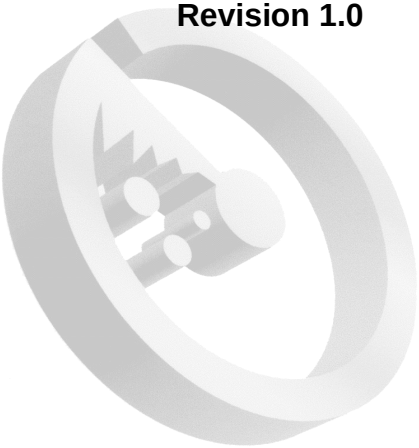
content technologies

MAILsweeper for SMTP

Version 4.0

Getting Started Guide

Revision 1.0



Published by Content Technologies Ltd, June 1999

Content Technologies Ltd.
Forum 1, Station Road
Theale
Berkshire RG7 4RA
United Kingdom
Tel: +44 (0) 118 930 1300
Fax: +44 (0) 118 930 1301

Content Technologies France
24, Rue Jacques Ibert
92300 Levallois-Perret
France
Tel: +33 (0) 1 47 59 21 80
Fax: +33 (0) 1 47 59 20 53

Content Technologies Inc.
204-D Central Way
Kirkland
WA 98033
USA
Tel: +1 425 889 4724
Fax: +1 425 889 5841

Content Technologies (Asia Pacific) Pty Ltd.
Suite 4, 47 Neridah Street
Chatswood
NSW 2067
Australia
Tel: +61 2 9413 1444
Fax: +61 2 9411 3025

email: msw.support@mimesweeper.com
web: http://www.mimesweeper.com

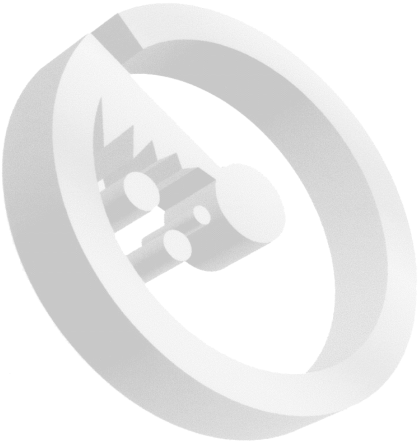
Revision 1.0 June 1999

Contents

CHAPTER 1

Introduction

This chapter presents an overview of MAILsweeper for SMTP and discusses options for deployment of a MAILsweeper system.



Overview

MAILsweeper for SMTP implements your business security by:

- Protecting your organisation's information
- Maintaining your operational effectiveness
- Minimizing legal liability
- Protecting your organisation's image

Threats to SMTP Mail Systems

Electronic messaging has revolutionised the way organisations do business. It has however, led to the emergence of a variety of electronic threats capable of severely compromising an organisation's security and integrity.

Threats to the security and integrity of your organisation, contained in electronic messages (email) and their attachments, include:

- Legal liability
- Potential breaches of confidentiality
- Viruses
- Malicious code which can siphon off data
- Unsolicited mail ("spam")
- Messages from a disguised source ("spoof" mail)
- Offensive or libellous material

A network can also be adversely affected by the receipt of very large emails or file attachments.

MAILsweeper for SMTP helps you combat these threats by enabling you to design and apply your own security policies, implemented for all email passing through your mail system. For example, MAILsweeper can:

- Add legal disclaimers to outgoing messages to guard against legal action

- Examine the content of messages and their attachments to detect possible breaches of confidentiality, unsolicited mail, or offensive material
- Run virus-checking software to detect infected messages and attachments

For more information about how MAILsweeper helps you implement security policies for your electronic messaging system, see *Chapter 7*.

Deployment

MAILsweeper acts as an SMTP mail relay. It has three services:

- MAILsweeper for SMTP Receiver Service
- MAILsweeper for SMTP Delivery Service
- MAILsweeper for SMTP Security Service

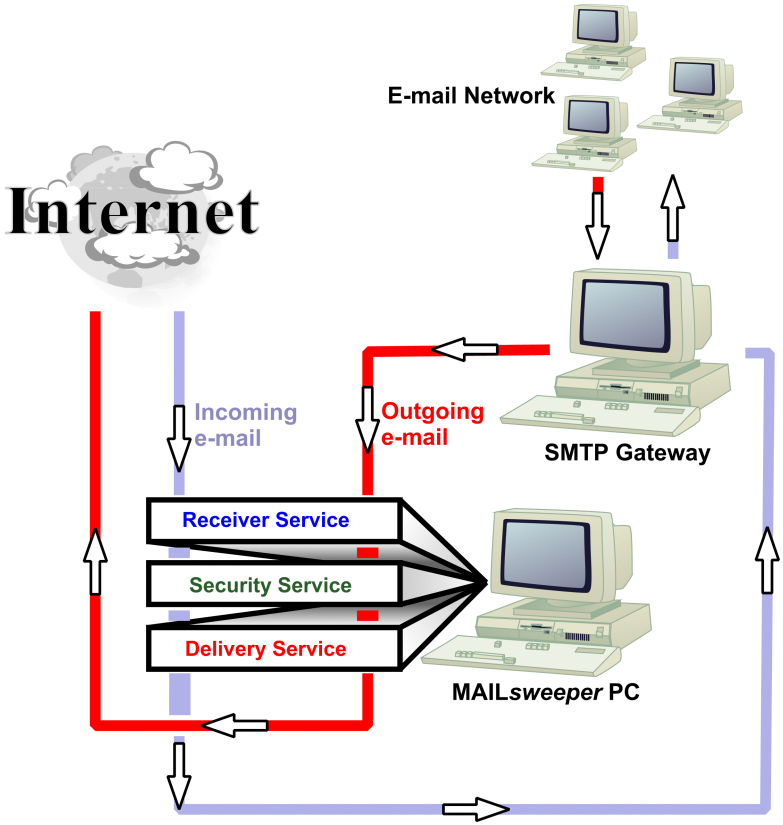


Figure 1-1: MAILsweeper General Arrangement

Logically, MAILsweeper for SMTP is placed between the SMTP gateway and the mail feed from the Internet.

Messages flow through the system as shown in *Figure 1-1: MAILsweeper General Arrangement*

- The *Receiver* service intercepts all incoming and outgoing messages and passes them to the Security service for processing.
- The *Security* service processes each message, using the appropriate policy. It then passes messages that meet your security criteria to the *Delivery* service for onward delivery, and treats other messages according to the configured policy.
- The *Delivery* service uses Domain Name System (DNS) or MAILsweeper routing to determine where to send each mail message after processing.

Firewall and Gateway Considerations

When deploying MAILsweeper for SMTP, you must decide where to place it on the network. The choices depend on whether you have a firewall or not, and whether you intend to use a dialup connection.

Without a Firewall

If you do not have a firewall in place, the MAILsweeper machine is connected to your network and all mail, incoming and outgoing, is routed through MAILsweeper.

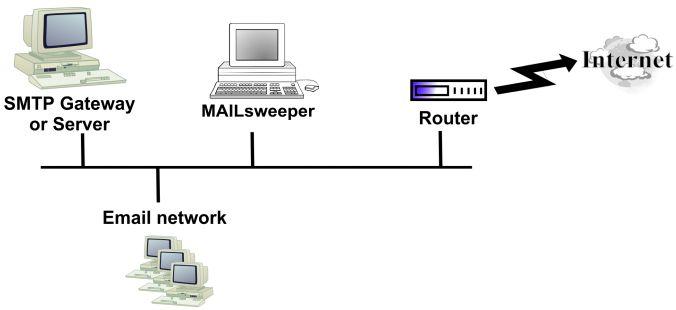


Figure 1-2: MAILsweeper Deployment – No Firewall

With a Firewall

If you have a firewall in place, you have several deployment options, as shown in *Figure 1-3: MAILsweeper Deployment – With Firewall.*

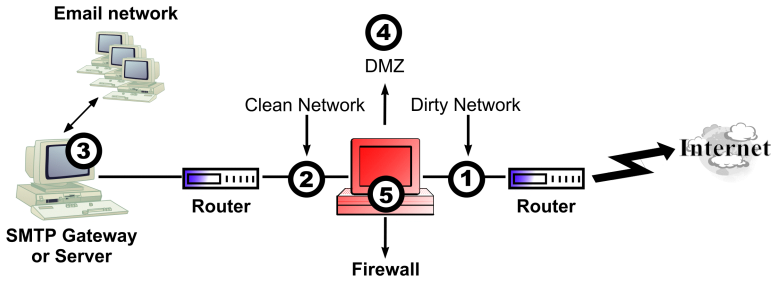


Figure 1-3: MAILsweeper Deployment – With Firewall

These options are:

1. On the **Dirty** network – MAILsweeper is deployed between the Internet (or router) and the firewall
2. On the **Clean** network – MAILsweeper is deployed on the internal network, inside the firewall
3. On the **SMTP Gateway** – MAILsweeper is deployed on the SMTP gateway machine
4. On the **DMZ** – MAILsweeper is deployed in the special demilitarized zone network.

Although it is possible to install MAILsweeper on the firewall, this is not recommended. To pursue this type of installation, contact technical support.

Using a Dialup Connection

MAILsweeper can be configured to use a dialup connection for sending and receiving mail. This arrangement may suit small- to medium-sized companies that do not maintain a permanent internet connection.

At predefined intervals, a dialup connection is made to the Internet Service Provider (ISP). Once connected, a request is made to the ISP mail server to send your incoming mail. MAILsweeper also attempts to deliver outgoing mail through the normal mail routing mechanism; that is, DNS and routing. You can configure the routing so that all outgoing mail is routed to your ISP's mail server for forwarding. This may help to reduce connection times. When there is no more outgoing mail to send and no more incoming mail to receive, the dialup connection is closed.

Locating the MAILsweeper Snap-Ins

The user interface to MAILsweeper for SMTP is supplied in the form of two snap-in tools for the Microsoft Management Console (MMC). These are:

- The Policy Editor, which is used for configuring the system to reflect the policies you want to establish
- The MAILsweeper Manager, which is used for controlling the services and for inspecting messages that have been intercepted

It is normal practice for an organisation's network server and firewall (if it has one) to be located in a secure environment. The Windows NT workstation where you install MAILsweeper should be in this secure area. This machine must have the Policy Editor installed, and it is convenient, though not essential, for it also to have the Manager installed.

You can install a MAILsweeper Manager on any one or more workstations on your network, to allow different people to administer the system from a more convenient location. With more than one Manager components installed, different people can take responsibility for different mail areas. If you do this, you must set up the permissions on the Policy Editor machine to enable the control functions for the remote user or users.

What Next?

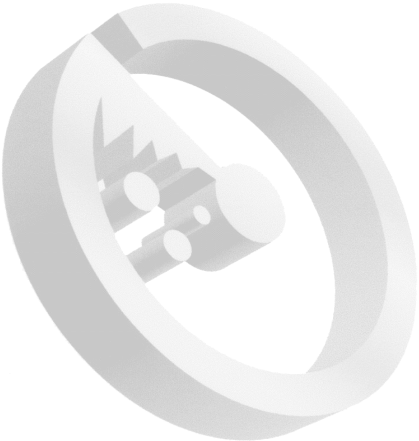
When you have decided how to deploy your MAILsweeper for SMTP system, do the following:

1. Install MAILsweeper for SMTP. See *Chapter 2*.
2. Load any anti-virus tools you require. See *Chapter 2*.
3. Add the Manager snap-in (only after a Remote management only installation). See *Chapter 3*.
4. License your MAILsweeper system. See *Chapter 4*.
5. Set up your network routing. See *Chapter 5*.
6. Set up your security policies. See *Chapter 7*.

CHAPTER 2

Installation

This chapter lists the installation prerequisites and describes how to install and remove MAILsweeper for SMTP. It also gives an overview of anti-virus tools.



