User's Guide

WebShield SMTP

McAfee
Network Security & Management

2805 Bowers Avenue
Santa Clara, CA 95051-0963

Phone: (408) 988-3832
Monday - Friday
6:00 A.M. - 6:00 P.M.

FAX: (408) 970-9727
BBS: (408) 988-4004

FEEDBACK

McAfee appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligations whatsoever. Please address your documentation feedback to: McAfee Associates, Inc., Documentation, 2805 Bowers Avenue, Santa Clara, CA 95051-0963, send e-mail to documentation@cc.mcafee.com, or send a fax to McAfee Documentation at (408) 970-9727.

Issued October 1997 / WebShield SMTP v3.0.0

Table of Contents

1 Introducing WebShield SMTP

What is WebShield SMTP?

WebShield SMTP is a comprehensive anti-virus solution for the Internet gateway. WebShield SMTP scans and cleans all inbound and outbound Internet e-mail and e-mail attachments for viruses, protecting your network from harmful infections. Using the Java™ -based Administration Console, you can remotely configure and maintain WebShield SMTP from a designated trusted machine.

WebShield SMTP is an important element of a comprehensive security program that includes a variety of safety measures, such as regular backups, meaningful password protection, training, and awareness. We urge you to set up and comply with such a security program as a preventive measure to protect against infection.

Why use WebShield SMTP?

Electronic mail is to date the most well known mechanism to transfer viruses, mainly because of the Word macro viruses found in document attachments. An e-mail message, addressed to multiple recipients with an attached Word macro virus has the ability to travel, undetected, through firewalls and server anti-virus scanners. Viruses have even been discovered that can propagate by mailing themselves. Until now, the only defense against these viruses was powerful virus detection at the desktop to prevent infected attachments from infecting the desktop system.

WebShield SMTP scans all SMTP e-mail at the server. It detects, cleans, logs, and quarantines infected file attachments. As a result, these tasks are handled at the point of entry before the virus proliferates to individual mail recipients.

Main features

- Scans electronic mail attachments at the SMTP mail gateway
- Can be configured for an automated response upon virus detection including notification, logging, deletion, isolation, or cleaning.
- Transparently operates on the network and requires very little user intervention.
- Offers secure remote management through an intuitive Java-based interface.

  ✍ *The WebShield SMTP user interface requires that the Java Runtime Environment (JRE) be installed. See Chapter 2, "Installing WebShield SMTP," for more information.*

- Offers a quarantine option for infected messages and attachments.
- Implemented as a Windows NT Service.

How to Contact McAfee

Customer Service

To order products or obtain product information, we invite you to contact our Customer Care department at (408) 988-3832, or at the following address:

McAfee Associates, Inc.
2805 Bowers Avenue
Santa Clara, CA 95051-0963
U.S.A.

Technical Support

McAfee is famous for its dedication to customer satisfaction. We have continued this tradition by making our website a valuable resource for answers to technical support questions. We encourage you to make this your first stop for answers to frequently asked questions, for updates to McAfee software, and for access to McAfee news and virus information.

World Wide Web	http://www.mcafee.com

If you do not find what you need or do not have web access, try one of our automated services.

Automated Voice and Fax Response System	(408) 988-3034
Internet	support@mcafee.com
McAfee BBS	(408) 988-4004
	1200 bps to 28,800 bps
	8 bits, no parity, 1 stop bit
	24 hours, 365 days a year
CompuServe	GO MCAFEE

America Online	keyword MCAFEE

If the automated services did not have the answers you need, contact McAfee technical support Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

For corporate-licensed customers:

Phone	(408) 988-3832
Fax	(408) 970-9727

For retail-licensed customers:

Phone	(972) 278-6100
Fax	(408) 970-9727

To provide the answers you need quickly and efficiently, the McAfee technical support staff needs some information about your computer and your software. Please have this information ready before you call:

- Product name and version number
- Computer brand, model, and any additional hardware
- Operating system type and version
- Network cards installed
- Contents of your WSHIELD.CFG
- Specific steps to reproduce the problem

International Contact Information

To contact McAfee outside the United States, use the addresses and numbers below.

McAfee Canada

139 Main Street, Suite 201

Unionville, Ontario

L3R 2G6 CANADA

Phone: (905) 479-4189

Fax: (905) 479-4540

McAfee Europe B.V.

Gatwickstraat 25

1043 GL Amsterdam

THE NETHERLANDS

Phone: 31 20 586 6100

Fax: 31 20 586 6101

McAfee France

50 rue de Londres

75008 Paris

FRANCE

Phone: 33 1 44 90 87 37

Fax: 33 1 45 22 75 54

McAfee GmbH

Industriestrasse 1

82110 Germering

GERMANY

Phone: 49 89 894 356-0

Fax: 49 89 894 356-99

McAfee UK

Hayley House
London Road

Bracknell

RG12 2TH

UNITED KINGDOM

Phone: 44 1344 304 730

Fax: 44 1344 306 902

McAfee Japan KK

4F Toranomon Mori
Bldg. 33

3-8-21 Toranomon

Minato-Ku, Tokyo 105

JAPAN

Phone: 81 3 3435 8246

Fax: 81 3 3435 1349

2 Installing WebShield SMTP

Before You Start

Before you install WebShield SMTP, be sure you are logged on to your Windows NT network with Administrator rights.

