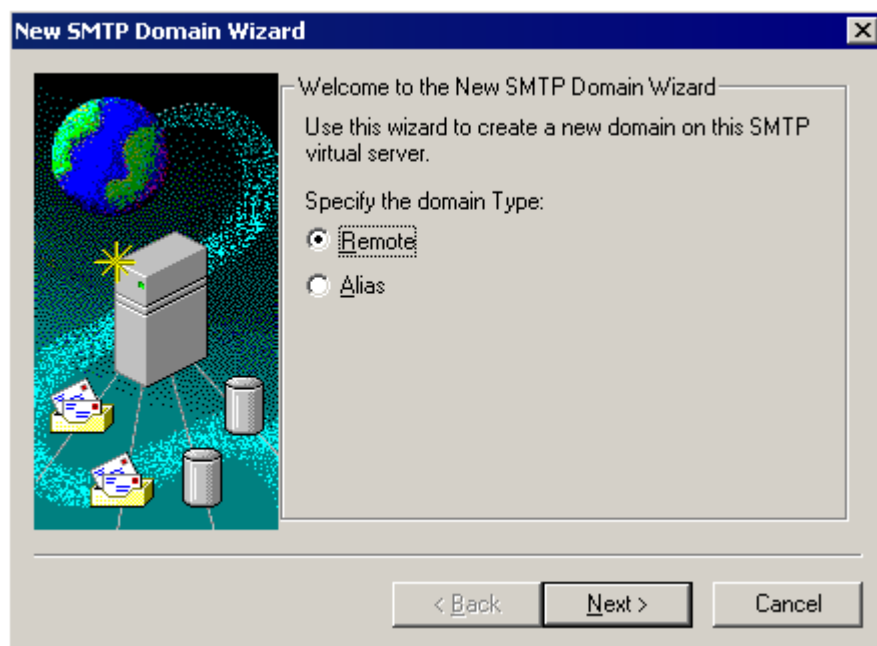


Imagen 3 – Asistente de Dominio SMTP – Seleccionando el tipo de dominio

b) Seleccione **Remoto** y haga clic sobre **Siguiente**.

c) Escriba el nombre de dominio en el campo Nombre y haga clic sobre **Finalizar**.

NOTA IMPORTANTE SOBRE DOMINIOS LOCALES

NOTA: Durante la instalación, MailSecurity importará los Dominios Locales del servicio IIS SMTP. Si agrega más Dominios Locales en el servicio IIS SMTP, también debe agregar estos dominios en GFI MailSecurity porque este no detecta automáticamente los Dominios Locales recién agregados. Puede agregar más/nuevos Dominios Locales utilizando la configuración de GFI MailSecurity. Para más información, refiérase a la sección 'Agregar dominios locales' en el capítulo Opciones Generales de este manual.

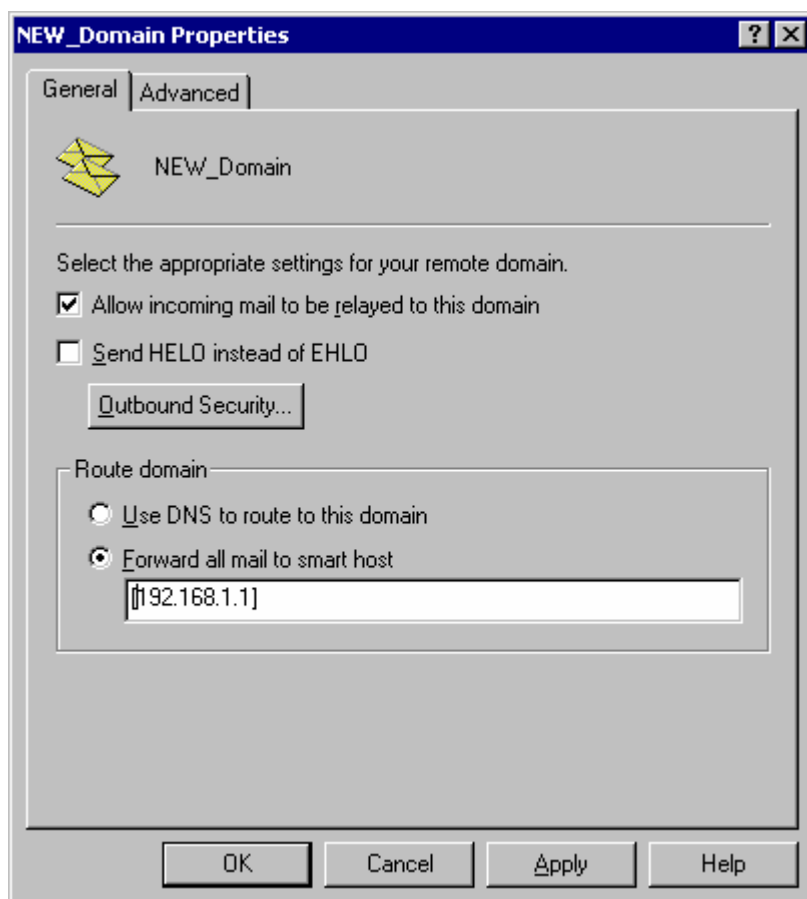


Imagen 4 – Configure el nuevo dominio

Configure el dominio para retransmitir correo a su servidor de correo:

1. Haga clic con el botón derecho sobre el dominio que acaba de crear y seleccione **Propiedades** del menú contextual. Seleccione la casilla **Permitir que el correo entrante sea retransmitido a este dominio**.

2. En el diálogo Dominio de enrutamiento, seleccione la opción **Reenviar todo el correo al siguiente host inteligente** y especifique la dirección IP (entre corchetes) del servidor que gestionará el correo direccionado a este nuevo dominio. For example, [123.123.123.123]

NOTA: Los corchetes se utilizan para diferenciar una dirección IP de un nombre de host (que no necesita los corchetes), es decir, el servidor detecta una dirección IP por los corchetes.

3. Haga clic sobre **Aceptar** para guardar las entradas y cerrar el diálogo.

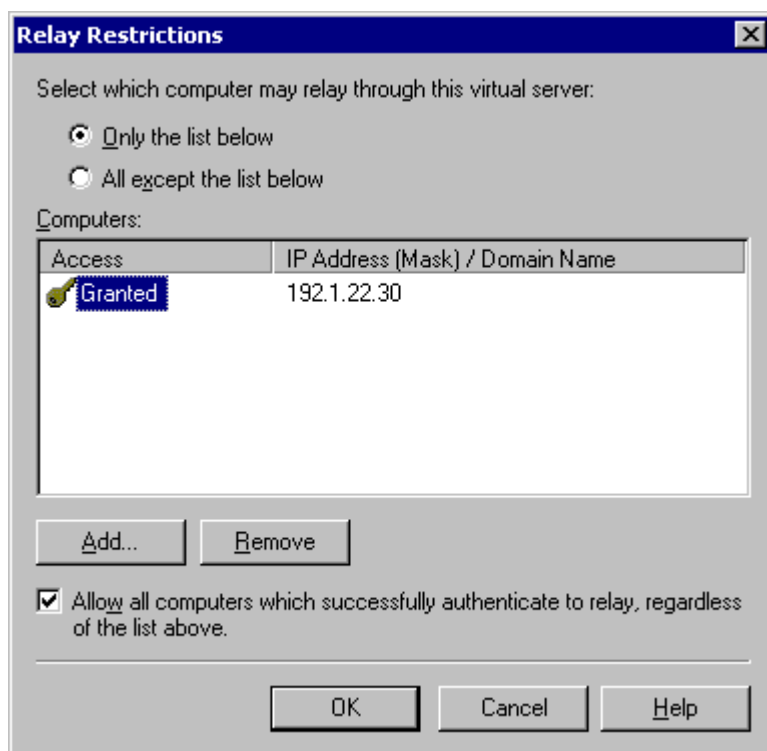


Imagen 5 – Diálogo de Restricciones de Retransmisión

Paso 4: Asegure su servidor retransmisor de correo

En este paso, configurará las restricciones de retransmisión de su servidor virtual SMTP. Esto significa que debe especificar qué equipos pueden retransmitir correo a través de este servidor virtual (es decir, limitar efectivamente los servidores que pueden enviar correo mediante este servidor).