Installation Prerequisites

For a full installation of MAILsweeper for SMTP, your machine must meet the following requirements:

Hardware

- Pentium processor
- Minimum of 128 MB of RAM memory
- Minimum or 500 MB of free disk space
- Access to CD-ROM for installation (this could be over the network)
- Network interface card or cards
- A colour graphics system
- A mouse

Software

- Microsoft Windows NT Workstation or Server Version 4.0
- Windows NT Service Pack 4
- TCP/IP including a host and domain name and a Domain Name System (DNS) server entry (check the **Protocols** tab accessed through **Network** in the **Control Panel**)
- Remote Procedure Call (RPC) service
- Remote Access Service (RAS) [1]
- SNMP service[2]
- Microsoft Management Console (MMC) Version 1.1[3]

---

1. RAS is required for dialup support only.
2. The SNMP service is required for SNMP alerters only.
3. The Microsoft Management Console Version 1.1 is provided in the MAILsweeper kit.

- Internet Explorer Version 4.0 with Service Pack 1

If you have an earlier version of MAILsweeper for SMTP, you must remove it from your machine before installing Version 4.0.

Checklist

Before installation, make sure you have the following information:

- The company name for which MAILsweeper will validate messages.
- The local domain name or names for which MAILsweeper will validate messages.
- The IP address or host name of the existing mail gateway.
- The IP address or host name of your proxy-based firewall, if one is used.

Installation Procedure

Once you have determined the configuration required for your network, prepared your network for MAILsweeper deployment, and removed any earlier version of MAILsweeper for SMTP, you can install MAILsweeper for SMTP on the host machine.

MAILsweeper must be installed by a user with write access to the Windows NT registry (such as a user in the Administrator's group).

It is strongly recommended that you exit all Windows programs before running the setup program.

One of the files in the MAILsweeper for SMTP kit is called *SETUP.EXE*. Run this to start the installation, then follow the dialog boxes in the setup wizard.

Setup Type

Choose either:

- A full MAILsweeper for SMTP installation (that is, the MAILsweeper services, MAILsweeper Policy Editor and the MAILsweeper Manager).
- Remote management only. This installs only the Manager component, as described in *Chapter 1*.

Destination Location

Specify the folder in which MAILsweeper for SMTP will be installed. If you change the default setting, specify a folder that is on an NTFS partition.

Company and Domain Names

Specify your company name and your default domain name.

Figure 2-1: Company/Domain Name Dialog Box

The domain specified is used to distinguish between inbound and outbound messages. It is also used to configure MAILsweeper routing, and to construct the default addresses. These are:

- Server – `mailsweeper@<domain>`
- Administrator – `postmaster@<domain>`

You can change these addresses later in the policy editor.

Mail Routing

During installation you are prompted to enter addresses for the forwarding of inbound and outbound mail passing through MAILsweeper. This information is used to initialize the routing and anti-relay configuration

parameters. If you choose not to enter the information at this time, you must use the Policy Editor to configure these parameters later.

Specifying IP addresses rather than host names improves mail throughput.

Inbound

Normally, inbound mail should be forwarded to your SMTP gateway, so enter the IP address (or host name) of your gateway in the **Inbound mail** field.

An exception to this is if you are installing MAILsweeper outside a proxy-based firewall (that is, on the dirty network). In this case, enter the IP address (or host name) of the firewall, so that inbound mail is forwarded to the firewall.

If you are installing on the gateway itself, enter the loopback address (`127.0.0.1`) in the inbound mail field. After installation, you will need to reconfigure the TCP/IP port number used by the gateway and edit the Inbound route accordingly. See *Chapter 5* for more details.

MAILsweeper deems mail to be inbound if the destination domain matches your local domain. If you have multiple local domains, after installation, use the Policy Editor to enter domain synonyms, and to enter a new route for each additional domain.

Outbound

This field can be left blank, in which case DNS will be used for outbound mail routing. However, if you are installing MAILsweeper behind a proxy-based firewall (that is, on the clean network) or in the firewall's DMZ for example, then outbound mail should be forwarded to the firewall. In this case, enter the IP address (or host name) of the firewall.

Figure 2-2: Gateway/Firewall Address Dialog Box

To enable MAILsweeper to check your mail, you may need to modify your MX record or records in the DNS to reference your MAILsweeper machine instead of your existing email gateway.

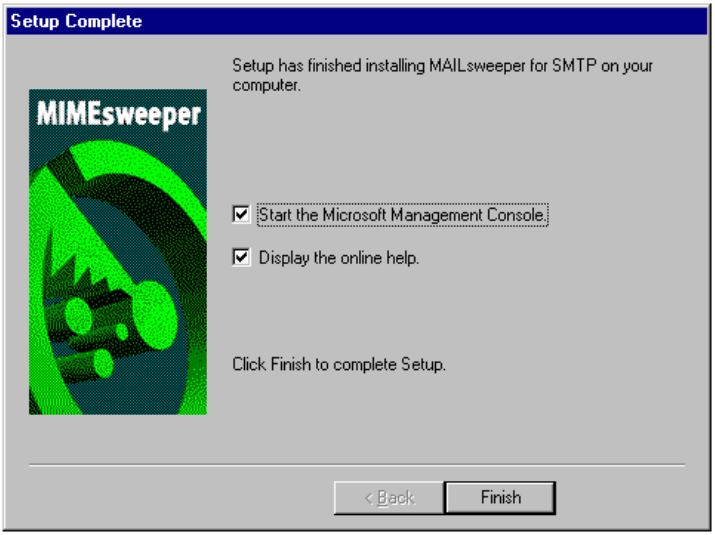


Figure 2-3: Setup Complete Dialog Box

On a full installation, the Policy Editor and Manager snap-ins are loaded automatically, and if you choose to start the Microsoft Management Console (MMC) on completion of the installation, the MMC console is launched.

After a Remote management only installation, you must add the MAILsweeper for SMTP Manager snap-in.

Anti-Virus Tools

You can choose to use almost any anti-virus tool. The MAILsweeper for SMTP kit includes a number of evaluation copies of anti-virus tools. To use any of these, install them separately, according to the instructions in the appropriate README file.

To use an anti-virus tool to check emails and their attachments:

1. Install the anti-virus tool.
2. Create a scenario which calls the tool to check, and if appropriate, clean the message.

   If your anti-virus tool runs as an executable file, use the *Virus Manager* scenario. Use the New Scenario wizard to create links to the anti-virus tool.

   If you install one of the anti-virus tools distributed with the MAILsweeper kit, set up scenarios to use the tool as described in the appropriate README file in the distribution kit. For licensing details, contact the supplier of the anti-virus tool.

Removing MAILsweeper for SMTP

You can remove the current version of MAILsweeper for SMTP from your machine. Do this, for example, if you have installed a MAILsweeper system for testing, or if you wish to move MAILsweeper to a different location.

To remove MAILsweeper for SMTP:

1. In the **Control Panel**, double-click **Add/Remove Programs**.
2. From the list of entries displayed on the **Install/Uninstall** tab, select **MAILsweeper for SMTP**, then click **Add/Remove**.

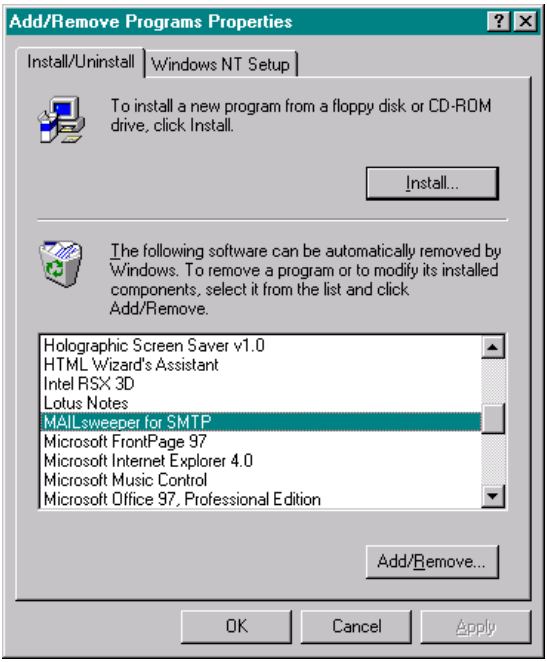


Figure 2-4: Add/Remove Programs

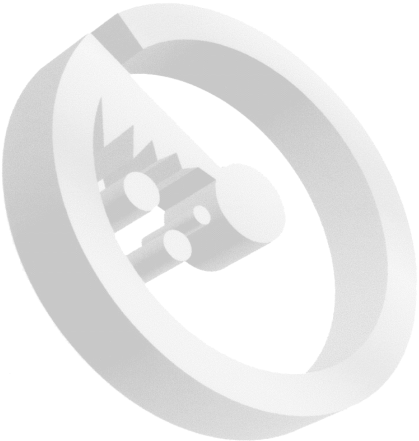
The uninstall process removes most of the MAILsweeper components from the host machine, including all of the *.dll* and *.exe* files. The licence details, configuration settings and the log files are retained.

Some elements cannot be removed by the uninstall program and should be removed after uninstall is complete. It is recommended that you check the *MAILsweeper for SMTP* folder and remove these elements manually.

CHAPTER 3

Adding Snap-ins

This chapter describes how to add the MAILsweeper for SMTP snap-ins to the Microsoft Management Console.



Snap-ins

MAILsweeper for SMTP uses two Microsoft Manager Console (MMC) snap-ins for policy and system management. These are the *Policy Editor* snap-in and the *Manager* snap-in. During a full installation, a default console named *MAILsweeper for SMTP Console* is created containing both of these snap-ins. During a Remote management only installation, no default console is created, and after such an installation you must create a console containing the manager snap-in.

A console contains all the settings of the snap-ins and is saved under its console name as an MSC file. You can create as many consoles as you want in addition to the default created during installation.

Starting the MMC

To start the MMC:

1. From the **Start** menu, choose **Run**.
2. Enter **MMC** and click **OK**.

The MMC starts and displays a default console.

Adding a Snap-in

To add a snap-in:

1. On the **Console** menu, select **Add/Remove Snap-in**.

   The **Add/Remove Snap-in** dialog box appears.

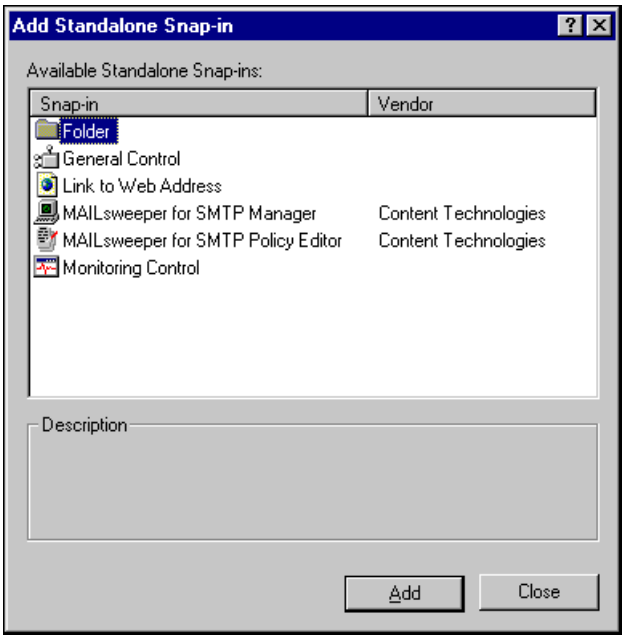


Figure 3-1: Add/Remove Snap-in

2. Click **Add**. The **Add Standalone Snap-in** dialog box appears.
3. Select either the **MAILsweeper for SMTP Policy Editor** or the **MAILsweeper for SMTP Manager** snap-in.