✍ *It is recommended that this product be installed by a Mail Administrator.*

Review the basic requirements for installing WebShield SMTP. You must have:

- A Windows NT server version 3.51 or later for running the WebShield SMTP server component

  ✍ *McAfee recommends running WebShield SMTP on a NT server that is equivalent to your SMTP server, at least 64MB of memory.*

- A Windows NT server or workstation, version 4.0, for running the WebShield SMTP Administration Console

  ✍ *The WebShield SMTP Administration Console and the WebShield SMTP server component may be installed on the same machine.*

- At least 6MB of free disk space to install the WebShield SMTP program files. Additionally, WebShield SMTP requires temporary space on your hard drive for mail scanning

- Java Runtime Environment (JRE)

  ✍ *To run the Java-based Administration Console, download and install the Java Runtime Environment. You can obtain the Java Runtime Environment from http://www.Javasoft.com/products/ .*

- McAfee recommends running the latest Microsoft Service Pack

Installation Procedure

To install WebShield SMTP, follow these steps:

Step	Action

1. Log on to the Windows NT SMTP server. You must have Administrator security rights to the Windows NT domain or local machine.

2. Do one of the following:

   - If installing from diskette or compact disc, insert it into your floppy disk drive or CD-ROM drive.

   - If installing from files downloaded from a BBS or the McAfee Web Site, decompress the zipped files into a directory on the network or your local drive.

3. Double-click the SETUP.EXE program in File Manager or run one of the following commands from the Windows NT command line:

   - If installing from compact disc, type:

     `x:\SETUP`

     where x is the drive that contains the CD-ROM.

   - If installing from downloaded files, type:

     `x:\path\setup.exe`

     where *x:\path* is the location of the files (for example, C:\DOWNLOAD\SETUP.EXE). Click OK.

Response: The WebShield SMTP License Agreement screen appears. Read it carefully before proceeding with the installation.

4. Click Yes to begin the installation, if you agree to the terms of the license.

   Response: The WebShield SMTP Welcome screen appears.

5. Click Next.

   Response: The Setup Type screen appears.

6. Select the destination directory for the WebShield SMTP program files.

7. Select the type of installation:

   - To install all WebShield SMTP options including the Console and Alert Manager, select Typical and click Next.
   - To configure WebShield SMTP to use the fewest resources, select Compact and click Next.

     ✍ *This option installs the Administration Console only. Select this option when installing the remote configuration capabilities.*

   - To perform a custom installation, select Custom and click Next. Select components to install and system options.

   Response: The Service Account Usage screen appears. Review the information provided and click Next to continue.

8. From the Service Account Information screen, do the following:

   Specify the type of account by selecting Use System Account or Use Custom Account.

   ✍ *Use Custom Account is the default account.*

   Enter a user name with Administrator rights and the appropriate password. Click Next.

   ✍ *Do not use a password that will expire.*

   Response: The Confirm Installation Settings screen appears.

9. Confirm the installation options are correct and click Next.

   Response: WebShield SMTP files are copied to the server.

10. It is strongly recommended you read the WebShield SMTP README.1ST and WHATSNEW.TXT files. These files contain important last-minute and licensing information. Click Finish.

    Response: WebShield SMTP is installed.

11. Configure your SMTP environment to transfer mail through WebShield SMTP. For detailed instructions, see "Post installation configuration" on page 14.

When installation concludes, McAfee WebShield SMTP Mail Configuration, Scan Services, and Alert Manager are started automatically.

✍ *You can verify that these components are enabled by double-clicking the Services icon in the Control Panel.*

Post installation configuration

To scan all SMTP traffic, WebShield SMTP must be positioned to receive all incoming and outgoing mail. If WebShield SMTP is installed on a machine separate from your SMTP mail server, see "Multiple server configuration" below. If WebShield SMTP and the SMTP server are running on the same machine, see "Single server configuration" on page 16.

Multiple server configuration

Figure 2-1 shows a multiple server environment where WebShield SMTP is installed on a machine other than the SMTP mail server.

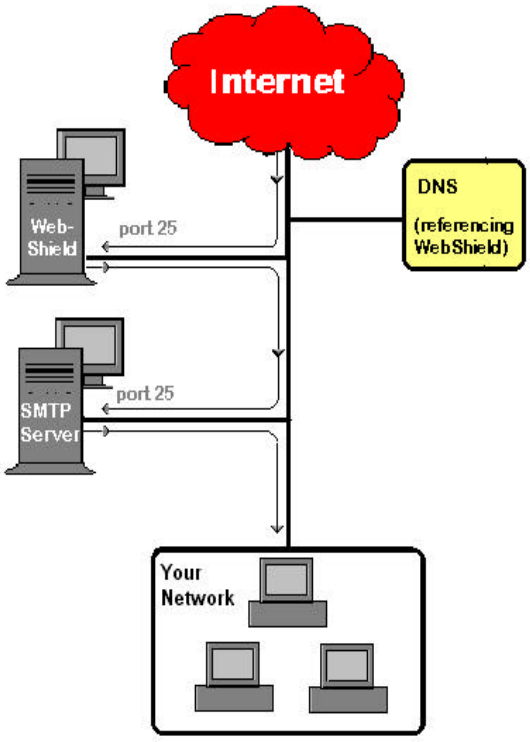

Figure 2-1. Multiple Server Environment

If your SMTP mail environment resembles the environment displayed in Figure 2-1, you must modify your Domain Name Server (DNS) to forward e-mail messages to the WebShield SMTP server before they are sent to your SMTP server. Follow the steps below to modify your local DNS:

Step	Action
1.	Edit your local DNS table to substitute WebShield SMTP for your existing mail server.
2.	Locate the Mail Exchanger (MX) resource record entry used by your existing SMTP mail server.
3.	Change this record by substituting the fully qualified domain name (such as webshield.mcafee.com) of the host where WebShield SMTP is installed.