1. Haga clic con el botón derecho sobre **Servidor Virtual SMTP Predeterminado** y seleccione **Propiedades**.
2. En la ventana propiedades, pulse la etiqueta **Acceso** y a continuación pulse el botón **Retransmisión** para abrir el diálogo de restricciones de retransmisión.
3. Haga clic sobre la opción **Sólo los de la lista siguiente** y a continuación pulse en **Agregar** para especificar la lista de equipos permitidos.

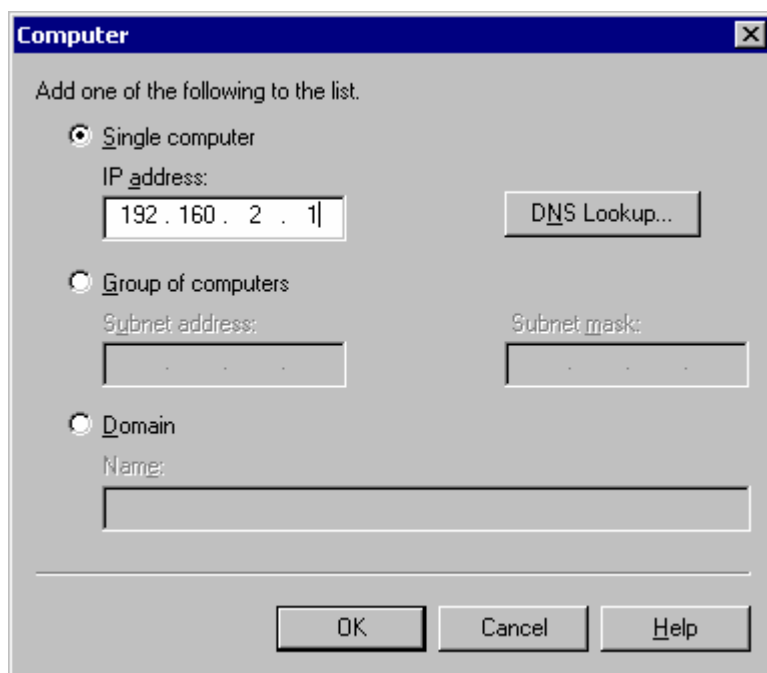


Imagen 6 – Indique los equipos que pueden retransmitir correo mediante el servidor virtual

4. En el diálogo recién abierto, indique la IP del servidor de correo que reenviará el correo a este servidor virtual y haga clic sobre el botón **Aceptar** para agregar la entrada a la lista.

NOTA: En este diálogo, puede especificar la IP de un único equipo, un grupo de equipos o un dominio:

- **Un único equipo:** Seleccione esta opción para especificar un host concreto que retransmitirá el correo a través de este servidor. Puede consultar la dirección IP de un host específico haciendo clic sobre el botón **Consulta DNS**.
- **Grupo de equipos:** Seleccione esta opción para especificar la IP base de los equipos que quiera que retransmitan.
- **Dominio:** Seleccione esta opción para incluir todos los equipos de un dominio especificado. Esto significa que el controlador de dominio retransmitirá abiertamente a través de este servidor. Por favor observe que esta opción supone mayor carga de proceso, y podría reducir el rendimiento del servicio SMTP porque incluye Consultas DNS inversas para verificar el nombre de dominio de todas las direcciones IP que intentan retransmitir.

Paso 5: Configure su servidor de correo para retransmitir el correo a través del servidor Gateway

Después de haber configurado el servicio SMTP de IIS para enviar y recibir correo, debe configurar su servidor de correo para retransmitir todo el correo a su servidor retransmisor de correo:

Si tiene Microsoft Exchange Server 4/5/5.5:

1. Inicie el Administrador de Microsoft Exchange y haga doble clic sobre **Internet Mail Service** para abrir la configuración de propiedades.

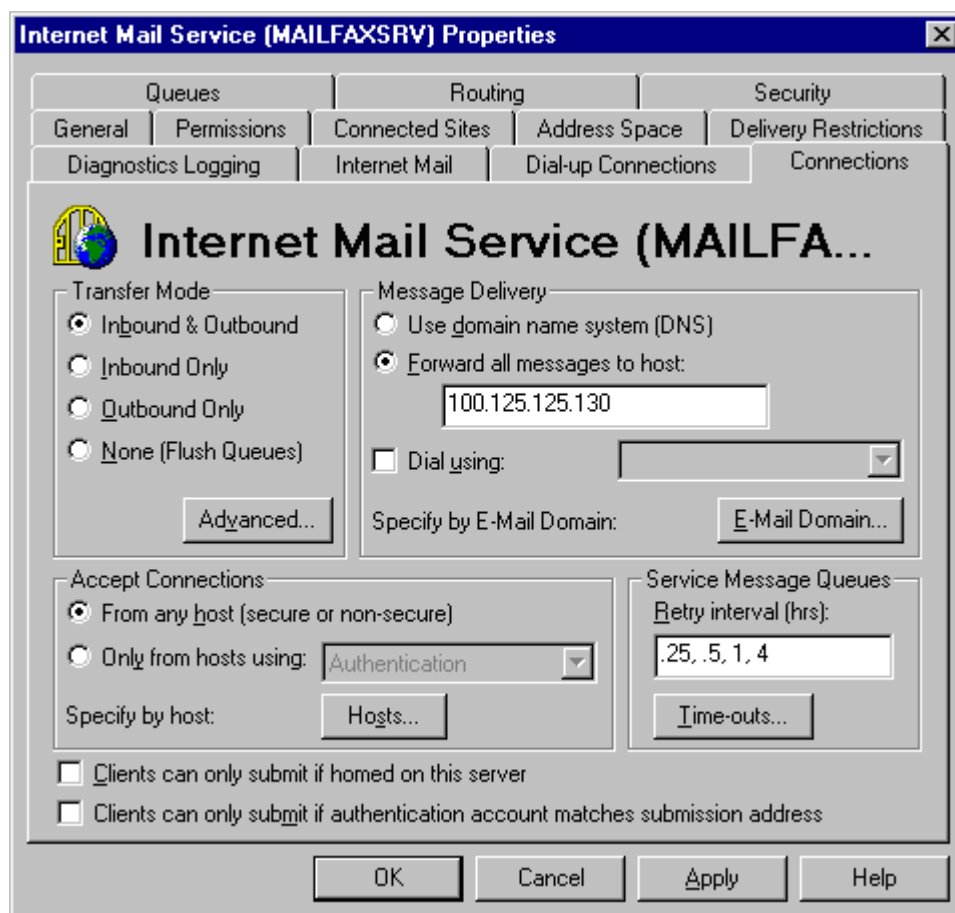


Imagen 7 - El conector Microsoft Internet mail

2. Haga clic la etiqueta **Connections**, y en la sección **Message Delivery** seleccione **Forward all messages to host**. Introduzca el nombre o la IP del equipo que ejecuta GFI MailSecurity.

3. Haga clic sobre **Aceptar** y reinicie el Servidor Microsoft Exchange desde el complemento servicios.

Si tiene Microsoft Exchange Server 2000/2003:

Necesitará configurar un conector SMTP que reenvíe todo el correo a GFI MailSecurity:

1. Inicie el Administrador del Sistema Exchange.
2. Haga clic derecho en el nodo **Conectores**, vaya a **Nuevo ▶ Conector SMTP** e indique el nombre del conector.
3. Seleccione la opción **Reenviar todo el correo a través de este conector al siguiente host inteligente**, y escriba la IP del servidor GFI MailSecurity (el servidor de retransmisión/Gateway de correo) y haga clic en **Aceptar**.

NOTA: Encierre siempre la dirección IP entre corchetes []. Por ejemplo, [100.130.130.10].

4. Seleccione el Servidor SMTP que debe asociarse a este Conector SMTP. Vaya a la etiqueta **Espacio de Direcciones**, y haga clic en **Agregar**. Seleccione **SMTP** y haga clic en el botón **Aceptar** para aceptar los cambios.