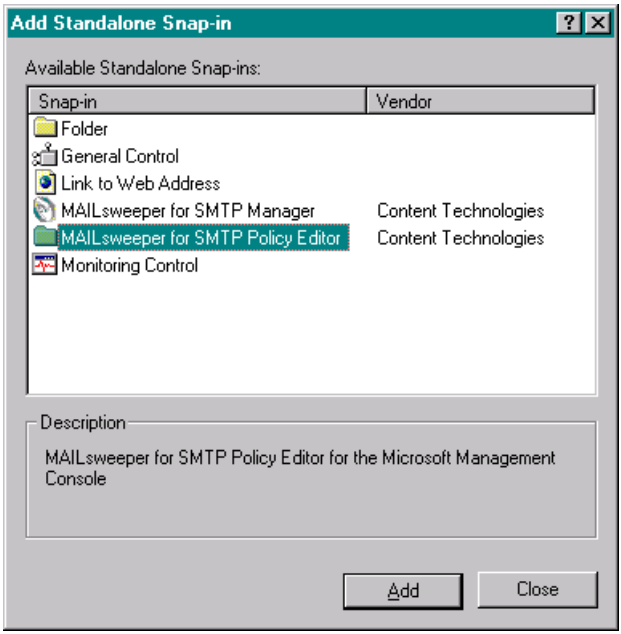


Figure 3-2: Add Snap-in

4. Click **Add**. The *Snap-in* wizard appears. Click **Next**.
5. The process now depends upon which snap-in you are adding:
   a. If you are adding a Policy Editor snap-in, enter the name for the snap-in.
   b. If you are adding a Manager snap-in, enter the machine name. This is the name of the machine running the security service you wish to manage (that is, the machine on which a full installation has been completed).

Figure 3-3: Wizard Machine Name Page

If you are unsure of the machine name, click **Browse** and select from the displayed list.

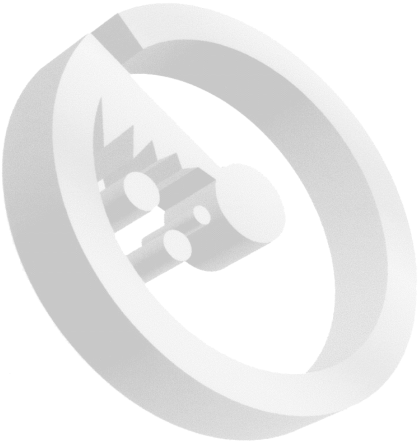
There may be machines whose names do not appear in the browse list. As an alternative to a machine name you can enter its IP address.

6. Repeat steps 3, 4 and 5 to add further snap-ins.
7. Click **Close**, then **OK**.

CHAPTER 4

Licensing

This chapter describes how to license MAILsweeper for SMTP.



Adding a Licence

Before you can use the MAILsweeper for SMTP system, you must add a valid licence on the machine where you did a full installation. To do this:

1. Expand the MAILsweeper Policy Editor tree.
2. Right-click the *Licences* folder, point to **New**, then click **MAILsweeper for SMTP Licence**.

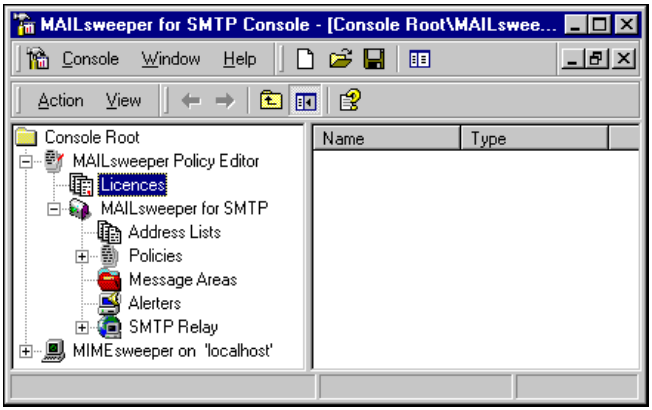


Figure 4-1: Licences

3. In the *New Licence* wizard, enter the details of your new licence. Ensure that you enter the details exactly as supplied.

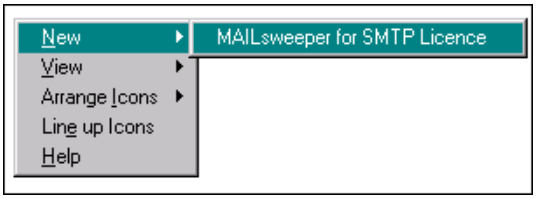


Figure 4-2: New Licence

.

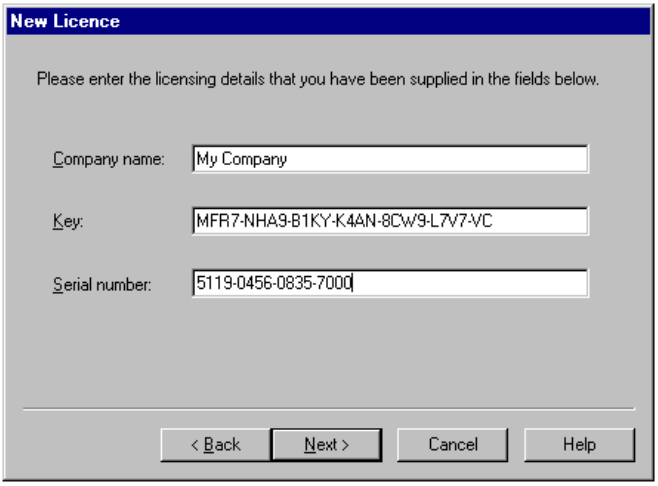


Figure 4-3: Licence details

After setup is complete, the newly-entered licence is listed in the details pane of the console, as shown in *Figure 4-4: New Licence Entry*.

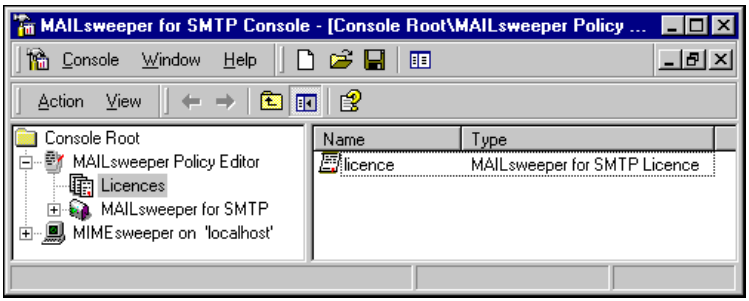


Figure 4-4: New Licence Entry

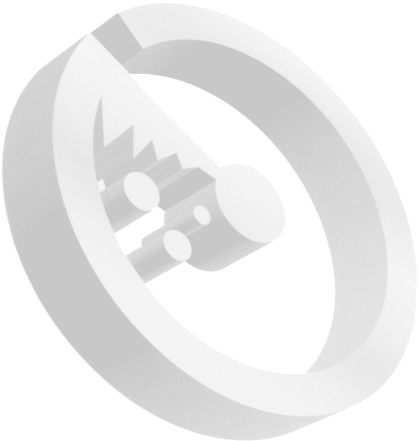
You can now start the delivery, receiver, and security services.

Licences are cumulative. For example, if you have a licence for 100 users and request an upgrade for another 100 users, enter the details of the new licence. Your system will then be licensed for the sum of the two licences, namely 200 users.

CHAPTER 5

Deployment

This chapter describes how to deploy MAILsweeper for SMTP.



Without a Firewall

To deploy MAILsweeper for SMTP on a network without a firewall:

1. Configure the SMTP gateway to forward all outgoing mail to the MAILsweeper machine.

   Refer to the documentation for your gateway for details of how to do this.

2. Ensure that mail routing is configured on the MAILsweeper machine so that incoming mail for your domain or domains is forwarded to the SMTP gateway.

   If, during installation, you entered the IP address or host name of your SMTP gateway as the inbound forwarding address, the MAILsweeper machine is automatically configured to forward mail to the gateway for the domain you entered during installation.

   If you did not enter the IP address or host name of your SMTP gateway during installation you must configure this route. If your organisation has more than one domain, you must configure routing for the remaining domains.

   Routing is configured using the SMTP Relay folder of the MAILsweeper Policy Editor. For further details, click **Help** on the New Route wizard pages.

3. Alter the MX records on the Domain Name Server (DNS) that currently reference your SMTP gateway to reference the address of the MAILsweeper machine.

With a Firewall

If you have a firewall, the deployment options are:

- On the **Dirty** network – MAILsweeper is deployed between the Internet (or router) and the firewall.
- On the **Clean** network – MAILsweeper is deployed on the internal network, inside the firewall.
- On the **SMTP Gateway** – MAILsweeper is deployed on the SMTP gateway machine.
- On the **DMZ** – MAILsweeper is deployed in the special de-militarised zone network.

On the Dirty Network

To deploy MAILsweeper for SMTP on the dirty network:

1. For a **packet-based** firewall, configure the SMTP gateway to forward outgoing mail to the MAILsweeper machine.

   Refer to the documentation for your gateway for details of how to do this.

   For a **proxy-based** firewall, change routing on the firewall to forward outgoing mail to the MAILsweeper machine.

   Refer to your firewall documentation for details.

2. For a **packet-based** firewall, ensure that mail routing is configured on the MAILsweeper machine so that all incoming mail for your domain or domains is forwarded to the SMTP gateway.

   If during installation you entered the IP address or host name of your SMTP gateway as the inbound forwarding address, the MAILsweeper machine is automatically configured to forward incoming mail to the gateway for the domain entered during installation.

   In the example shown in *Figure 5-1: Routing for Packet-Based Firewall*, `mycompany.com` is the name of your organisation's email domain and `gateway` is the name of the SMTP gateway.

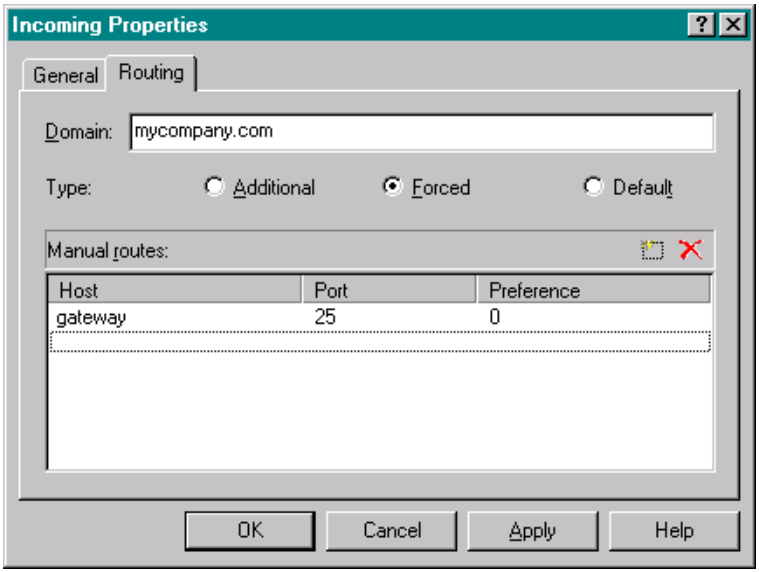


Figure 5-1: Routing for Packet-Based Firewall

If you did not enter the IP address or host name of your SMTP gateway during installation you must configure this route. Additionally, if your organisation has more than one domain, you must configure routing for the remaining domains. Use the SMTP Relay folder of the MAILsweeper Policy Editor to do this.

For a **proxy-based** firewall, ensure that mail routing is configured on the MAILsweeper machine so that all incoming mail for your domain or domains is forwarded to the firewall. The SMTP proxy on the firewall will route the mail to the SMTP gateway machine.

If during installation you entered the IP address or host name of your firewall as the inbound forwarding address, the MAILsweeper machine is automatically configured to forward incoming mail to the firewall for the domain you entered during installation.

In the example shown in *Figure 5-2: Routing for Proxy-Based Firewall*, `mycompany.com` is the name of your organisation's email domain and `firewall` is the name of the firewall.