Example

Name	Type	Data
mail.mcafee.com	MX	webshield.mcafee.com

In the above example, all incoming and outgoing mail intended for the host, mail.mcafee.com, will be forwarded through webshield.mcafee.com

✍ *The procedure to modify your DNS will vary depending upon your network environment.*

Single server configuration

Figure 2-2 shows a single server configuration environment where WebShield SMTP and the SMTP server are running on the same machine.

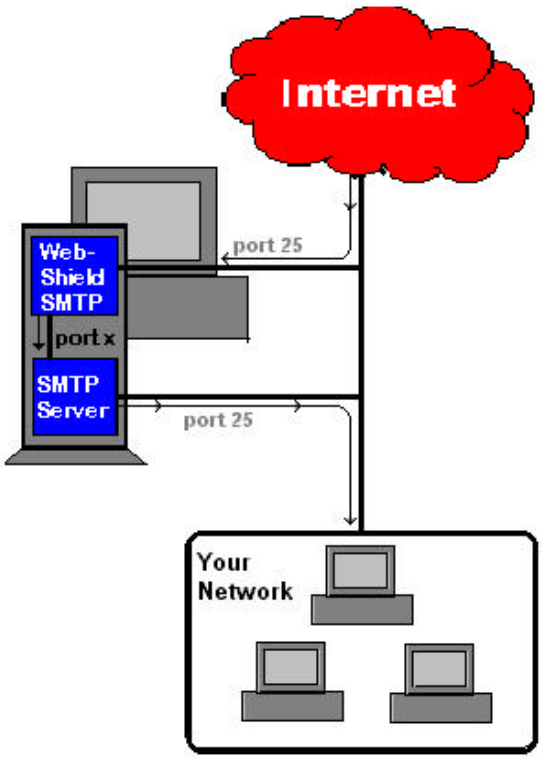

Figure 2-2. Single System Environment

If your SMTP mail environment resembles the environment displayed in Figure 2-2, you must modify ports in WebShield SMTP and your SMTP server. To modify the ports, do the following:

Step	Action
1.	Start the Administration Console. See “Starting the Administration Console” on page 18 for instructions on starting the console.

2. Open the Configuration property page and change the send-port within WebShield SMTP to any available port other than 25.

3. Modify the incoming mail-port for your SMTP mail server to be consistent with WebShield's send-port number.

   ✍ *The procedure to modify your SMTP mail server ports will vary according to your mail server software.*

Registering additional trusted clients

You can configure the WebShield SMTP server from any machine within your network. To remotely configure the WebShield SMTP servers, you must register the remote computer as a trusted machine by adding it to the WebShield SMTP Server List. To do this, follow the instructions below from the WebShield SMTP server.

Step **Action**

1. Do one of the following:

   - For Windows NT 3.51, choose File/Run and type `REGEDIT`.
   - For Windows NT 4.0, choose Start/Run and type `REGEDIT`.

   Response: The Windows Registry Editor appears.

2. Go to HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\WebShield SMTP\Mail Config.

3. Modify the Allowed_Clients "localhost" key to add additional trusted hosts.

   Example: Allowed_Clients "localhost1, localhost2, localhost3"

4. Choose Exit from the Registry menu when complete.

3 Using WebShield SMTP

Starting the Administration Console

After installation, all WebShield SMTP configuration and management is controlled through the WebShield Administration Console. This chapter outlines the options that are available using the Administration Console and details the steps to take to configure your software.

The WebShield Administration Console can be opened on the machine where WebShield SMTP is installed or on a remote machine.

✍ *To run the Administration Console from a remote machine, you must register your computer as a trusted machine. For instructions see* *"Registering additional trusted clients" on page 17**.*

To start the Administration Console, click Start, point to Programs, point to McAfee WebShield SMTP, and click Webshield SMTP Console.

✍ *The Java Runtime Environment is not yet available for Windows NT 3.51 systems. Windows NT 3.51 systems running WebShield SMTP may not be able to run the Administration Console. Refer to the JRE documentation for more information.*

Response: The Administration Console is displayed (Figure 3-1).