5. Haga clic en el botón **Aceptar** para salir. Ahora todos los correos se reenviarán al equipo GFI MailSecurity.

Si dispone de Lotus Notes:

1. Haga doble clic sobre el botón **Address Book** de Lotus Notes.
2. Haga clic sobre el elemento Servidor para abrir sus sub-elementos.
3. Haga clic en **Domains** y a continuación en **Add Domains**.
4. En la sección Basics, seleccione **Foreign SMTP Domain from the Domain Type field** y en la sección **Messages Addressed to**, escriba "*" en el campo **Internet Domain**.
5. En el campo **Internet Host** de la sección **Should be routed to**, especifique la IP del equipo GFI MailSecurity.
6. Guarde la configuración y reinicie el servidor Lotus Notes.

Si tiene un servidor de correo SMTP/POP3:

1. Inicie el programa de configuración de su servidor de correo.
2. Busque la opción para retransmitir todo el correo saliente a través de otro servidor de correo. Esta opción se mencionará como algo similar a **Reenviar todos los mensajes al host**. Introduzca el nombre o la IP del equipo que ejecuta GFI MailSecurity.
3. Si es necesario, haga clic en **Aceptar** y reinicie su servidor de correo.

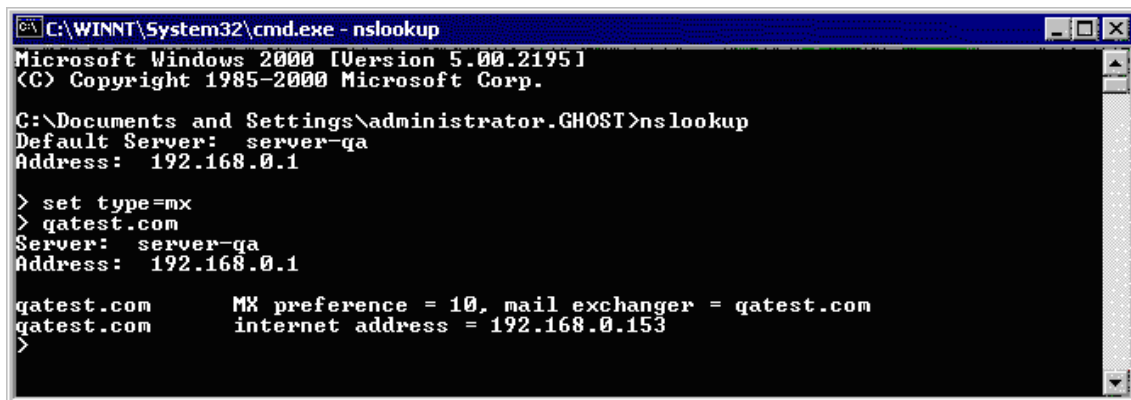
Paso 6: Apunte el registro MX de su dominio al servidor retransmisor de correo

Debido a que el nuevo servidor retransmisor de correo debe recibir primero todo el correo entrante y saliente, deberá actualizar el registro MX de su dominio para que apunte a la IP del nuevo servidor retransmisor/Gateway de correo. De otra forma el correo seguirá yendo a su servidor de correo y puenteará GFI MailSecurity.

Actualice el registro MX de su servidor DNS como sigue:

NOTA: Si su ISP administra el servidor DNS, consulte a este proveedor para actualizarla por usted.