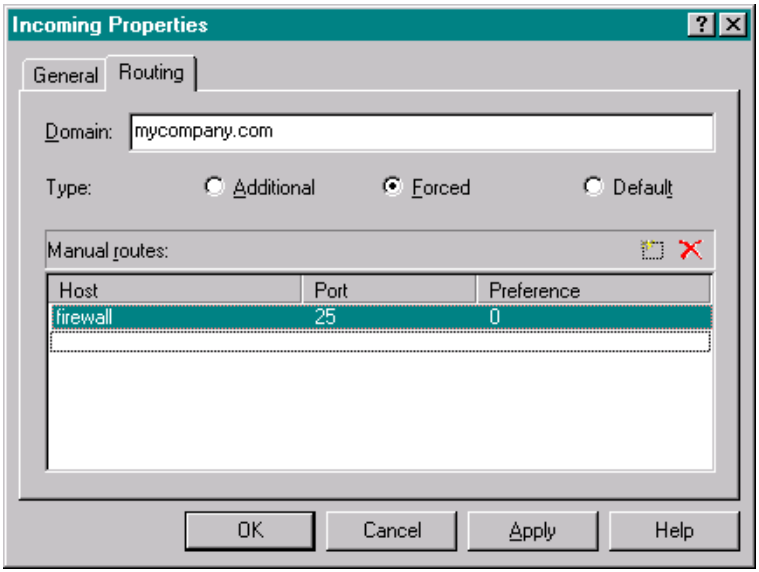


Figure 5-2: Routing for Proxy-Based Firewall

If you did not enter the IP address or host name of your firewall during installation you must configure this route. Additionally, if your organisation has more than one domain, you must configure routing for the remaining domains. Use the SMTP Relay folder of the MAILsweeper Policy Editor to do this.

3. Secure the firewall so that:

   • Outgoing SMTP mail can go only to the MAILsweeper host.

   • Incoming SMTP mail can come only from the MAILsweeper host.

4. Alter the MX records on the Domain Name Server (DNS) that currently reference your SMTP gateway or proxy-based firewall to reference the address of the MAILsweeper machine.

5. Secure the MAILsweeper machine.

   See *Chapter 7* for details of how to secure the MAILsweeper host machine.

On the Clean Network

To deploy MAILsweeper for SMTP on the clean network:

1. Configure the SMTP gateway to forward outgoing mail to the MAILsweeper machine.

   Refer to the user documentation for your gateway for details of how to do this.

2. For a **proxy-based** firewall, change routing on the firewall to send incoming mail to the MAILsweeper machine.

   Refer to your firewall documentation for details.

3. Ensure that mail routing is configured on the MAILsweeper machine so that all incoming mail for your domain or domains is forwarded to the SMTP gateway.

   If during installation you entered the IP address or host name of your SMTP gateway as the inbound forwarding address, the MAILsweeper machine is automatically configured to forward incoming mail to the gateway for the domain you entered during installation.

   In the example shown in *Figure 5-1: Routing for Packet-Based Firewall*, `mycompany.com` is the name of your organisation's email domain and `gateway` is the name of the SMTP gateway.

   If you did not enter the IP address or host name of your SMTP gateway during installation you must configure this route. Additionally, if your organisation has more than one domain, you must configure routing for the remaining domains. Use the SMTP Relay folder of the MAILsweeper Policy Editor to do this.

   For a **proxy-based** firewall, it is also necessary to ensure that mail routing is configured on the MAILsweeper machine so that mail for all other domains (outgoing mail), is forwarded to the firewall.

   If during installation you entered the IP address or host name of your firewall as the outbound forwarding address, the MAILsweeper machine is automatically configured to forward outgoing mail to the firewall.

   In the example shown in *Figure 5-3: Routing for Proxy-Based Firewall*, * represents mail for all other domains (outgoing mail) and `firewall` is the name of the firewall.

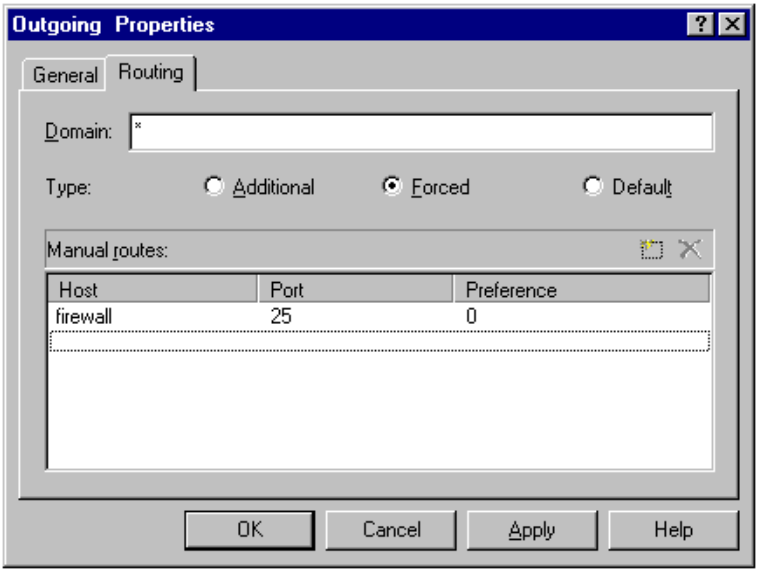


Figure 5-3: Routing for Proxy-Based Firewall

If you did not enter the IP address or host name of your firewall during installation you must configure this route. Use the SMTP Relay folder of the MAILsweeper Policy Editor to do this.

4. Secure the firewall so that:

   • Outgoing SMTP mail can come only from the MAILsweeper host.

   • Incoming SMTP mail can go only to the MAILsweeper host.

5. Secure the MAILsweeper machine.

   See *Chapter 7* for details of how to secure the MAILsweeper host machine.

On the SMTP Gateway

To deploy MAILsweeper for SMTP on the SMTP gateway:

1. Allocate a new TCP/IP port for routing SMTP mail within the gateway machine.

   This must be a port that is not allocated to any other service. For example, you might allocate `20025`. Check the *Services* files to ensure that the port is free.

2. Configure the SMTP gateway to listen on the newly-allocated port.

   Refer to the documentation for your gateway for details of how to do this.

The choice of SMTP port for receiving mail must be configurable on the SMTP gateway. It is only possible to deploy MAILsweeper for SMTP on the gateway if the gateway has this facility.

3. Configure the SMTP gateway to forward all outgoing mail to the *localhost* host name, which is an alias to the address `127.0.0.1` or loopback address. This forwards all outgoing mail to MAILsweeper for processing.

   Refer to the documentation for your gateway for details of how to do this.

4. Ensure that mail routing is configured on the MAILsweeper machine so that all incoming mail for your domain or domains is forwarded to `127.0.0.1`. This forwards all incoming mail to the SMTP gateway, which is listening on the newly-allocated port.

   If during installation you entered the *localhost* host name or IP address (`127.0.0.1`) as the inbound forwarding address, the MAILsweeper machine is configured to forward incoming mail to this address for the domain you entered during installation. However, you must configure the *Port* entry to reflect the newly-allocated port that the SMTP gateway listens on (by default the installation sets this to `25`).

   In the example shown in *Figure 5-4: Routing for the Gateway*, `mycompany.com` is the name of your organisation's email domain, `localhost` is the name of the SMTP gateway (you could also use `127.0.0.1`), and `20025` is the newly-allocated port.

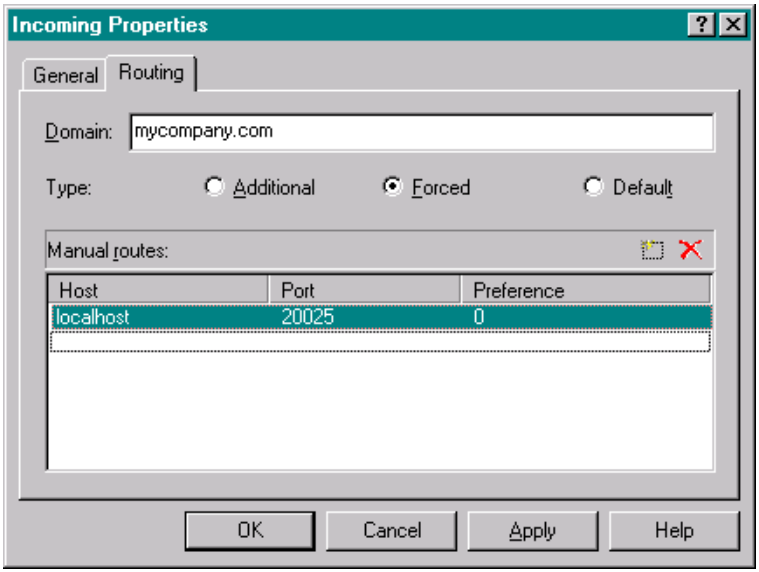


Figure 5-4: Routing for the Gateway

If you did not enter the *localhost* name or IP address during installation you must configure this route now. Additionally, if your organisation has more than one domain, you must configure routing for the remaining domains. Use the SMTP Relay folder of the MAILsweeper Policy Editor to do this.

If the gateway is inside a **proxy-based** firewall, you must also ensure that mail routing is configured so that mail for all other domains (outgoing mail), is forwarded to the firewall.

If you entered the IP address or host name of your firewall during installation as the outbound forwarding address, the MAILsweeper machine is automatically configured to forward outgoing mail to the firewall.

If you did not enter the IP address or host name of your firewall during installation you must configure this route now. Use the SMTP Relay folder of the MAILsweeper Policy Editor to do this.

5. Secure the gateway machine.

See *Chapter 7* for details of how to secure the MAILsweeper host machine.

On the DMZ

To deploy MAILsweeper for SMTP on the DMZ:

1. For a **packet-based** firewall configure the SMTP gateway to forward outgoing mail to the MAILsweeper machine.

   Refer to the documentation for your gateway for details of how to do this.

   For a **proxy-based** firewall change routing on the firewall to send incoming mail to the MAILsweeper machine.

   Refer to your firewall documentation for details.

2. Ensure that mail routing is configured on the MAILsweeper machine so that all incoming mail for your domain or domains is forwarded to the SMTP gateway.

   If during installation you entered the IP address or host name of your SMTP gateway as the inbound forwarding address, the MAILsweeper machine is automatically configured to forward incoming mail to the gateway, for the domain you entered during installation.

   In the example of *Figure 5-1: Routing for Packet-Based Firewall*, `mycompany.com` is the name of your organisation's email domain and `gateway` is the name of the SMTP gateway.

   If you did not enter the IP address or host name of your SMTP gateway during installation, you must configure this route. Additionally, if your organisation has more than one domain, you must configure routing for the remaining domains. Use the SMTP Relay folder of the MAILsweeper Policy Editor to do this.

   For a **proxy-based** firewall, it is also necessary to ensure that mail routing is configured on the MAILsweeper machine so that mail for all other domains (outgoing mail), is forwarded to the firewall.

   If during installation you entered the IP address or host name of your firewall as the outbound forwarding address, the MAILsweeper machine is configured to forward outgoing mail to the firewall.

In the example of *Figure 5-3: Routing for Proxy-Based Firewall*, `*` represents mail for all other domains (outgoing mail) and `firewall` is the name of the firewall.

If you did not enter the IP address or host name of your firewall during installation you must configure this route. Use the SMTP Relay folder of the MAILsweeper Policy Editor to do this.

3. Secure the firewall so that:

   • Outgoing SMTP mail can come only from the MAILsweeper host.

   • Incoming SMTP mail can go only to the MAILsweeper host.

4. For a **packet-based** firewall only, alter the MX records on the Domain Name Server (DNS) that currently reference your SMTP gateway to reference the address of the MAILsweeper machine.
5. Secure the MAILsweeper machine.

   See *Chapter 7* for details of how to secure the MAILsweeper host machine.

If there is more than one route, the order of routes is important. The delivery service traverses the list from top to bottom and stops at the first entry with a matching domain. It is vital that the more specific entries (incoming) appear before the wildcard entries (outgoing).

Using a Dialup Connection

If you have a firewall, and you intend to use a dialup connection, you should deploy MAILsweeper on the dirty network (see *Chapter 1*).

To configure MAILsweeper for SMTP to use a dialup connection:

1. Install Windows NT Remote Access Service (RAS). Dialup support requires this service.
   a. On the **Control Panel**, double-click **Network**.
   b. Select the **Services** tab and click **Add**.

   Refer to the Windows NT documentation for more details.
2. Define a phone book entry for connecting with your ISP.

   MAILsweeper uses Windows NT Dial-Up Networking (part of the Remote Access Service) to initiate the dial-up connection. A Dial-Up Networking phone book entry must be defined, specifying the phone number you need to dial to connect to your ISP.