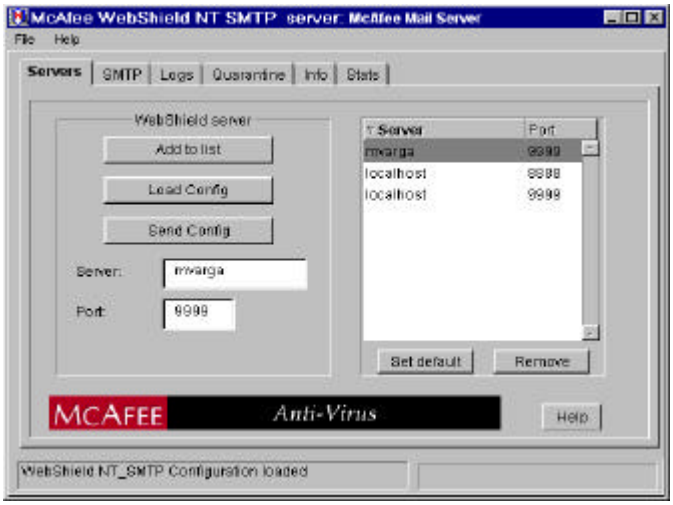

Figure 3-1. WebShield SMTP Administration Console (Servers property page)

Using the Administrative Console

From the WebShield Administration Console (Figure 3-1), you can select menu items for configuration and management. Use the property pages to customize, manage, and maintain all aspects of WebShield. The property pages include:

- **Servers.** Use this page to add or remove servers from the WebShield SMTP configuration. To perform these actions, see "Using the Servers Property Page" on page 21.

- **SMTP.** Use this page to customize your virus scanning and action options, port configuration, and address exclusion list. To customize these settings, see "Using the SMTP Property Page" on page 23.

- **Logs.** Use this page to enable mail and virus logging and configure log rotation and removal settings. To configure log settings, see "Using the Logs Property Page" on page 29.

- **Quarantine.** Use this page to enable the Quarantine option, allowing infected files to be detained and disabled in a separate folder for observation. To enable the Quarantine option, see "Using the Quarantine Property Page" on page 32.

- **Info.** Use this page to display information about the server, version of scan engine, and Virus Definition (DAT) files. To review the data, see "Displaying WebShield SMTP Information" on page 34.

- **Stats.** Use this page to display statistics on incoming and outgoing mail, as well as, statistics on infected and clean mail. To review Webshield SMTP statistics, see "Displaying Mail and Virus Statistics" on page 35.

Using the Servers Property Page

To use the WebShield SMTP Servers property page (Figure 3-1), start the Administration Console and click Servers.

From this page, you can:

- Load and send Webshield SMTP configuration settings
- Add WebShield servers to WebShield SMTP
- Remove WebShield servers from the WebShield SMTP configuration
- Set a default WebShield server

Loading and sending WebShield SMTP configurations

To view and modify specific WebShield SMTP server configurations, follow the instructions below.

Step	Action
1.	Select a server in the WebShield List and click Load Config to retrieve the WebShield SMTP configuration for the selected server. **Response**: The specified server's WebShield SMTP configuration settings are loaded and displayed in the console.
2.	Modify the configuration settings by using the tabbed property pages.
3.	Return to the Servers property page and click Send Config to update other WebShield SMTP servers with the new configuration settings.

Adding a WebShield server

To add a WebShield server to the Administration Console, use the Servers property page (Figure 3-1) and follow the instructions below.

Step	Action
1.	Enter the new WebShield SMTP server name and port number in the text boxes provided.
2.	Click Add to List. **Response**: The WebShield SMTP server and port number are displayed in the WebShield list.

Removing a WebShield server

To remove a WebShield SMTP server from the Administration Console, use the Servers property page (Figure 3-1) and follow the instructions below.

Step	Action
1.	Select the WebShield SMTP server you want to remove by selecting the WebShield name in the WebShield SMTP list.
2.	Click Remove. **Response**: The WebShield server and port number are removed from the WebShield SMTP list.

Setting a default WebShield server

You can set a default WebShield SMTP server if there are multiple WebShield SMTP servers. Select a WebShield server in the WebShield list and click Set Default. Click Send Config for the changes to take effect.

Using the SMTP Property Page

Use the WebShield SMTP property page (Figure 3-2) to customize WebShield's scanning options and protect the network from virus infected e-mail messages and file attachments.

Step **Action**

1. At the Administrative Console click the SMTP tab.

Response: The WebShield SMTP property page is displayed with the Scan tab on top (Figure 3-2).

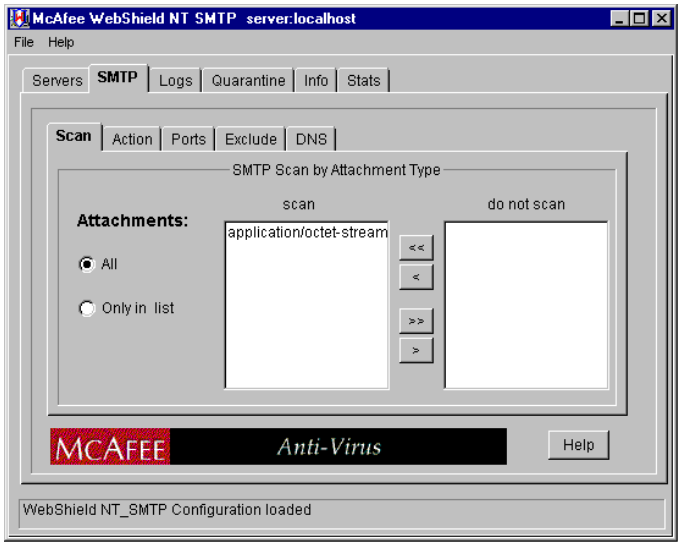

Figure 3-2. WebShield SMTP Administration Console (SMTP Scan tab)

2. Do one of the following:

- To scan all file attachments passing through the SMTP server, select the All option.