1. Abrir la línea de comandos y escribir **nslookup**.
2. A continuación escriba **set type=mx** e introduzca su nombre de dominio.
3. El registro MX debe devolver una única IP que debe corresponder a la IP del equipo 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
>
```

Imagen 8 - Comprobar el registro MX de su dominio

Paso 7: Pruebe su nuevo retransmisor de correo

Antes de proceder con la instalación de GFI MailSecurity, verifique que su nuevo retransmisor de correo está funcionando correctamente.

1. Compruebe la conexión IIS 5 SMTP entrante de su servidor de retransmisión enviando un correo desde una cuenta externa a una cuenta interna (puede usar correo web, por ejemplo MSN Hotmail, si no dispone de una cuenta externa). Verifique que el cliente de correo recibe el correo.

2. Compruebe la conexión saliente IIS 5 SMTP de su servidor de retransmisión enviando un correo a una cuenta externa desde un cliente de correo. Verifique que el usuario externo recibe el correo.

NOTA: En lugar de usar un cliente de correo electrónico, puede usar Telnet para enviar manualmente un correo. Esto le aportará más información de resolución de problemas. Para más información, refiérase a este artículo de la base de conocimientos de Microsoft.

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

Paso 8: Instalar GFI MailSecurity en el servidor de retransmisión de correo

Para información sobre cómo instalar GFI MailSecurity, refiérase a la sección 'Instalar GFI MailSecurity' en este capítulo.

Preparación para instalar GFI MailSecurity en su servidor de correo

No se necesita configuración adicional si está instalando GFI MailSecurity directamente en su servidor de correo. Para información sobre cómo instalar GFI MailSecurity, refiérase a la sección 'Instalar GFI MailSecurity' en este capítulo.

Instalación de GFI MailSecurity

NOTA: Antes de instalar GFI MailSecurity, asegúrese de:

Iniciar sesión como Administrador o utilizando una cuenta con privilegios administrativos.

Guarde cualquier trabajo pendiente que pueda tener en el equipo, y cierre todas las aplicaciones abiertas.

1. Ejecute la configuración de GFI MailSecurity haciendo doble clic sobre **MailSecurityGW.exe** y en el momento en que se muestre el diálogo de entrada, pulse el botón **Next**.

2. Confirme el Acuerdo de Licencia y pulse el botón **Next**.

3. Introduzca su Nombre, Empresa y Clave de Licencia. Si esta evaluando el producto, deje el número de serie por defecto (es decir, 'Evaluation'). Haga clic en el botón **Next**.

4. Especifique la dirección de correo del administrador o la dirección a la que desea que GFI MailSecurity envíe las notificaciones.

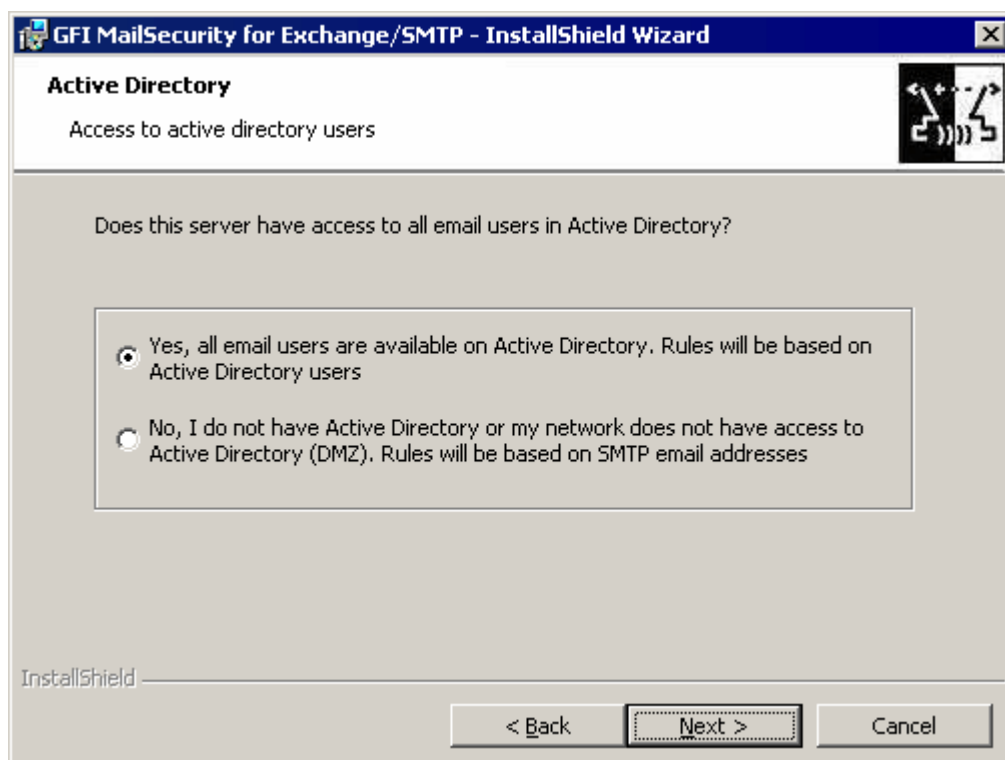


Imagen 9 – Defina si el servidor tiene acceso a todos los usuarios de correo en el Directorio Activo

5. La instalación le pedirá ahora que seleccione el modo en el que GFI MailSecurity recogerá la lista de sus usuarios de correo. Debe seleccionar una de las siguientes opciones:

- **Yes, all email users are available on Active Directory...** – Seleccione esta opción para continuar la instalación de GFI MailSecurity en **modo Directorio Activo**. En este modo, GFI MailSecurity crea reglas basadas en usuarios, por ejemplo reglas de Análisis de Adjuntos, en base a la lista de usuarios disponible en el Directorio Activo. Esto significa que el equipo que ejecuta GFI MailSecurity debe estar detrás de su cortafuegos (por ejemplo, el Servidor de Correo) y debe tener acceso al Directorio Activo que contiene todos sus usuarios de correo (es decir, el equipo en el que está instalado GFI MailSecurity debe ser parte del dominio del Directorio Activo).
- **No, I do not have Active Directory or my network does not have access to Active Directory (DMZ).** – Seleccione esta opción para continuar la instalación de GFI MailSecurity en **modo SMTP**. En este modo, GFI MailSecurity creará reglas basadas en usuarios, por ejemplo reglas de Análisis de Adjuntos, en base a la lista de usuarios/direcciones de correo importadas de su servidor de correo. Debe seleccionar este modo si está instalando GFI MailSecurity en un equipo que no tiene acceso al Directorio Activo que contiene la lista completa de sus usuarios de correo. Esto incluye equipos en una DMZ o equipos que no son parte del Directorio Activo del Dominio. Sin embargo, aún puede escoger este modo para instalar GFI MailSecurity en equipos que no tienen acceso al Directorio Activo que contiene todos sus usuarios de correo.

Haga clic sobre el botón **Next** para proceder con la instalación.

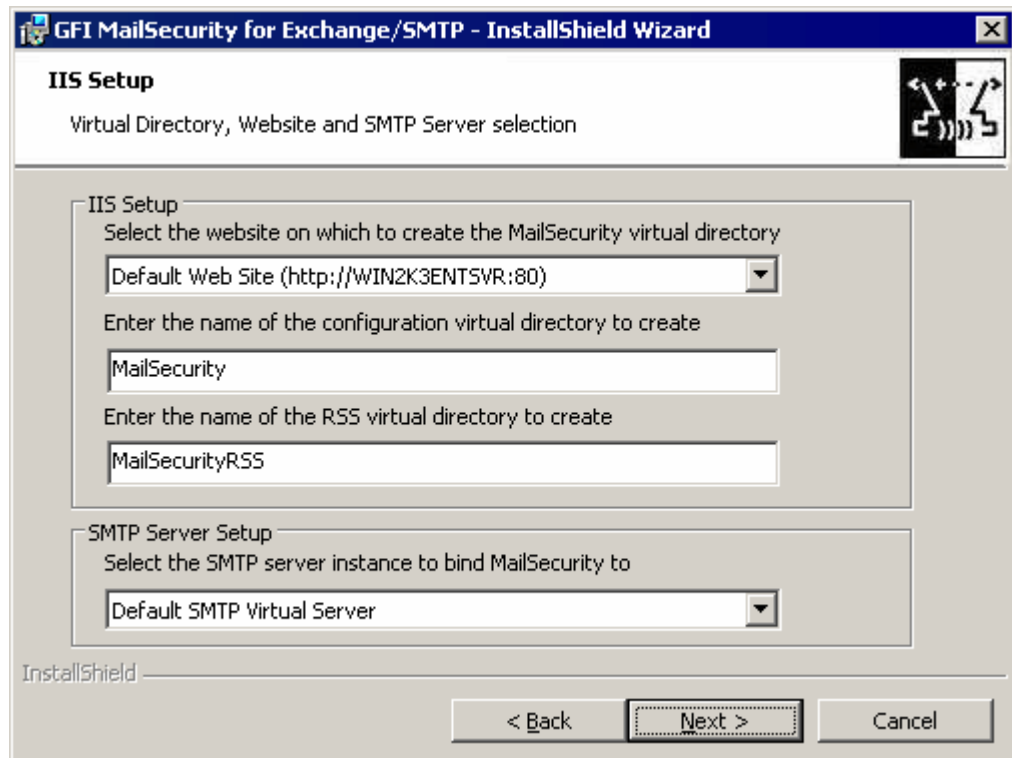


Imagen 10 – Defina su servidor SMTP y los datos de carpetas virtuales de GFI MailSecurity.