   This entry can be defined in either of two ways:

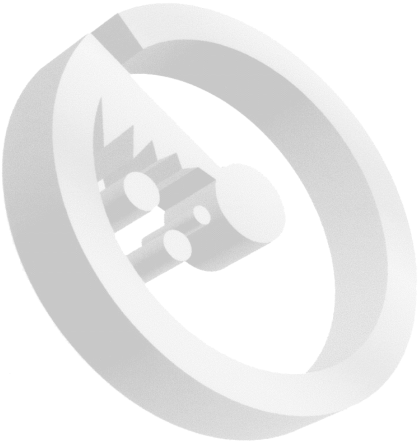
   a. Click the Windows **Start** button, point to **Programs**, then **Accessories**, then click **Dial-Up Networking**.
   b. From the **Dialup** settings in the SMTP Relay folder of the MAILsweeper Policy Editor.

   It is recommended that you test this dial-up connection manually, to ensure that it is set up correctly. This can be done using Dial-Up Networking or the *RASDIAL* command.
3. Configure the SMTP dialup connection for sending and receiving mail. This can be configured to your own requirements.

CHAPTER 6

Management

This chapter gives a brief tour of the options available in the MAILsweeper for SMTP Manager.



Messages

MAILsweeper for SMTP intercepts questionable messages according to the policies you have set up, and places them in message areas for later processing. If you have set up appropriate notifications it also informs you of the action it has taken.

You can examine the contents of the message and analyse the reasons for its being placed in a message area. You can also dispose of such messages in a variety of ways.

Message Areas

MAILsweeper for SMTP creates a number of message areas on installation, and you can use the policy editor to create more.

Once the security service is running you can view the message areas by expanding the Message Areas item in the console tree. Double-click the message area name to see the messages held.

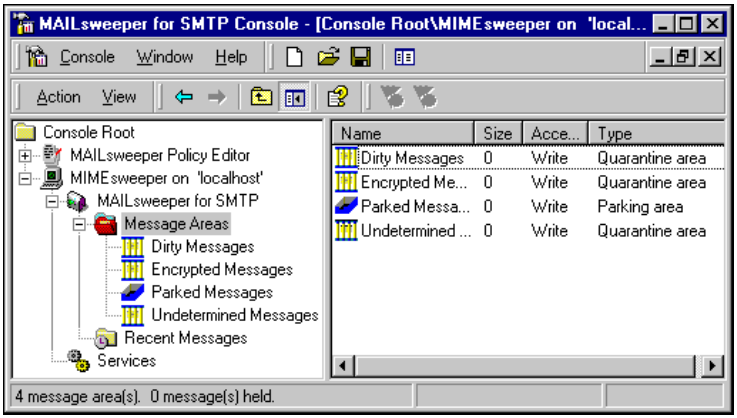


Figure 6-1: Message Areas

Examining the Details of a Message

Double-click the message entry in the details pane to see the message properties box.

To open a message in order to examine it in more detail, right-click the message then click **Open**. Click **Help** for more information.

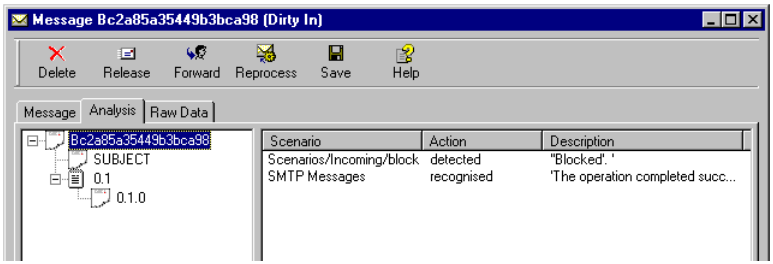


Figure 6-2: Open Message Detail

Processing Options

To process a message, right-click the message and choose one of the options from the menu that is displayed. These options are:

- **Open** – as described.
- **Delete** – deletes the message.
- **Release** – releases the message into the delivery queue.
- **Forward** – forwards a copy of the message to the recipient of your choice.
- **Reprocess** – puts the message back through the security service to be reprocessed. Use this option, for example, if you are testing a policy or if you have changed the policy.
- **Save** – saves the message in a file area.

For further details click **Help**.

Recent Messages

You can display the Recent Messages to monitor the behaviour of the system. The details pane shows a rolling display of all processed messages. Messages that are intercepted will be diverted to message areas or simply blocked.

Double-click a message to examine its details. The display is similar to that for messages in the message areas.

Services

You can start and stop each of the three services (delivery, receiver, and security).

To start a service, select **Services** in the console tree, select the service name in the details pane and click the green flag icon.

To stop a service, select the service name and click the red flag icon.

Figure 6-3: Services

CHAPTER 7

Implementing Security Policies

This chapter describes the basic concepts and elements of MAILsweeper for SMTP, and lists the main properties of the system. It also describes how to secure the MAILsweeper host machine.

The second half of the chapter shows a worked example for use as a model for setting up your own policies.

MAILsweeper Concepts and Elements

MAILsweeper for SMTP protects your organisation from threats such as those described in *Chapter 1* through the implementation of *policies* that you define. Policies identify:

- Which messages to check
- What threats to guard against
- What to do with offending or suspect messages, and who to inform about them

Which Messages to Check

MAILsweeper implements security policies according to the intended route or routes of each message, as defined by its sender and recipients. You can, for example, specify a security policy to apply to all messages sent from outside your organisation to all users within your organisation. Other policies may apply only to particular groups or individuals, such as members of staff in the Sales department, or anyone working in a rival organisation.

Many email messages are sent to multiple recipients. If different policies apply to different routes of the same message, MAILsweeper for SMTP splits the message into separate messages and processes each according to the relevant policy.

When you set up a security policy on MAILsweeper for SMTP, you create a *scenario folder* for the sender/recipient routes to which the policy is to apply. You can specify individual sender/recipient combinations, or use *address lists* to define these routes.

Scenario folders can be arranged in a hierarchy, with higher-level folders applying to more general routes (such as all messages entering your organisation's domain) and lower levels defining more specific sets of users. When processing a message, MAILsweeper checks each scenario folder, starting at the top of the hierarchy, and for each route of the message,

finds the folder with the best match (that is, the match made using the least amount of wild cards).

What Threats to Guard Against

For each potential threat you want to guard against, such as virus-infected messages or the leaking of confidential material, you set up a *scenario*, which implements a single security check. MAILsweeper provides a number of scenario types, such as those that check the content for confidential material and those that run virus-checking software to check for infected messages.

Scenarios are set up in scenario folders according to the routes to which they are to apply.

What Action to Take

Classifications define what to do with messages processed by a scenario. Each classification determines *actions* (what to do with the message) and *notifications* (how to record and disseminate information about the message).

When implementing a security policy, you create a classification which you then reference as you create scenarios.

MAILsweeper for SMTP defines several types of action and notification. One type of notification is an *alert*, which uses the alerter mechanism to broadcast a message to the administrator. To use this type of notification, you must first set up an *Alerter*.

Classifications can be either *Exclusive* or *Inclusive***:**

- Exclusive classifications define actions, such as deletion or delivery, that are performed only once for any message.
- Inclusive classifications define actions to be applied in addition to an exclusive classification. Any number can be applied to a message.

The order in which classifications are listed is significant. Exclusive classifications are listed order of priority, so that when a message matches more than one such classification, only the first is applied. Inclusive

classifications are listed after exclusive classifications. The order in which inclusive classifications appear is not important.

Properties

Before you configure your security policies, examine the properties of the Policy Editor folders shown in Table 7-1.

Table 7-1: MAILsweeper Properties

Property	Description
MAILsweeper for SMTP	Basic MAILsweeper options.
Policies	Transport protocol security and message format options.
SMTP Relay	The retry schedule for delivering messages, and transport protocol logging options.

To display the properties, right-click the folder in the console tree, then click **Properties**. Details of the properties are given in the help. To see the help, click **Help** on the property page.

Once you are familiar with the properties, make any changes you require.

SMTP Relay

When you select the *SMTP Relay* folder in the console tree, the items shown in Table 7-2 are listed in the details pane:

Table 7-2: SMTP Relay Items

Item	Description
Routing	Defines the routing of email messages, according to their destination domain. See *Chapter 5*.
Aliases	Defines equivalent email addresses.
Dialup	Settings for dialup support.
Domain	Synonyms for your local domain.

Reloading Policies

When you make any changes to the system properties or policies, you must stop and restart the affected service (see *Chapter 6*), or reload your policies.

To reload your policies, right-click **MAILsweeper for SMTP**, then click **Reload policy**.

Securing the Host Machine

It is important to secure the MAILsweeper host machine to protect it from unauthorized access and to prevent it from providing access to the rest of the network. To do this:

1. In the **Control Panel**, double-click the **Network** icon.
2. Disable forwarding of IP, to stop the MAILsweeper machine acting as a router, as follows:
   i. On the **Protocols** tab of the **Network** dialog box, select the **TCP/IP** entry, then click **Properties**.

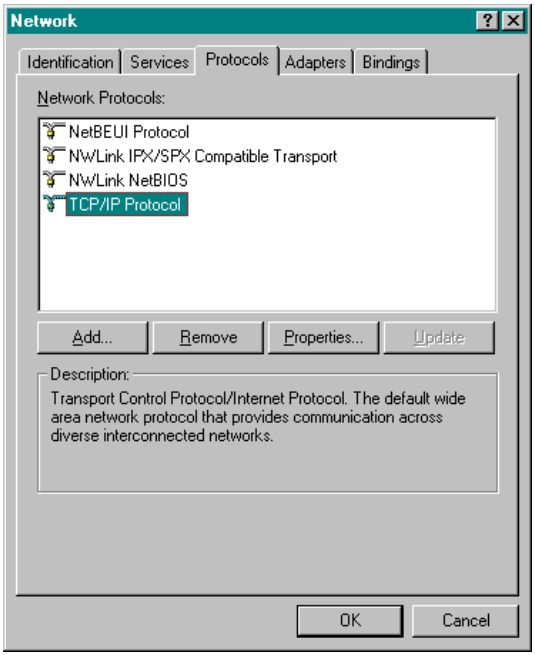


Figure 7-1: Network Protocols

ii. On the **Microsoft TCP/IP Properties** dialog box, select the **Routing** tab.

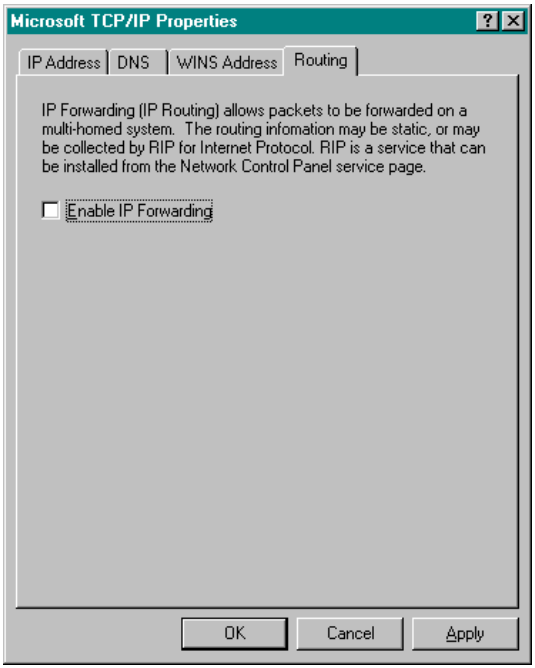


Figure 7-2: TCP/IP Properties Dialog Box

iii. Clear the **Enable IP Forwarding** box.

iv. Click **OK**.

3. Disable the WINS client (TCP/IP) binding to the Server service. This disables remote access to shared resources over TCP/IP.

This may affect other network operations, such as logging in to NT domains, when the only network protocol used is TCP/IP.

To disable the WINS client (TCP/IP) binding:

i. Select the **Bindings** tab of the **Network** dialog box.