- To scan only specific file attachments passing through the SMTP server, select the Only In List option. Select all of the file attachments you want WebShield SMTP to scan. The options are listed below.
  - **Application**. Select this option to scan all application types.
  - **Application/octet-stream**. Select this option to only scan octet-stream applications.
  - **Text**. Select this option to scan all text files.
  - **Text/HTML**. Select this option to scan only HTML text files.
  - **Text/Plain**. Select this option to scan only plain text files.
  - **Text/Enriched**. Select this option to scan only enriched text files.

To move specific file types between the Scan and Do Not Scan lists, select the file type and use the arrow buttons provided.

3. Click the Action tab to configure how you want WebShield SMTP to respond to infected e-mail attachments and scan errors.

Response: The SMTP Action tab (Figure 3-3) is displayed.

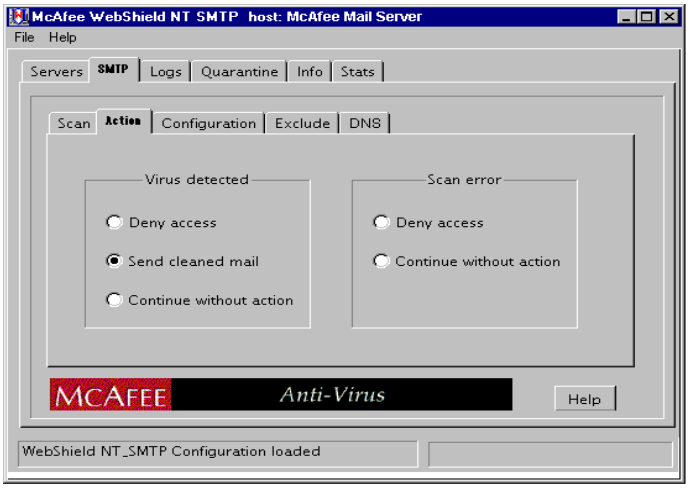

Figure 3-3. WebShield SMTP Administration Console (SMTP Action tab)

4. Specify what action you want WebShield SMTP to take when a virus is detected by selecting one of the following options:

   - **Deny Access**. Select this option if you want WebShield SMTP to intercept infected mail upon entering the mail server and withhold it from the recipient. The infected file is then quarantined and logged.

   - **Send Cleaned Mail.** Select this option if you want WebShield SMTP to quarantine, log, and clean infected mail, then forward to the intended recipient.

     ✍ *If WebShield SMTP cannot remove the virus, the infected file is deleted. WebShield SMTP replaces the file with a warning text file to forward to the intended recipient.*

   - **Continue Without Action.** Select this option if you want WebShield SMTP to only quarantine and log infected mail then send it (still infected) to the recipient.

   ✍ *Infected files will not be quarantined or logged unless these options are enabled. See "Using the Quarantine Property Page" on page 32, for more information about the Quarantine option and "Using the Logs Property Page" on page 29, for information about logging.*

5. Specify how you want WebShield SMTP to handle scan errors by selecting one of the following options:

   ✍ *Scan errors result when WebShield SMTP cannot scan a file due to file corruption, malformation, etc.*

   - **Deny Access.** Select this option if you want WebShield SMTP to intercept files that cannot be scanned upon entering the mail server and withhold it from the recipient. The scan error is then quarantined and logged.

   - **Continue Without Action.** Select this option if you want WebShield SMTP to log the error and send it (possibly infected) to the recipient.

6. Click the Configuration tab to specify the Read and Send ports.

Response: The SMTP Configuration tab is displayed (Figure 3-4).

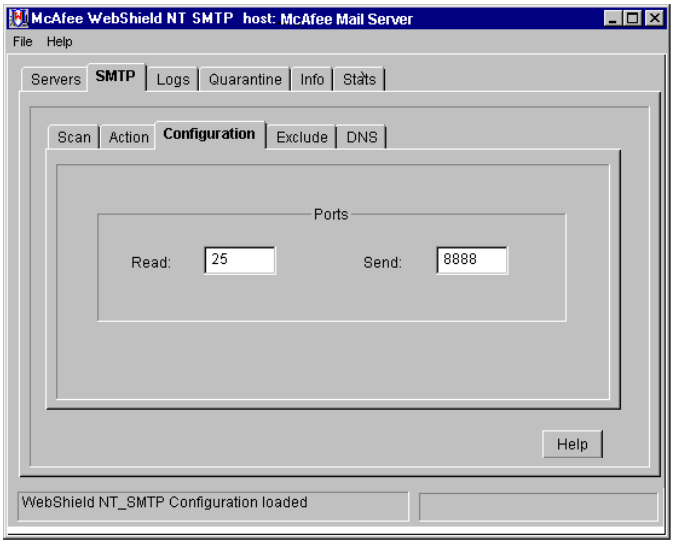

Figure 3-4. WebShield SMTP Administration Console (SMTP Configuration tab)

7. Enter the Read and Send port numbers in the text boxes provided.

✍ *The Read port number specifies the port that WebShield STMP uses for the incoming SMTP connection. The Send port number specifies the port that WebShield STMP uses for outgoing SMTP connections.*

8. Click the Exclude tab to specify addresses you want to exclude from cleaning.

Response: The SMTP Exclude tab is displayed (Figure 3-4).