6. A continuación necesita seleccionar el servidor en el que desea albergar las páginas de configuración de GFI MailSecurity. En este servidor, se crean dos directorios virtuales para albergar las páginas de configuración y las listas RSS de cuarentena. Puede especificar nombres de directorio personalizados si lo desea, o dejar los predeterminados.

GFI MailSecurity confía en el servicio SMTP de IIS para enviar y recibir correo SMTP. Se enlaza con su servidor virtual SMTP predeterminado (es decir, el servidor especificado en el registro MX de su Servidor DNS). Sin embargo, si dispone de varios servidores virtuales SMTP en su dominio, puede enlazar GFI MailSecurity a cualquier servidor virtual SMTP disponible. Para cambiar la conexión SMTP predeterminada, seleccione el servidor requerido de la lista de Servidores Virtuales SMTP disponibles proporcionada en este diálogo.

OBSERVACION 1: Para más información sobre las opciones del servicio IIS SMTP refiérase a la sección 'Instalar y configurar los servicios IIS SMTP y World Wide Web' de este manual.

OBSERVACION 2: Después de instalar el producto, aún puede enlazar GFI MailSecurity con otro servidor virtual SMTP desde la configuración de GFI MailSecurity (**Raíz de la consola ▶ Settings ▶ Bindings**). Para más información, refiérase a la sección 'Enlaces al servidor SMTP' en el capítulo Opciones Generales.

Haga clic sobre el botón **Next** para continuar la instalación.

7. La configuración buscará ahora en su red e importará una lista de sus Dominios Locales del servicio IIS SMTP. GFI MailSecurity determina si un correo en entrante o saliente comparando el dominio de la dirección del remitente con la lista de dominios locales. Si la dirección existe en la lista, entonces el correo es saliente. Compruebe

que todos sus Dominios Locales han sido incluidos en la lista en pantalla. Si no, asegúrese de agregar cualquier dominio no listado una vez la instalación finalice. Para más información, refiérase a la sección 'Agregar dominios locales' en el capítulo Opciones Generales. Haga clic sobre el botón **Next** para continuar.

8. Ahora la configuración le pedirá que defina la carpeta en la que desea instalar GFI MailSecurity. GFI MailSecurity necesita aproximadamente 40 MB de espacio libre en disco. Además de esto, deberá reservar aproximadamente 200 MB para los archivos temporales. Pulse el botón **Change** para especificar una nueva ruta de instalación o **Next** para instalar en el lugar predeterminado y proceder con la instalación.

9. El asistente de instalación ya ha recodificado todas las opciones requeridas para la instalación y está listo para instalar GFI MailSecurity. Si quiere hacer cambios en estas opciones, pulse el botón **Back**. De lo contrario, pulse **Install** para comenzar el proceso de instalación.

10. A la finalización, la instalación le informará que es necesario reiniciar los servicios SMTP. Para reiniciar instantáneamente estos servicios y finalizar la instalación, pulse el botón **Yes**.

Agregar GFI MailSecurity a la Lista Windows de Excepciones DEP

La Prevención de Ejecución de Datos (DEP) es un conjunto de tecnologías hardware y software que realizan chequeos de memoria para ayudar a prevenir la ejecución de código malicioso en un sistema.

La tecnología DEP está disponible sólo en Microsoft Windows XP Service Pack 2 y en Microsoft Windows 2003 Service Pack 1. En Microsoft Windows 2003 Service Pack 1, DEP está habilitado por defecto para todos los programas y servicios excepto aquellos que el administrador seleccione.

Si instaló GFI MailSecurity en Microsoft Windows 2003 Service Pack 1, necesitará agregar el ejecutable del motor de análisis de GFI MailSecurity (**GFIscanM.exe**) y el ejecutable del Motor Anti-Virus Kaspersky (**kavss.exe**) a la lista de excepciones de la Prevención de Ejecución de Datos.

Para introducir los ejecutables de GFI en la lista de excepciones DEP siga estos pasos:

1. Desde el menú **Inicio** cargue el **Panel de Control** y escoja el complemento **Sistema**.
2. En la etiqueta **Opciones avanzadas**, pulse el botón **Configuración** bajo el grupo **Rendimiento**.
3. Seleccione la etiqueta **Prevención de Ejecución de Datos**.
4. Habilite la opción **Activar DEP para todos los programas y servicios excepto los que seleccione**.
5. Haga clic en **Agregar** y vaya a la carpeta de instalación de GFI MailSecurity, <GFI\ContentSecurity\MailSecurity>, y escoja **GFIscanM.exe**.

6. Haga clic en **Agregar** y vaya a la carpeta de instalación de GFI MailSecurity, <GFI\ContentSecurity\AntiVirus\Kaspersky>, y escoja **kavss.exe**.
7. Haga clic en **Aplicar** y **Aceptar** para aplicar los cambios.
8. Reinicie los servicios “GFI Content Security Auto-Updater Service” y “GFI MailSecurity Scan Engine”.