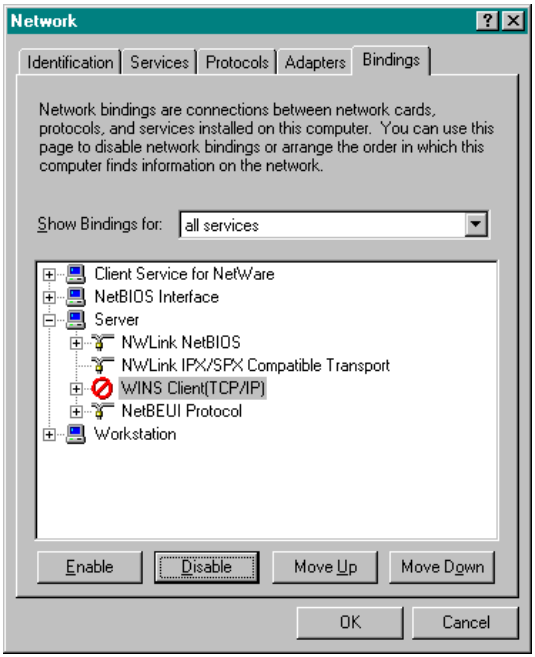


Figure 7-3: Network Bindings

ii. Select **all services** in the **Show Bindings for** field.

iii. Expand the **Server** entry, then select **WINS Client (TCP/IP)**.

iv. Click **Disable**. A red warning symbol to the left of the **WINS Client (TCP/IP)** entry indicates that the service is disabled (as shown in *Figure 7-3: Network Bindings*)

v. Click **OK**.

You can enable further security settings by clicking **Advanced** on the **IP Address** tab of the **Microsoft TCP/IP Properties** dialog box.

Worked Example

The following sections work through an example based on the details shown in Table 7-3.

Table 7-3: Example Details

Company	*Example Exports Ltd.* (entered during installation).
Domain	*example.com* (entered during installation).
Partners with	*Ally Exports Ltd.* and *Friendly Exports Inc.*, who have domains *ally.com* and *friendly.com* respectively.
Rivals with	*Enemy Exports Ltd.* and *Rival Export Corporation*, who have domains *enemy.com* and *rival.com* respectively.

The example specifies the following policies:

- All messages must be scanned for viruses.
- A legal disclaimer must be added to all outgoing messages.
- Messages over 1 MB should not be sent during a working day.
- Confidential material can be sent to partners, but to no one else.
- No messages can be sent between the company and its rivals.
- Prevent the company gateway being used for mail relay.

This example assumes that you have installed anti-virus software that runs as an executable file.

These policies are to be enforced as follows:

- **Address Lists**

  Create address lists for partners and rivals. See *page 7-13*.

- **Incoming virus-infected messages**

  Quarantine all incoming messages infected with a virus for two days and send a message to the intended recipients asking them to contact the administrator for a clean copy.

  i. Create a new scenario. See *page 7-14*.

ii. Create a quarantine action. See *page 7-15*.

iii. Create an inform notification. See *page 7-16*.

- **Outgoing virus-infected messages**

  Destroy all outgoing messages infected with a virus and notify the sender with instructions to clean their system before sending any more mail.

  i. Create a new scenario. See *page 7-18*.

  ii. Create an inform notification. See *page 7-19*.

- **Legal disclaimer**

  Add legal disclaimers to the end of all outgoing messages. See *page 7-20*.

- **Large messages**

  Park outgoing messages larger than 1MB between the hours of 9am and 6pm weekdays. See *page 7-21*.

- **Confidential material**

  If confidential material is detected in outgoing mail, send a message to the administrator and quarantine the message in a quarantine area with no automatic deletion. Exclude messages sent to partners from this rule.

  i. Create a new quarantine area. See *page 7-23*.

  ii. Create a new classification. See *page 7-23*.

  iii. Create a new quarantine action. See *page 7-24*.

  iv. Create an inform notification. See *page 7-25*.

  v. Create a new scenario. See *page 7-26*.

  vi. Create a new scenario folder. See *page 7-27*.

  vii. Set the *Text Analyzer* scenario state. See *page 7-28*.

- **Prohibited messages**

  Forward to the administrator any message addressed to a rival, and destroy the message.

  i. Create a new scenario folder. See *page 7-29*.

ii. Create a new exclusive classification. See *page 7-30*.

iii. Create a new action. See *page 7-31*.

iv. Create a new scenario. See *page 7-32*.

- **Relay prevention**

  Ban all mail arriving at MAILsweeper that is not destined for your local domains, and is not from your local gateway. See *page 7-32*.

Address Lists

Create address lists for the company's partners and rivals. These will be used later, when setting up routes in the scenario folders.

1. Right-click the *Address Lists* folder, point to **New** then click **Address List**.
2. In the wizard, enter the user addresses as shown in *Figure 7-4: Partners Address List*.
3. Give the list the name *Partners*.
4. Use the same procedure to create the *Rivals* list as shown in *Figure 7-5: Rivals Address List*.

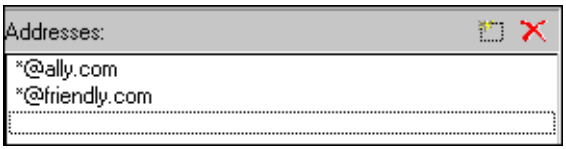


Figure 7-4: Partners Address List

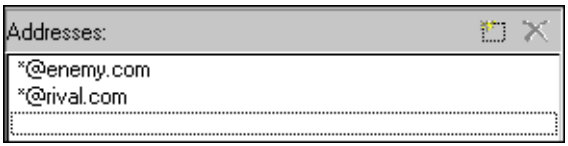


Figure 7-5: Rivals Address List

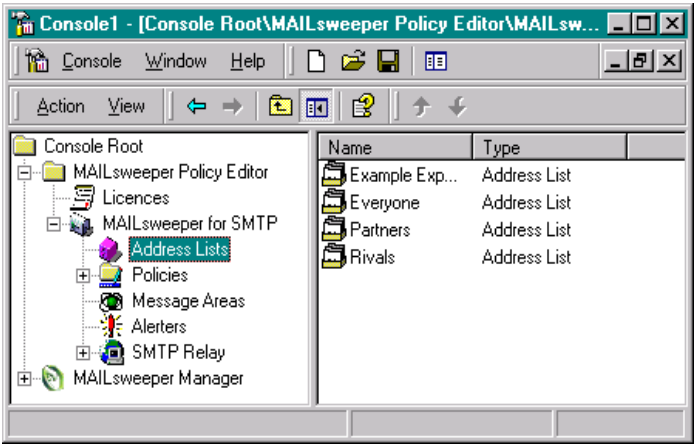


Figure 7-6: Address List Folder

The *Rivals* and *Partners* address lists are added to the *Address Lists* folder, together with the two address lists created during installation, which, in the case of Example Exports Ltd., are:

- *Example Exports Ltd.*, which has one entry representing everyone at the company's domain (**@example.com*).
- *Everyone*, which has one entry (*@*).

Incoming Virus-Infected Messages

Quarantine all incoming messages infected with a virus for two days and send a message to the intended recipients asking them to contact the administrator for a clean copy.

Create a new scenario

1. Select the *Scenarios/Incoming* folder.

   The route for this folder, set up during installation, is from any sender (*@*) to any recipient at your domain (**@example.com*). To see the route, right-click the folder in the console tree, then click **Properties**.

Figure 7-7: Folders

2. Right-click the *Scenarios/Incoming* folder, point to **New**, then **Scenario**, then click **Virus Manager**.
3. In the wizard, retain the default settings that specify the scenario is enabled and overridable and that it is to apply to all formats (**Always**).
4. Specify details of your anti-virus software.
5. Choose whether infected messages are to be cleaned.
6. Associate the scenario with the classification *Dirty In*.

On completion, the new scenario is listed in the *Scenarios/Incoming* folder.

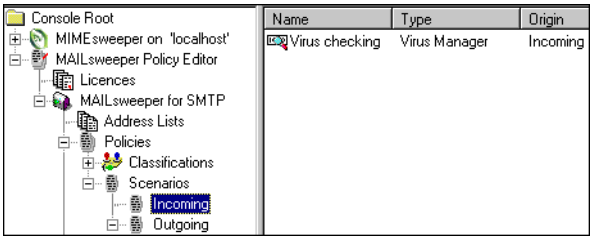


Figure 7-8: New Scenario

Create a new quarantine action

Create this action in the *Dirty In* classification folder.

1. Right-click the *Classifications/Dirty In* folder, point to **New**, then **Action**, then click **Quarantine**.

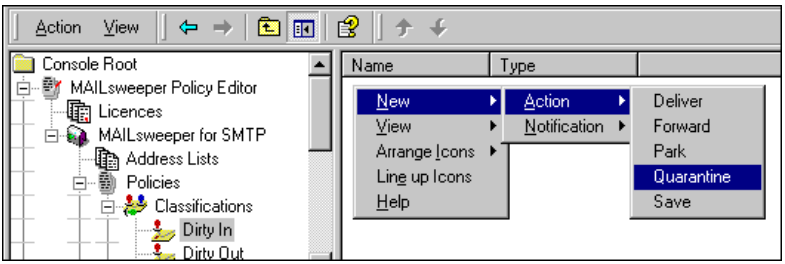


Figure 7-9: Classifications

2. In the wizard, specify that messages are to be placed in the *Dirty Messages* quarantine area.
3. Open the *Message Areas* folder and in the details pane, double-click **Dirty Messages**.
4. On the **Delete** tab, check that the area is set to delete messages automatically after two days.

Figure 7-10: Delete Messages

Create a new inform notification

Inform notifications are email messages used to inform recipients of actions taken on messages. To create an inform notification:

1. Right-click the *Dirty In* classification, point to **New,** then **Notification**, then click **Inform**.
2. Use the `%RCPTS%` token to specify that the inform notification is to be sent to all intended recipients of the original message.

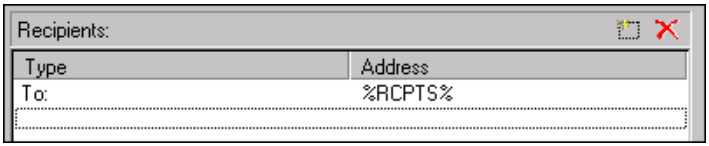


Figure 7-11: Recipient Addresses

3. Give the inform message a subject and some suitable body text.

Figure 7-12: Message

On completion, the newly-created action and notification are listed in the *Dirty In* folder, in the order in which they were created.

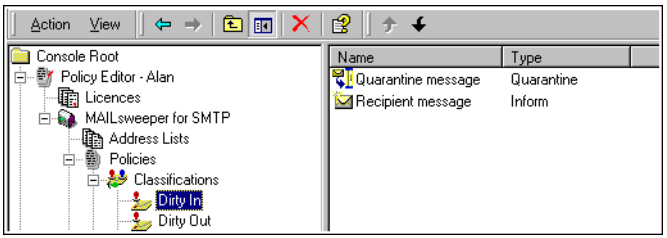


Figure 7-13: Ordering

Select an entry and click the arrows displayed above the details pane to change the order.

Outgoing Virus-Infected Messages

All outgoing messages infected with a virus will be destroyed and the sender notified, with instructions to clean their machine before sending any more mail.

Create a new scenario

1. Select the *Scenarios/Outgoing* folder.

   The route for this folder, set up during installation, is from any sender at your company (**@example.com*) to any recipient (**@**).

Figure 7-14: Outgoing Folder

2. Create a new *Virus Manager* scenario, as described in the section on *Incoming Virus-Infected Messages*. Associate the scenario with the classification *Dirty Out*.

   On completion, the new scenario is listed in the *Scenarios/Outgoing* folder.