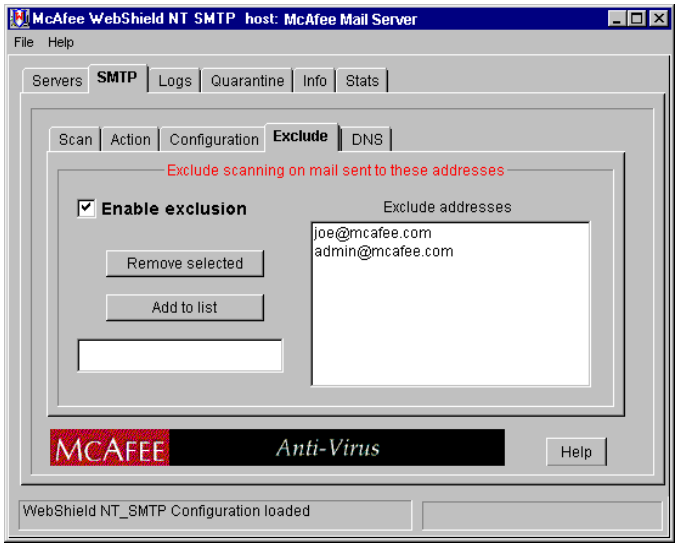

Figure 3-5. WebShield SMTP Administration Console (SMTP Exclude tab)

9. Select the Enable Exclusion checkbox if you want to exclude mail sent to certain addresses from cleaning.

✍ *If this checkbox is selected, all addresses in the Exclude Addresses list are excluded from cleaning.*

10. Enter the e-mail address you want to exclude from scanning in the text box provided. Click Add to List.

11. To re-enable cleaning of messages sent to an e-mail address, select the address and click Remove Selected.

12. Click the DNS tab to add and remove DNS addresses.

Response: The SMTP DNS tab is displayed (Figure 3-6)

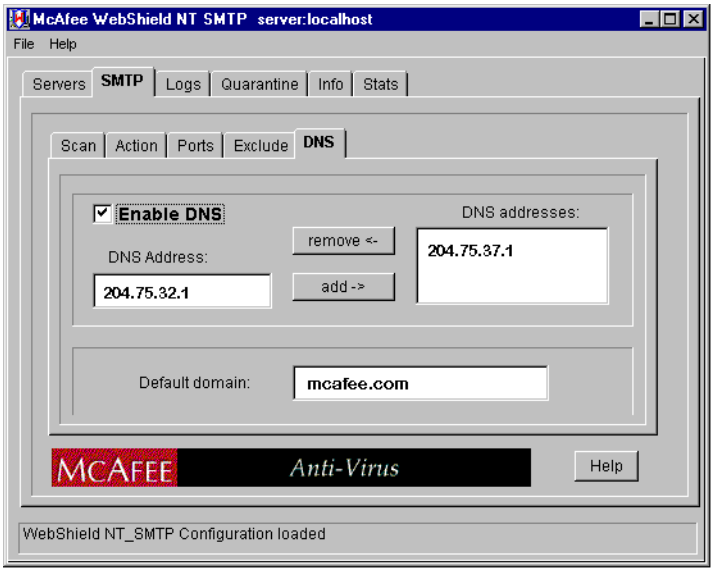

Figure 3-6. WebShield SMTP Administration Console (SMTP DNS tab)

13. Select the Enable DNS checkbox to allow WebShield SMTP to query the local domain name service to deliver remote mail (i.e., mail to internet recipients).

14. Enter the IP addresses of the system that provides domain name service for your network and click Add.

15. Enter your network domain name in the Default Domain field.

16. Click Send Config in the Servers property page for the changes to take effect or select another property page to further configure WebShield SMTP.

Using the Logs Property Page

Use this property page to enable Mail and Virus activity logging and to specify the interval for log rotation and log removal.

✍ *Changes to the Mail and Virus tab settings modify what information appears in the MAIL.LOG and VIRUS.LOG files. These log files will be created within the /log subdirectory of your WebShield installation directory. You can view these files to examine the network's mail and virus history.*

Step	Action

1. At the Administrative Console click Logs.

Response: The WebShield SMTP Logs property page is displayed with the Mail tab on top (Figure 3-7).

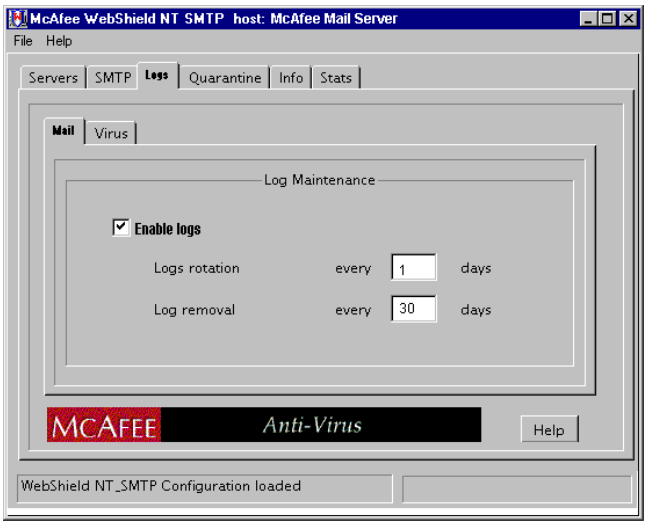

Figure 3-7. WebShield SMTP Administration Console (Mail Log tab)