Asegurar el acceso a la configuración/cuarentenas de GFI MailSecurity

La configuración y el almacén de cuarentenas de GFI MailSecurity pueden ser accedidos a través de un navegador web y por lo tanto es imperativo que configure apropiadamente la seguridad de acceso de forma que sólo los usuarios autorizados puedan configurar reglas y administrar el almacén de cuarentenas.

Puede configurar la seguridad de acceso para las páginas de configuración y el almacén de cuarentenas de GFI MailSecurity y mediante la aplicación GFI MailSecurity SwitchBoard. Para configurar la seguridad de acceso, siga estos pasos:

1. Inicie **GFI MailSecurity SwitchBoard** desde **Inicio ▶ Programas ▶ GFI MailSecurity**.
2. Se carga la aplicación **GFI MailSecurity SwitchBoard**. Ahora necesitará seleccionar si quiere permitir sólo acceso sólo local a la Configuración y al Almacén de cuarentenas o ambas, local y remota. Para permitir sólo acceso local, seleccione la opción **Local mode**, para que la Configuración y el Almacén de cuarentenas sólo puedan ser accedidos cuando se trabaja directamente en el equipo servidor donde está instalado GFI MailSecurity. Por otro lado, para permitir ambos accesos local y remoto, seleccione la opción **IIS mode**, para que los usuarios autorizados, tanto del equipo local como de otros equipos remotos, puedan acceder a la Configuración y al Almacén de Cuarentenas de GFI MailSecurity.



Imagen 11 – GFI MailSecurity SwitchBoard

3. Si seleccionó la opción **Local mode**, no necesitará configurar nada más. Si seleccionó la opción **IIS mode** a continuación necesitará configurar las cuentas y grupos del Directorio Activo que tienen acceso a la Configuración y al Almacén de Cuarentenas, y además puede cambiar el nombre del directorio virtual que almacena las páginas de GFI MailSecurity.

NOTA: Si selecciona **Local mode** necesita agregar 'http://127.0.0.1' a la lista de sitios de confianza en Internet Explorer. Para mayor información, refiérase a la posterior sección 'Agregar el host local a la lista de sitios de confianza'.



Imagen 12 – La dirección del host local debe ser agregada a la lista de sitios de confianza

4. Para configurar la seguridad de acceso, pulse el botón **Security...** junto al campo **Virtual Directory**.

5. Se muestra el diálogo **IIS mode access control list**. Este diálogo le permite configurar quién tiene acceso a las páginas de configuración y al almacén de cuarentenas en distintas listas de control de acceso.

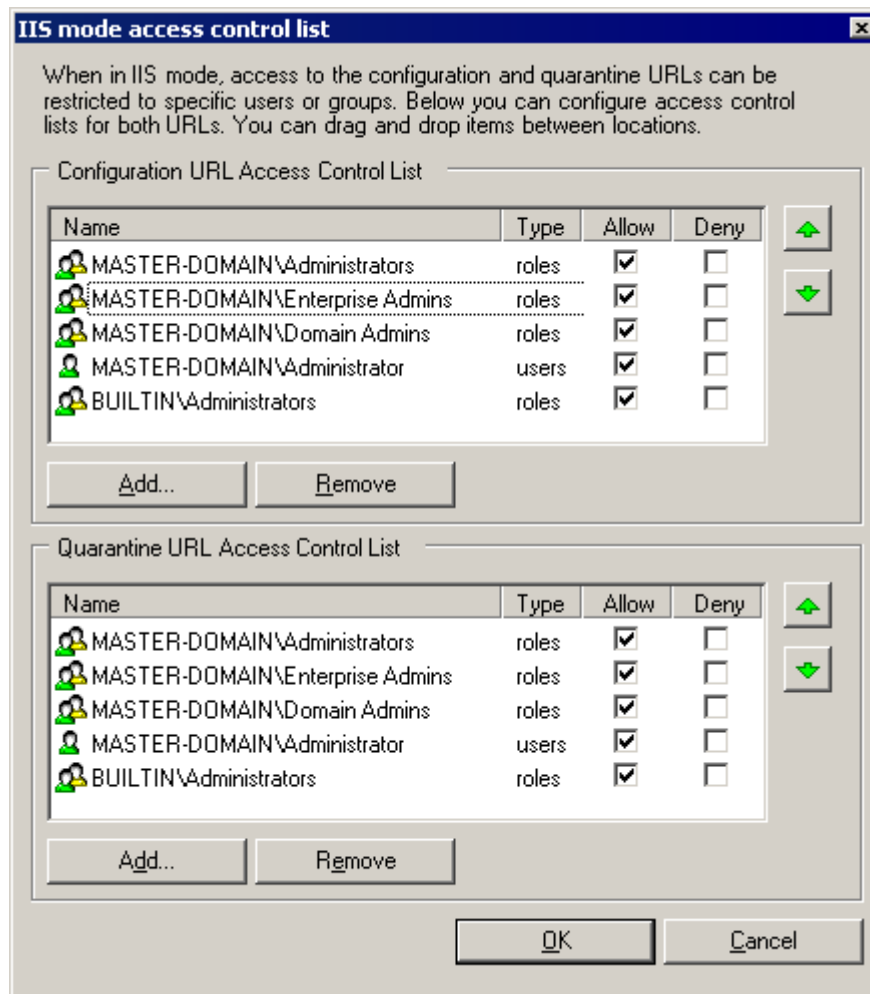


Imagen 13 – Listas de Control de Acceso a Configuración / Almacén de Cuarentenas

6. Para configurar las cuentas que tienen acceso a las páginas de configuración, utilice los botones **Add** y **Remove** bajo **Configuration URL Access Control List**. Si quiere denegar el acceso a una cuenta listada sin eliminarla de la lista, seleccione la casilla bajo la columna **Deny**.

7. Para configurar las cuentas que tienen acceso al almacén de cuarentenas, utilice los botones **Add** y **Remove** bajo **Quarantine URL Access Control List**. Si quiere denegar el acceso a una cuenta listada sin eliminarla de la lista, seleccione la casilla bajo la columna **Deny**.

NOTA: Para evitar reelegir dos veces las mismas cuentas, una vez por lista, sencillamente puede arrastrar y soltar cuentas y grupos entre las dos listas.

8. Cuando esté listo pulse **Aceptar** para cerrar el diálogo.

9. Si quiere especificar un nombre de directorio virtual diferente, puede hacerlo editando la entrada del campo **Virtual directory**.

10. Haga clic en **Aceptar** para guardar sus cambios. Aparecerá un diálogo mostrando el progreso de aplicar las nuevas opciones.



Imagen 14 – Nuevas opciones SwitchBoard aplicadas satisfactoriamente

11. Cuando finalice el proceso, haga clic en **Aceptar**.

Agregar el host local a la lista de sitios de confianza

Cuando configure GFI MailSecurity para ser accesible sólo localmente, necesita agregar la dirección del host local, 'http://127.0.0.1', a la lista de sitios de confianza de Internet Explorer. Para hacerlo, siga estos pasos:

1. Inicie el **Panel de Control** desde el menú **Inicio**.
2. Desde el **Panel de Control** abra las **Opciones de Internet**.
3. Se mostrará el diálogo **Propiedades de Internet**. Acceda a la etiqueta **Seguridad** y pulse el icono **Sitios de confianza** de la lista **Zona de contenido web**.

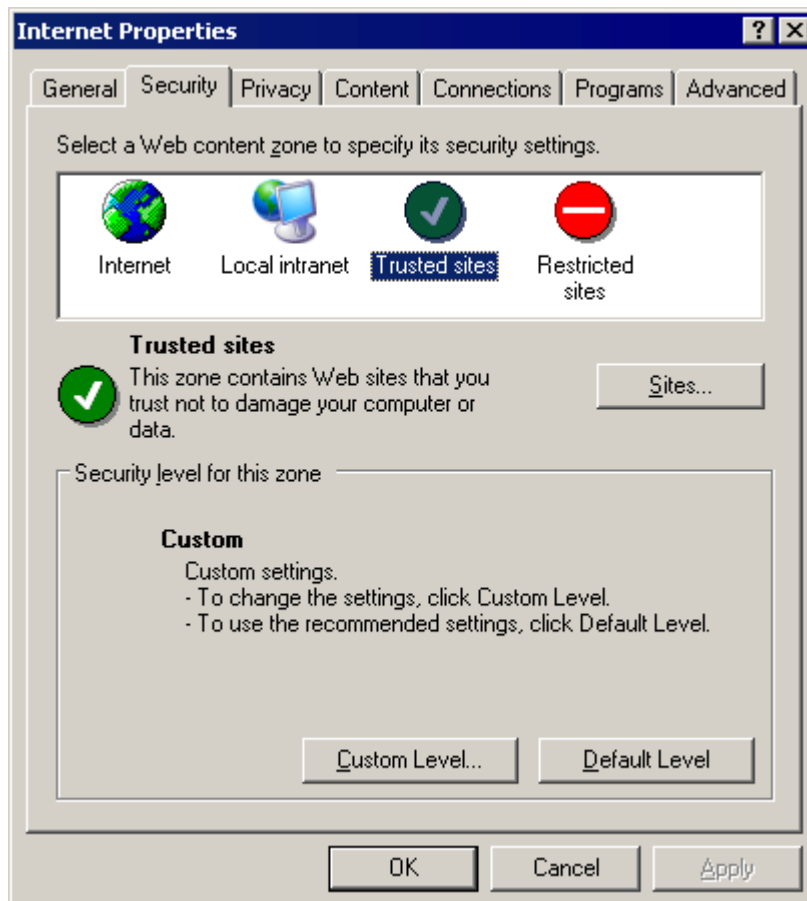


Imagen 15 – Propiedades de Internet

4. Haga clic en el botón **Sitios...**
5. Se muestra el diálogo **Sitios de confianza**. En la casilla **Agregar este sitio web a la zona**: especifique 'http://127.0.0.1'.