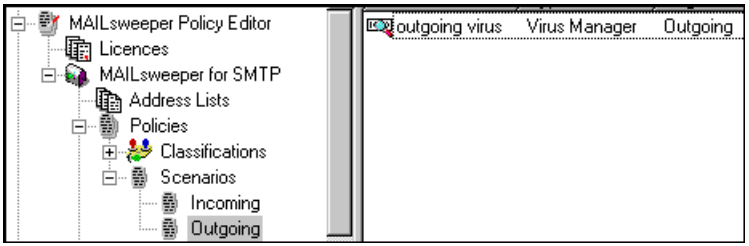


Figure 7-15: New Scenario

Create a new inform notification

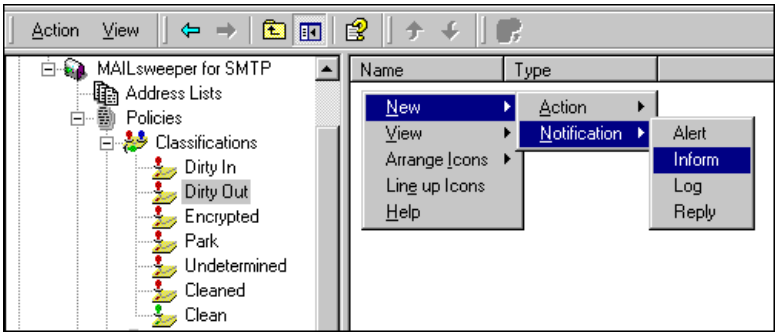


Figure 7-16: Classifications

1. Right-click the *Dirty Out* classification, point to **New**, then **Notification**, then click **Inform**.

   Use the %SENDER% token to specify that the inform notification is to be sent to the sender of the original message.

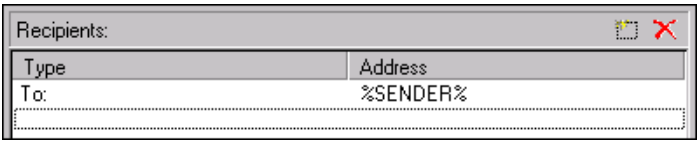


Figure 7-17: Sender Address

2. Give the inform message a subject and suitable body text.

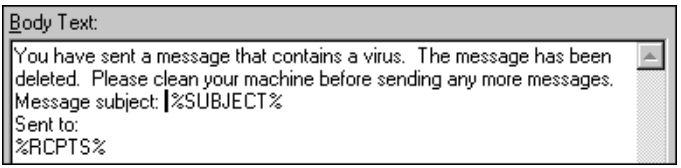


Figure 7-18: Message

On completion, the notification is listed in the *Dirty Out* folder.

Legal Disclaimer

Add legal disclaimers to the end of all outgoing messages.

Create a new scenario

1. Right-click the *Scenarios/Outgoing* folder, point to **New**, then **Scenario**, then click **Legal Disclaimer**.
2. Accept the default setting to make this scenario enabled and overridable.
3. Enter the text for the legal disclaimer and set the slider to **End of Message**.

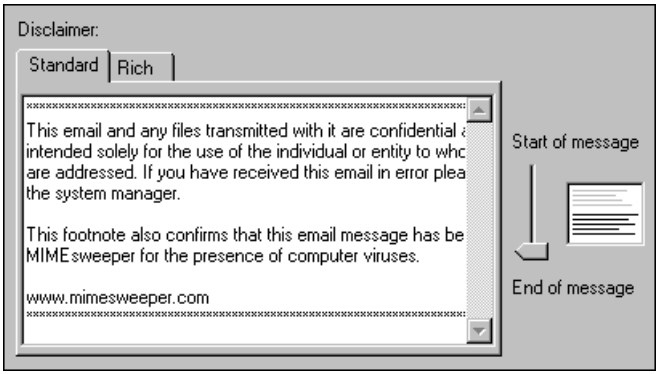


Figure 7-19: Legal Disclaimer

On completion, the scenario is listed in the *Scenarios/Outgoing* folder.

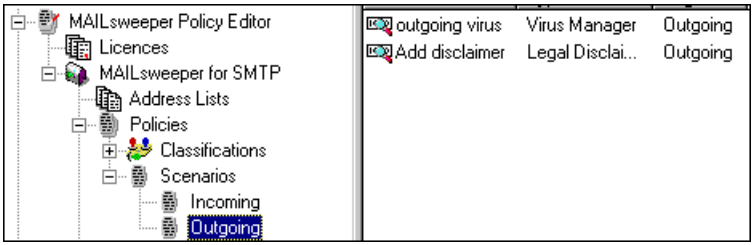


Figure 7-20: New Scenario

Large Messages

Park outgoing messages larger than 1MB between the hours of 9am and 6pm weekdays.

Create a new scenario

1. Right-click the *Scenarios/Outgoing* folder, point to **New**, then **Scenario**, then click **Size Manager**.
2. Accept the default setting to make this scenario enabled and overridable.
3. Set the smaller threshold to 1 MB. Do not set a larger threshold.

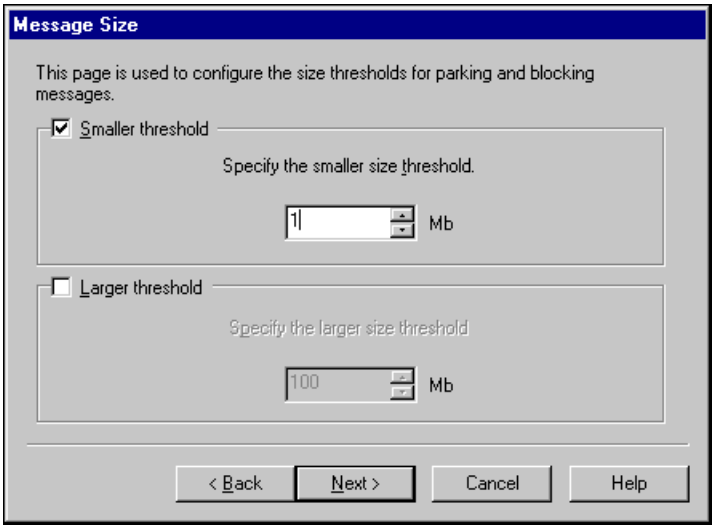


Figure 7-21: Sizes

4. Specify a schedule of 9am to 6pm weekdays, during which the size manager scenario will be active.

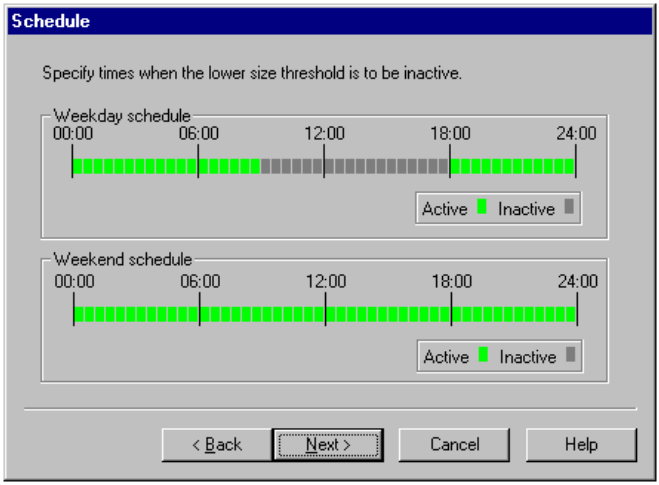


Figure 7-22: Time Schedule

5. Associate the scenario with the exclusive classification *Park* so that messages are held in the *Parked Messages* message area until released. To see the release schedule for this parking area, right-click the area in the details pane, then click **Properties**.

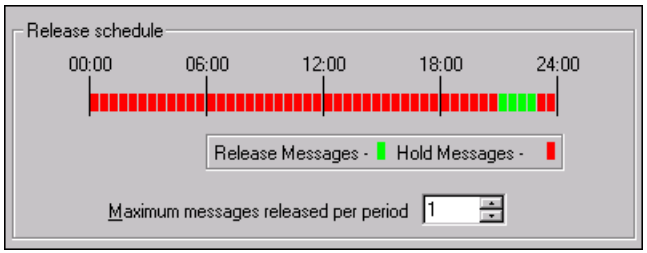


Figure 7-23: Release Schedule

On completion, the scenario is listed in the *Scenarios/Outgoing* folder, with the other configured scenarios.

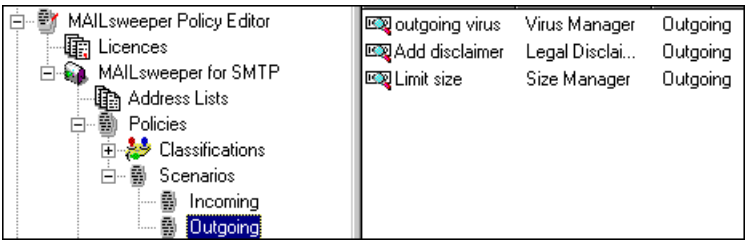


Figure 7-24: New Scenario

Confidential Material

If confidential material is detected in outgoing mail, send a message to the administrator and quarantine the message in a quarantine area with no automatic deletion. Exclude messages sent to partners from this rule.

Create a new quarantine area

1. Right-click the *Message Areas* folder, point to **New**, then click **Quarantine Area**.
2. Give the area the name *Confidential Messages.* This area will be used to hold suspect messages.
3. Give *Full Control* access to the user who is to have responsibility for this area. Do not set automatic deletion.

Figure 7-25: No Delete

Create a new exclusive classification

This classification will determine the actions taken and notifications sent for messages suspected of containing confidential material.

1. Right-click the *Classifications* folder, point to **New**, then click **Classification**.

2. In the wizard, ensure the **Exclusive** box is selected.
3. Give the classification the name *Confidential*.
4. When the classification has been created, it is placed above the *Clean* classification in the priority list. Select it and click the displayed up arrow to move it to above *Encrypted*.

   This means that if, in addition to the scenario that checks for confidential material, a message is processed by a scenario that is linked to an exclusive classification further down the list, the action and notification specified in the *Confidential* classification are applied to the message rather than those in the lower-priority classification.

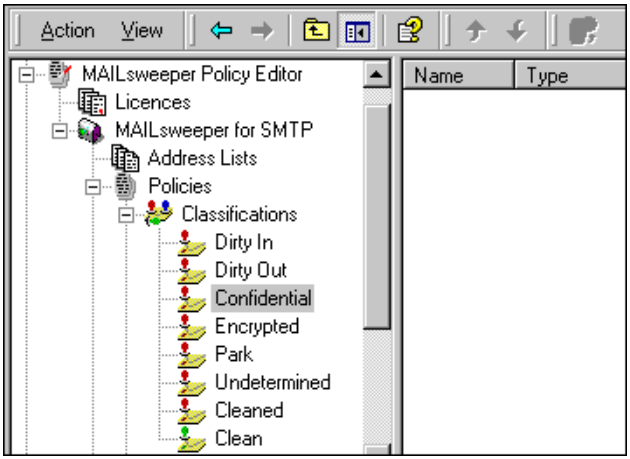


Figure 7-26: Classification Priorities

Create a new quarantine action

1. Right-click the *Confidential* classification, point to **New**, then **Action**, then click **Quarantine**.
2. In the wizard, choose the new *Confidential Messages* quarantine area.

Figure 7-27: Quarantine Areas

Create an inform notification

This notification is to inform the administrator of the action taken.

1. Right-click the *Confidential* classification, point to **New**, then **Notification**, then click **Inform**.
2. In the wizard, use the `%ADMIN%` token to specify that the notification is to be sent to the administrator.

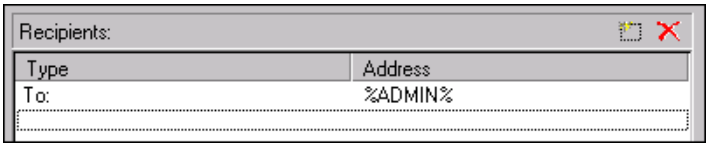


Figure 7-28: Administrator Addresses

3. Give the inform message a subject and suitable body text.

On completion, the newly-created action and notification are listed in the *Confidential* folder, in the order in which they were created.