2. Click the Mail tab to configure mail logging or click the Virus tab to enable virus logging.

3. Select the Enable Logs checkbox to activate logging services.

✍ *If this checkbox is clear, the log files will not be updated.*

When Mail logging is enabled, all mail passing through the WebShield mail server (incoming/outgoing) is logged in the MAIL.LOG file. The following information is noted in this logfile:

- Date and time of mail received
- Date and time of mail sent
- Sender and recipient's e-mail address
- Size of the message
- WebShield-assigned ID number

When Virus logging is enabled, all infected mail attachments passing though the server are logged in the VIRUS.LOG file. The following information is noted in this logfile:

- Date and time of mail received
- Date and time of mail sent
- Virus name
- Sender and recipient's e-mail address
- Partfile
- WebShield-assigned ID number
- WebShield action taken

4. Specify how many days you want to record into one log file until a new log file is generated. When the logfiles are rotated, an archived copy is created and renamed to the following:

   MAIL.LOG → MAIL<date>.LOG

   VIRUS.LOG → VIRUS <date>.LOG

   The MAIL.LOG and VIRUS.LOG files are cleared upon rotation.

   ✍ *These logs are automatically rotated when the Mail Scan service is manually restarted.*

5. Specify how many days you want between removal of the archived log files.

6. Return to the Servers tab and click Send Config.

Using the Quarantine Property Page

Use this property page to enable or disable the quarantine process and view quarantined files.

Step	Action
1.	At the Administrative Console click the Quarantine property page. **Response**: The WebShield SMTP Quarantine property page (Figure 3-8) is displayed.

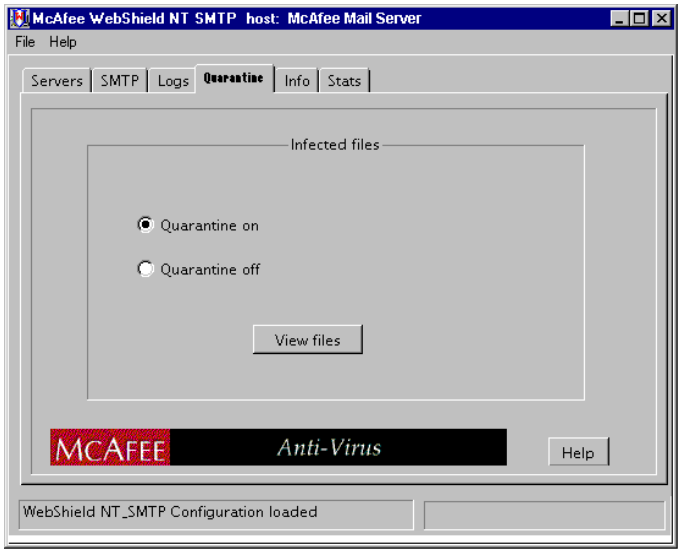

Figure 3-8. WebShield SMTP Administration Console (Quarantine property page)

2. Select the Quarantine On option. When this option is selected, all infected files detected by WebShield SMTP are automatically quarantined.

3. Return to the Servers tab and click Send Config.

Viewing a quarantined file

Administrators may find it necessary to examine e-mail messages to determine their origin. The Quarantine files will be created within the \quarantine subdirectory of your WebShield installation directory. To view the quarantined files, follow these steps:

Step	Action

1. At the Quarantine property page, click View Files.

Response: A list of quarantined files (Figure 3-9) is displayed.

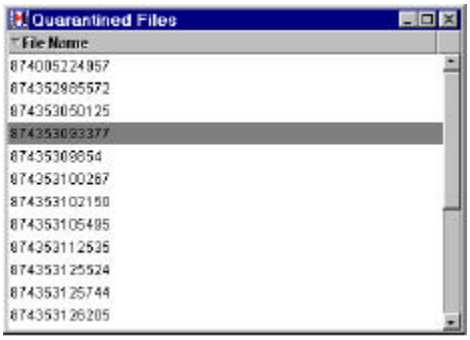

Figure 3-9. Quarantined Files List

2. The Quarantined Files are listed by the ID number assigned to the mail message.

✍ *The ID numbers are listed in the MAIL.LOG and VIRUS.LOG files located in WebShield's /log directory.*

To view a quarantined message, double-click its ID number.

Response: The message is displayed.

Displaying WebShield SMTP Information

Use the Info property page to verify version numbers of the scan engine and virus definition (DAT) files. Click Info in the Administration Console to view this information.