6. Haga clic en el botón **Agregar**. La dirección del host local se agregará a la lista **Sitios web**.

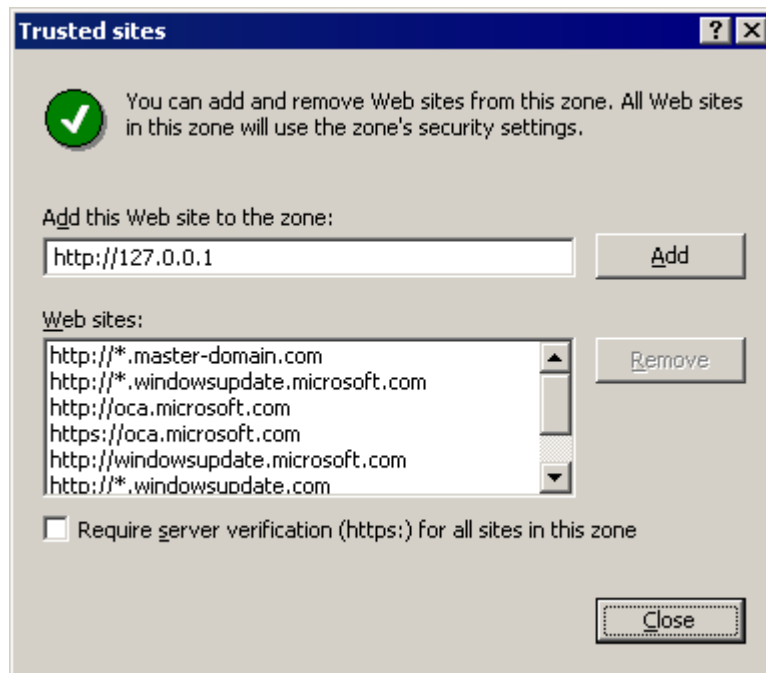


Imagen 16 – Sitios de confianza

7. Haga clic en el botón **Cerrar**.

8. Pulse el botón **Aceptar** en las **Propiedades de Internet** para cerrarlas y guardar los cambios.

Asegurar el acceso a las Listas RSS de cuarentenas de GFI MailSecurity

Puede configurar GFI MailSecurity para crear listas RSS de cuarentena sobre carpetas de cuarentena específicas. Para configurar quién puede suscribirse a las listas RSS de cuarentena, siga estos pasos:

1. Inicie **GFI MailSecurity SwitchBoard** desde **Inicio ▶ Programas ▶ GFI MailSecurity**.
2. Se carga la aplicación **GFI MailSecurity SwitchBoard**.

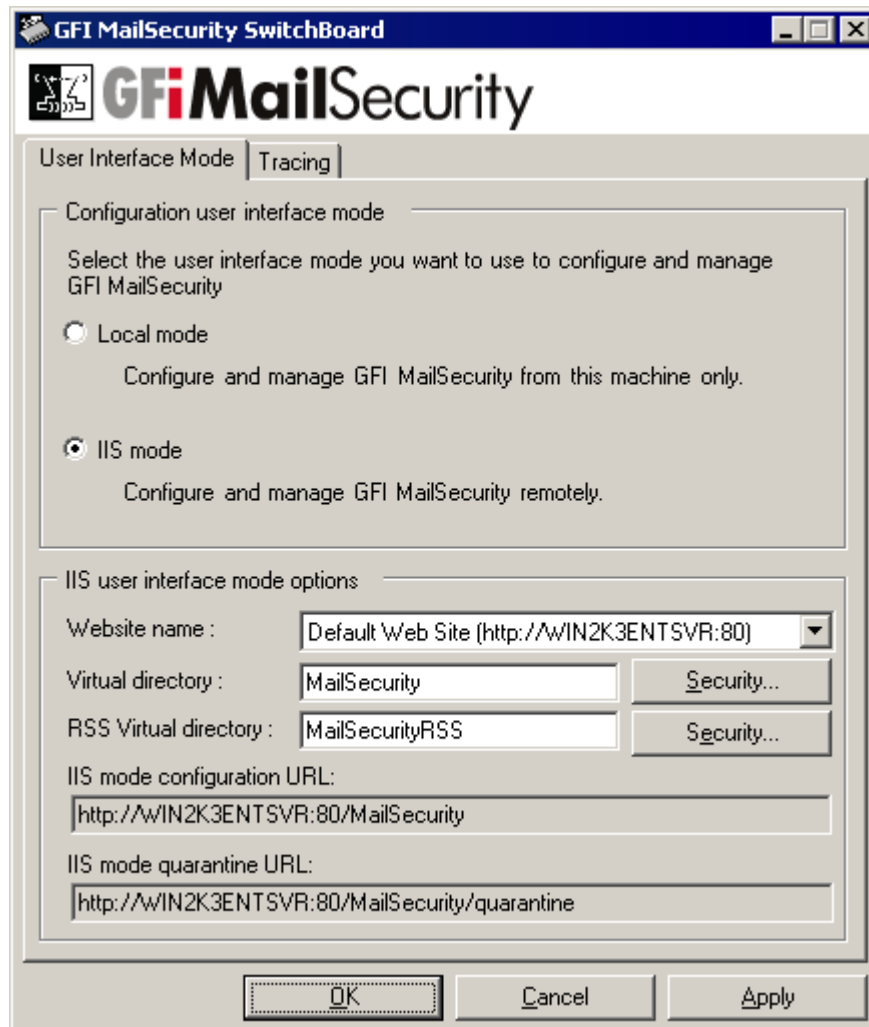


Imagen 17 – GFI MailSecurity SwitchBoard

3. Pulse **Security...** junto a la casilla **RSS Virtual Directory**.
4. Se muestra el diálogo **IIS mode access control list**. Este diálogo le permite configurar quién puede suscribirse a las listas RSS de cuarentena.

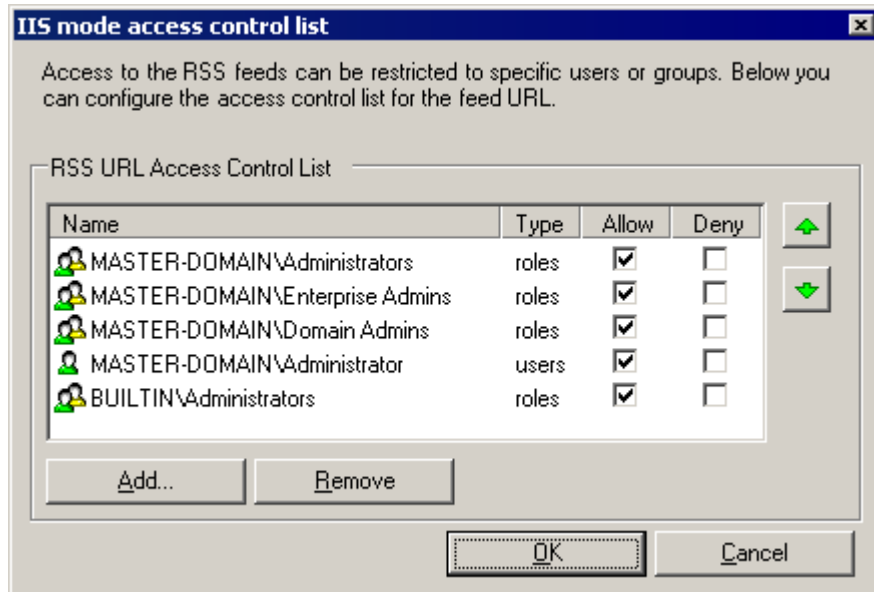


Imagen 18 – Control de Acceso de listas RSS de Cuarentena

5. Utilice los botones **Add** y **Remove** bajo **RSS URL Access Control List**. Si quiere denegar el acceso a una cuenta listada sin eliminarla de la lista, seleccione la casilla bajo la columna **Deny**.
6. Cuando esté listo pulse **Aceptar** para cerrar el diálogo.
7. Si quiere especificar un nombre de directorio virtual diferente, puede hacerlo editando la entrada del campo **RSS Virtual directory**.
8. Haga clic en **Aceptar** para guardar sus cambios. Aparecerá un diálogo mostrando el progreso de aplicar las nuevas opciones.



Imagen 19 – Nuevas opciones SwitchBoard aplicadas satisfactoriamente

9. Cuando finalice el proceso, haga clic en **Aceptar**.

Acceder a la Configuración y Almacén de Cuarentenas de GFI MailSecurity

Esta sección mostrará cómo acceder a la Configuración y Almacén de Cuarentenas de GFI MailSecurity desde el equipo local o desde un equipo remoto.

Acceder a la configuración desde el equipo GFI MailSecurity

Para acceder a la configuración o al almacén de cuarentenas de GFI MailSecurity desde el mismo equipo en el que está instalado, es decir, localmente, siga estos pasos:

1. Inicie **GFI MailSecurity** desde **Inicio ▶ Programas ▶ GFI MailSecurity**.

2. Si ha configurado GFI MailSecurity para ser accesible sólo localmente, mediante la aplicación GFI MailSecurity SwitchBoard, se cargará una aplicación mostrando la configuración y el almacén de cuarentenas de GFI MailSecurity.



Imagen 20 – Accediendo a GFI MailSecurity cuando sólo hay acceso local

Acceder a la configuración desde un equipo remoto

Para acceder a la configuración o al almacén de cuarentenas de GFI MailSecurity desde un equipo remoto, siga estos pasos:

1. Cargue Microsoft Internet Explorer.
2. En la barra de dirección, especifique la siguiente dirección:
'http://<equipo>/<directorio virtual>' para acceder a la configuración o
'http://<equipo>/<directorio virtual>/quarantine' para acceder al almacén de cuarentenas directamente.

Por ejemplo:

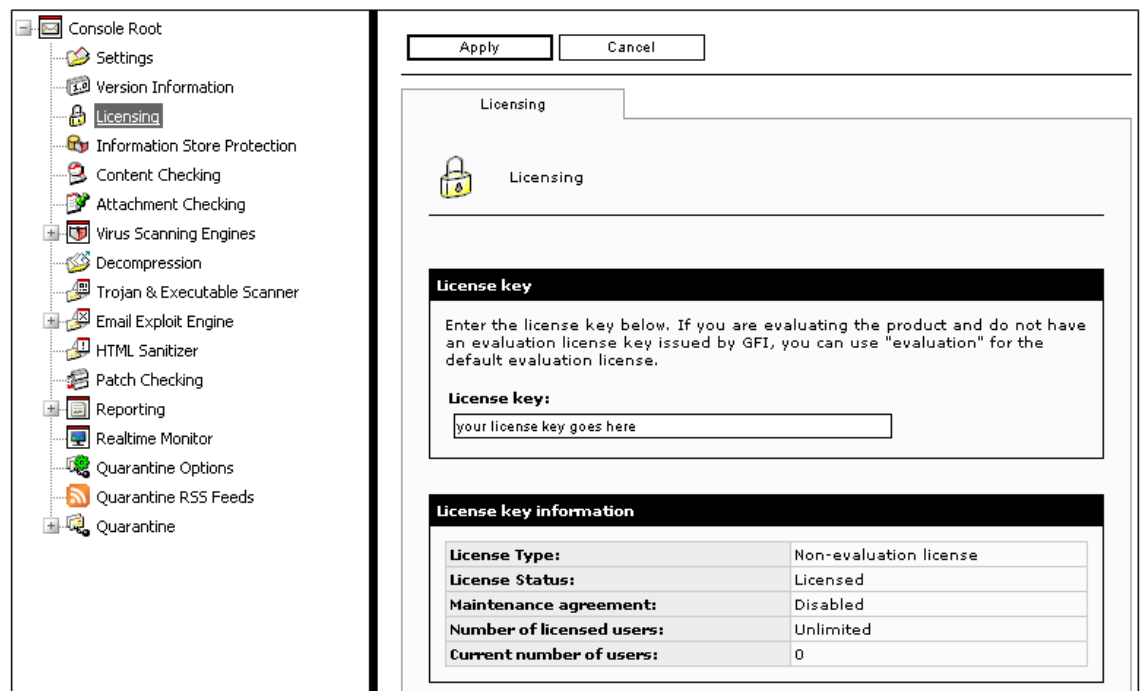
'http://win2k3entsvr.master-domain.com/mailsecurity' para la configuración o 'http://win2k3entsvr.master-domain.com/mailsecurity/quarantine' para el almacén de cuarentenas.

3. Se le pedirá que indique un usuario y contraseña de autenticación para determinar si tiene acceso a la página solicitada. Si la cuenta especificada tiene acceso, se mostrará la configuración o el almacén de cuarentenas de GFI MailSecurity.



Imagen 21 – Accediendo a GFI MailSecurity desde un equipo remoto

Introducir su clave de licencia después de la instalación



Si ha comprado GFI MailSecurity, puede introducir su Clave de licencia en el nodo **Licensing** bajo la **Raiz de Consola**.

Si está evaluando GFI MailSecurity con una clave de evaluación, el producto expirará después de varios días. Si entonces decide comprar GFI MailSecurity, solo tiene que introducir aquí la clave de licencia sin tener que reinstalarlo.

Introducir la clave de licencia no debe ser confundido con el proceso de registrar los detalles de su empresa en nuestro sitio web. Esto es importante, ya que nos permite darle soporte y avisarle sobre noticias importantes sobre los productos. Registre en <http://www.gfi.com/pages/regfrm.htm>.

Actualizar de GFI MailSecurity 8 a GFI MailSecurity 10

Debido a cambios fundamentales de arquitectura entre GFI MailSecurity 10 y GFI MailSecurity 8, no es posible instalar GFI MailSecurity sobre una instalación existente de GFI MailSecurity 8.

Por lo tanto esta sección le muestra cómo:

- Reemplazar su instalación en curso de GFI MailSecurity 8 con GFI MailSecurity 10.