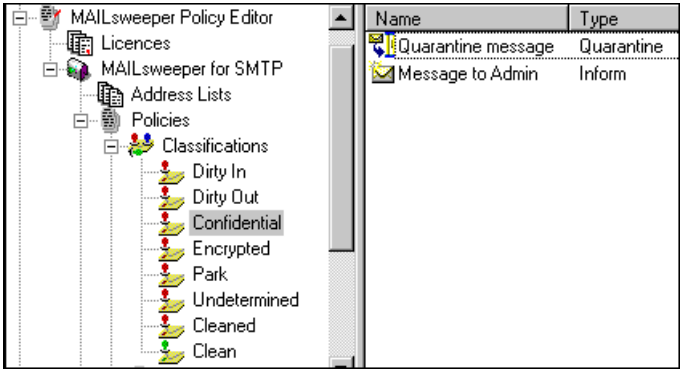


Figure 7-29: Actions and Notifications

Create a new scenario

1. Right-click the *Scenarios/Outgoing* folder, point to **New**, then **Scenario**, then click **Text Analyzer**.
2. Accept the default setting to make this scenario enabled and overridable.
3. Enter the confidential expressions you want to block, and their considered numeric weightings.

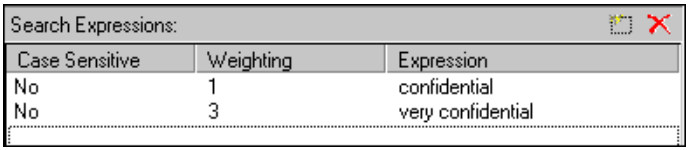


Figure 7-30: Expressions

4. Associate the scenario with the exclusive classification *Confidential*.

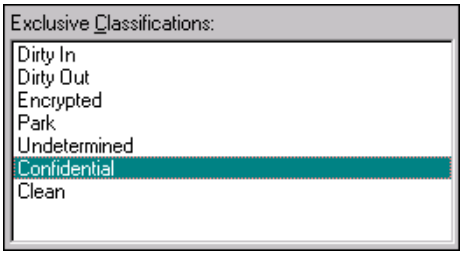


Figure 7-31: Classifications

5. Call the scenario *Block confidential*.

On completion, the newly-created scenario is listed in the *Scenarios/Outgoing* folder, with the other configured scenarios.

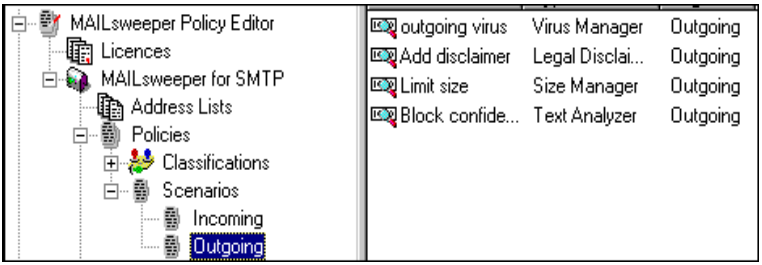


Figure 7-32: Configured Scenarios

Create a new scenario folder

This folder is for outgoing messages to your partners.

1. Right-click the *Scenarios/Outgoing* folder, point to **New**, then click **Folder**.
2. In the **Routes** page of the wizard, select the (*Example Exports Ltd*) address list as the sender and the (*Partners*) address list as the recipient.

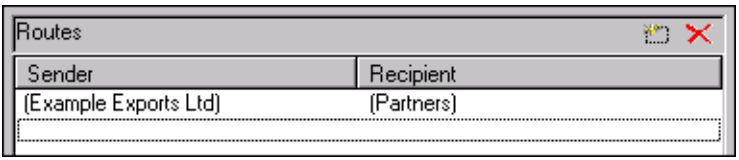


Figure 7-33: Address Lists

3. Name the folder *To Partners*.

Figure 7-34: To Partners Folder

The *To Partners* folder inherits all the scenarios set up by its parent folders; in this case the *Scenarios/Outgoing* folder, as indicated in the **Origin** field.

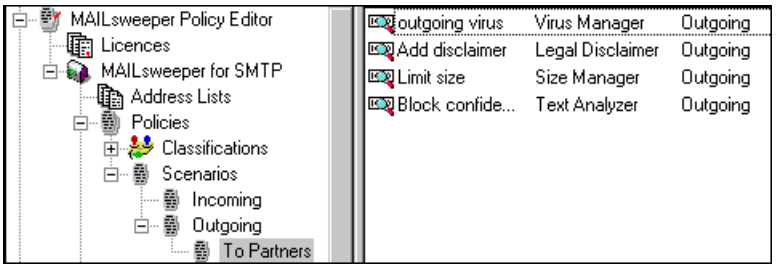


Figure 7-35: Inherited Scenarios

Set the states of the scenarios

Confidential material can be sent to partners, so the *Block confidential* scenario must be deactivated in the *To Partners* folder.

1. In the details pane, right-click the *Block confidential* scenario, and click **Active**. This clears the check mark next to **Active**, and changes the state of the scenario to Inactive.

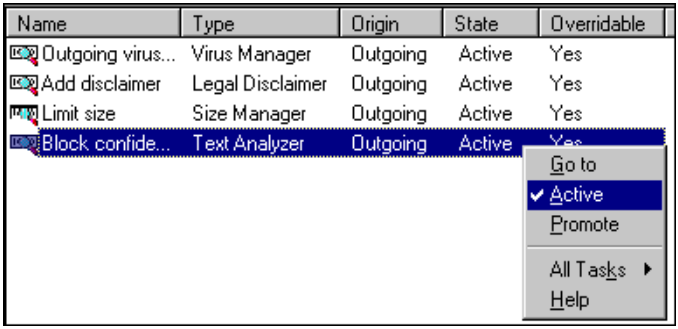


Figure 7-36: Active State

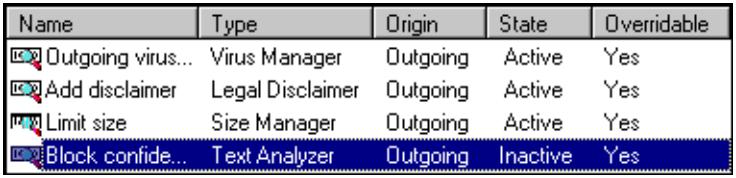


Figure 7-37: Inactive State

Prohibited Messages

Forward to the administrator any message addressed to a rival, and destroy the message.

Create a new scenario folder

1. Right-click the *Scenarios* folder, point to **New**, then click **Folder**.
2. In the **Routes** page of the wizard, select the (*Example Exports Ltd*) address list as the sender and the (*Rivals*) address list as the recipient.

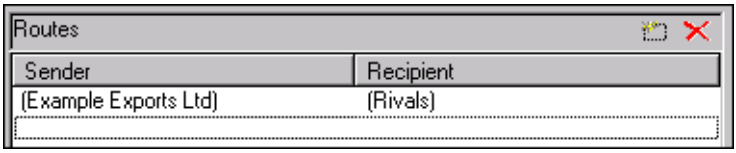


Figure 7-38: Message Route

3. Name the folder *To Rivals.*

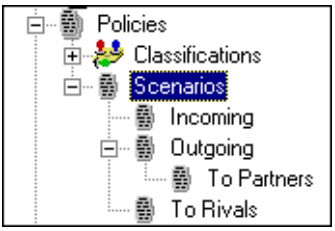


Figure 7-39: Folders

The *To Rivals* folder inherits all scenarios set up by its parent folders, in this case the *Scenarios* folder, as indicated in the **Origin** field. As the *Scenarios* folder is empty, there is no need to change the state of any inherited scenarios.

Create a new exclusive classification

This determines the actions and notifications for any message being sent to a rival.

1. Right-click the *Classifications* folder, point to **New**, then click **Classification**.
2. Make the classification exclusive, and call it *Forward*.
3. Use the arrows to move the classification to a position above the *Forward* classification, as shown in *Figure 7-40: Classification List.*

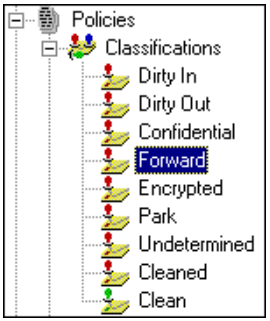


Figure 7-40: Classification List

Create a new action

This action is used to forward messages to the administrator.

1. Right-click the *Forward* classification, point to **New**, then **Action**, then click **Forward**.

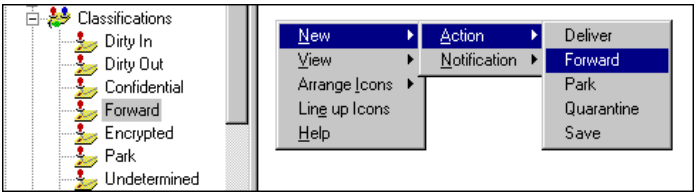


Figure 7-41: New Classification

2. Select *New* then *Action* then *Forward*.
3. In the wizard, use the `%ADMIN%` token to specify that messages are to be forwarded to the administrator.

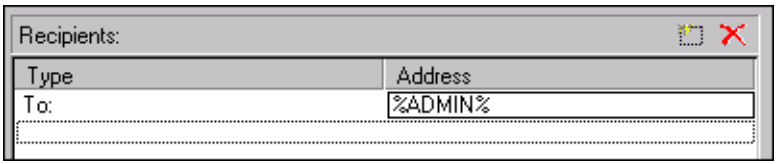


Figure 7-42: Admin Address

4. Give the notification message a subject and suitable body text. Ensure that messages are forwarded in their original state.

Figure 7-43: Message Forwarding

On completion, the action is listed in the *Forward* classification folder.

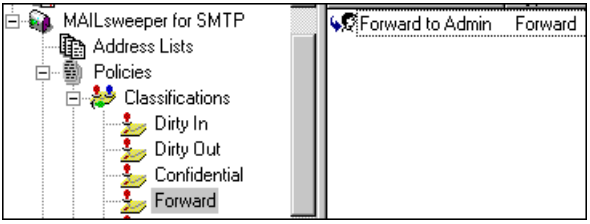


Figure 7-44: Classifications

Create a new scenario

The *Classifier* scenario blocks delivery of messages.

1. Right-click the *Scenarios/To Rivals* folder, point to **New**, then **Scenario**, then click **Classifier**. By default this scenario is enabled and overridable.
2. Associate the scenario with the classification *Forward*.

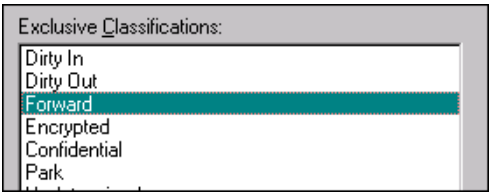


Figure 7-45: Forward Classification

On completion, the newly-created scenario is listed in the *Scenarios/To Rivals* folder.

Relay Prevention

Ban all mail arriving at MAILsweeper that is not destined for your local domain or from your local gateway.

1. Right-click the *Policies* folder and select **Properties**.
2. Ensure your gateway address is specified on the **Relay Host** tab.

   If you specified the IP address or TCP/IP host name of your gateway during installation, this is already entered on the **Relay Host** tab.

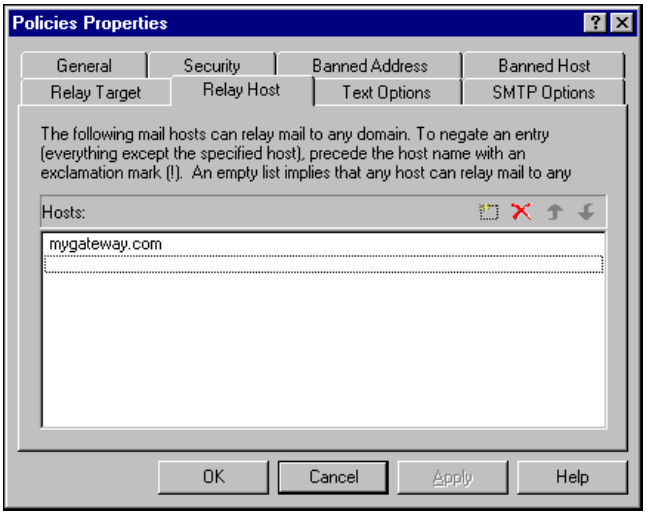


Figure 7-46: Relay Host Example