- Migre la configuración de GFI MailSecurity 8 al nuevo formato de configuración de GFI MailSecurity 10.

NOTA: Si GFI MailSecurity 8 fue instalado en modo SMTP y GFI MailSecurity está instalado en modo Directorio Activo, no podrá migrar la configuración debido a las reglas basadas en usuarios. Esto también se aplica si GFI MailSecurity 8 fue instalado en modo Directorio Activo y GFI MailSecurity 10 se instala en modo SMTP.

Para actualizar GFI MailSecurity 8 a GFI MailSecurity 10, siga estos pasos:

1. Desinstale GFI MailSecurity 8.
2. Cuando finaliza la desinstalación de GFI MailSecurity 8, permanecen ciertos archivos bajo la carpeta raíz en la que estaba instalado GFI MailSecurity 8. Uno de estos archivos es `avapicfg.rdb` localizado en la subcarpeta `Data`.

NOTA: No elimine este archivo ya que contiene la configuración de GFI MailSecurity 8. Necesitará este archivo para migrar la configuración de GFI MailSecurity 8 a GFI MailSecurity 10.

3. Instale GFI MailSecurity 10 como se muestra en la sección 'Instalación de GFI MailSecurity' de este capítulo.

NOTA: Para instalar GFI MailSecurity 10, necesita haber instalado en el equipo lo siguiente:

- Microsoft .Net framework 1.1 / 2.0
- MSMQ – Microsoft Messaging Queuing Service.
- Internet Information Services (IIS) – Servicio SMTP y servicio World Wide Web.

NOTA: No instale GFI MailSecurity 10 en la misma ruta en la que estaba instalado GFI MailSecurity 8, para prevenir que los archivos como el `avapicfg.rdb` sean sobrescritos.

4. Una vez completada la instalación de GFI MailSecurity, necesitas detener todos los servicios relativos a GFI junto con el servicio de Administración de IIS, desde el complemento Servicios. A continuación puede ejecutar la herramienta de migración de configuración de GFI MailSecurity 8.

NOTA: Debe detener los siguientes servicios antes de continuar con el siguiente paso:

- GFI Content Security Attendant Service
- GFI Content Security Auto-Updater Service
- GFI MailSecurity Attendant Service
- GFI MailSecurity Scan Engine
- Administración de IIS
- Protocolo de Transferencia Simple de Correo (SMTP).

5. Para migrar la base de datos de configuración de GFI MailSecurity 8 a GFI MailSecurity 10, necesita ejecutar la herramienta msec8upg.exe encontrada en la carpeta de GFI MailSecurity 10, por ejemplo:

C:\Archivos de programa\GFI\ContentSecurity\MailSecurity.

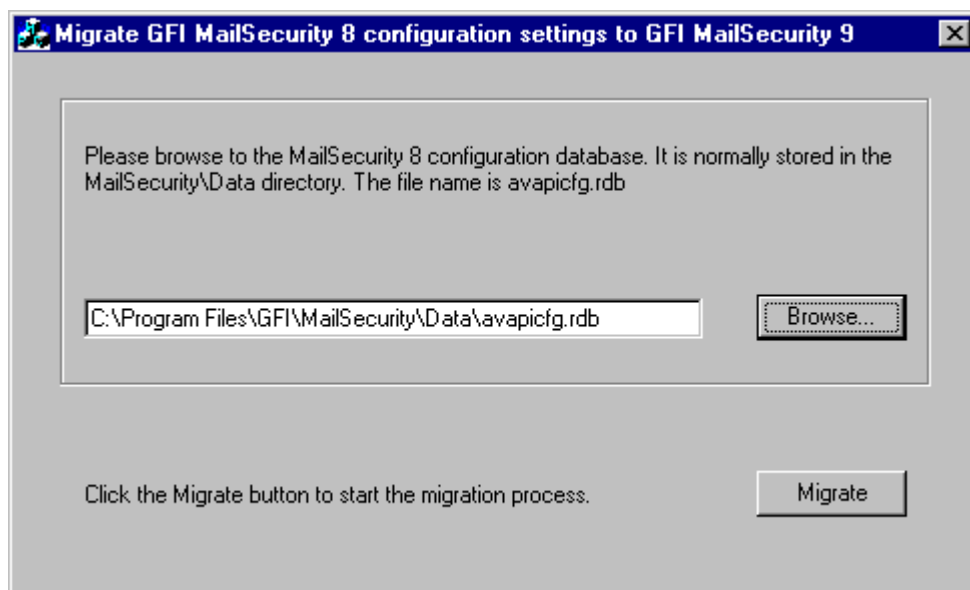


Imagen 23 – Herramienta de migración de la configuración de GFI MailSecurity 8

6. Haga doble clic sobre el archivo msec8upg.exe.

7. Cuando cargue la herramienta, haga clic en **Browse**. Seleccione el archivo avapicfg.rdb desde la subcarpeta Data bajo la carpeta raíz de GFI MailSecurity 8.

8. Haga clic en el botón **Migrate**.

NOTA: Si pulsa el botón de migración y el modo de búsqueda de usuarios de GFI MailSecurity 8 y de GFI MailSecurity 10 no coinciden (por ejemplo, GFI MailSecurity 8 se instaló en modo SMTP y GFI MailSecurity 10 se instaló en modo Directorio Activo o vice versa), se mostrará un error como el que aparece a continuación y no podrá migrar la configuración debido a las reglas de usuarios.

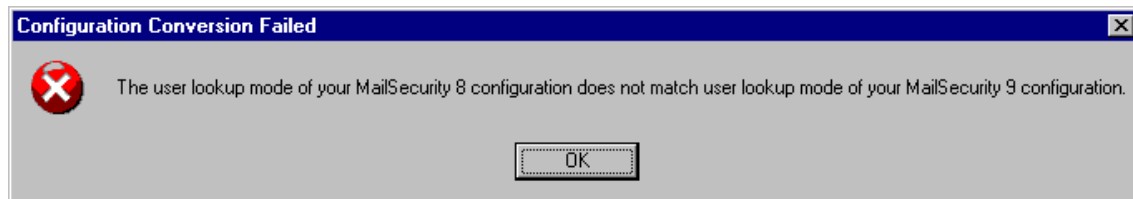



Imagen 24 – Los modos de consulta de usuarios no coinciden.

9. Cuando finalice el proceso de migración, se mostrará el diálogo **Configuration was successfully converted**. Pulse **Aceptar** para cerrar el diálogo y  para cerrar la herramienta de migración.

10. A continuación necesita iniciar todos los servicios que detuvo en el anterior paso 4, desde el componente Servicios.

11. Utilice la configuración de GFI MailSecurity 10 para comprobar que se migró correctamente la configuración de GFI MailSecurity 10.

Actualizar de GFI MailSecurity 9 a GFI MailSecurity 10

NOTA: El proceso de actualización no se puede revertir. Si actualiza GFI MailSecurity a la versión 10, no podrá volver a la versión 9.

Si está actualmente utilizando GFI MailSecurity 9, puede actualizar su instalación actual. Se mantiene la configuración de GFI MailSecurity 9. Necesita introducir la clave de licencia comprada tras finalizar la actualización. Para más información sobre cómo obtener la nueva clave de licencia, visite <http://customers.gfi.com>.

Para actualizar:

1. Inicie el archivo de instalación de GFI MailSecurity 10 en el equipo en el que haya instalado GFI MailSecurity 9. La instalación le consultará si desea eliminar GFI MailSecurity 9 e instalar GFI MailSecurity 10. Haga clic sobre el botón Yes para proceder.

2. La instalación procederá ahora a instalar GFI MailSecurity 10 de la misma forma que una nueva instalación (para una descripción detallada, lea este capítulo), sin embargo no le dejará cambiar la carpeta de destino.