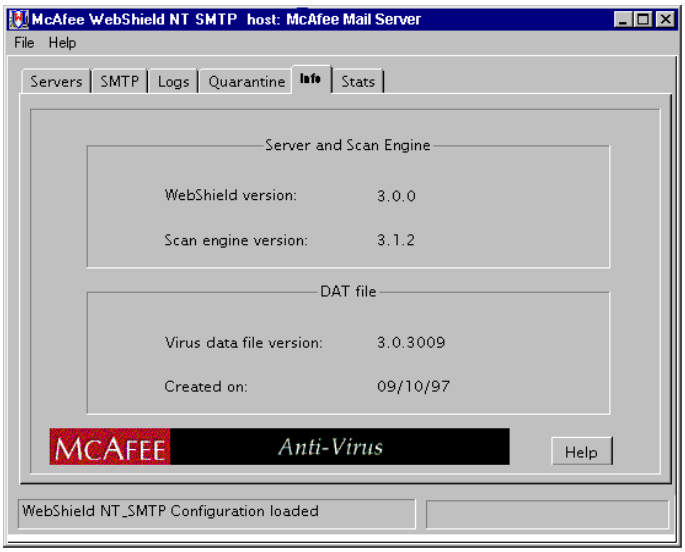

Figure 3-10. WebShield SMTP Administration Console (Info property page)

✍ *For information about upgrading and updating WebShield SMTP, see Appendix A, "Updating WebShield SMTP."*

Displaying Mail and Virus Statistics

Use the Stats property page (Figure 3-11) to view virus scanning statistics. The Stats property page displays an itemized report of scanned mail including: successfully scanned mail, infected mail, and cleaned mail. Use the Refresh button to retrieve a current report or select the Auto Refresh checkbox to automatically update the Stats report every five seconds.

Click Stats in the Administration Console to view this information (Figure 3-11).

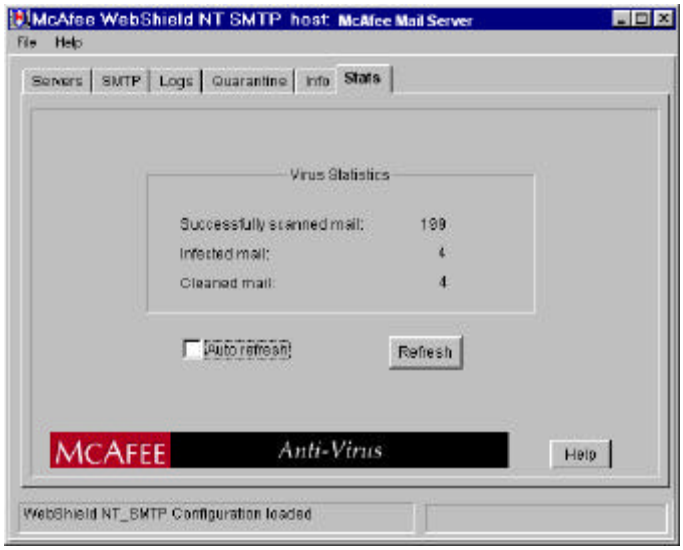

Figure 3-11. WebShield SMTP Administration Console (Statistics property page)

Shutting Down WebShield SMTP

WebShield SMTP is composed of three services: McAfee Mail Scan Service, McAfee Configuration Service; and McAfee Alert Manager Service. To shut down WebShield SMTP, all three services must be stopped. You can access these services by double-clicking the Services icon in the Control Panel. Click each WebShield SMTP service and select Stop.

4 Virus Notification

Using Alert Manager

In addition to automatically responding to infected mail attachments (cleaning, deleting, quarantining, etc.), WebShield SMTP can alert personnel in a variety of ways (pagers, printers, e-mail, fax, etc.).

WebShield SMTP supports the use of any combination of notification methods and multiples of each. Alerts can also be forwarded from one computer to another.

✍ *In large organizations, use alert forwarding to send alerts to centralized notification systems or to MIS departments to keep track of virus statistics and problem areas.*

To open the McAfee Alert Manager Properties window, do one of the following:

- For Windows NT 3.51: Open the McAfee WebShield SMTP program group in the Program Manager and select McAfee Alert Manager.
- For Windows NT 4.x: Click Start, point to Programs, point to McAfee WebShield SMTP, and click McAfee Alert Manager.

.

Figure 4-1. Alert Properties Window

Summary window

The Summary window lists all alert notification items configured on the other property pages.

- To view the properties of a notification item, highlight the item and click Properties.
- To delete a notification item, highlight the item and click Remove.

Forwarding alerts to another computer

WebShield SMTP can forward alerts to another computer. The computer receiving the forwarded message then sends alerts to recipients listed in the Summary window of its Alert Manager Properties window.

✍ *The McAfee Alert Manager Service must be running on both the SMTP server sending the Forward and the system receiving the forward.*

Step	Action
1.	Open the Alert Manager Properties window.
2.	Select the Forward tab. **Response**: The Forward window appears with a list of all systems configured to receive forwarded messages.
3.	To add a system to receive Forwards, click Add and specify a system or click Browse to locate the system.
4.	To test the forward, click Test. **Response**: The system receives a test message.
5.	To set the priority level of the messages this address receives, click Priority Alerts. ▪ To set the address to receive low, medium, and high priority alerts, select Low. ▪ To set the address to receive medium and high priority alerts, select Medium. ▪ To set the address to receive high priority alerts only, select High. ✍ *Configure High Priority items to be forwarded to multiple computers. This increases the number of alert notifications sent in an urgent situation and improves the chances of someone responding to the problem quickly.*

6. Click OK.

7. To add another computer to receive forwarded alerts, click Add.

8. To configure other notification options, select another property window. To save the changes and exit, click OK. To cancel any changes, click Cancel.

✍ *The WebShield SMTP Administration Console must be installed and running on the computer receiving forwarded messages.*

Sending a network message

The Alerts Manager supports the sending of network messages to specified computers. To send alert notifications via network messages, complete the following procedure:

✍ *To receive messages on Windows 95 machines, you must be running WinPopup.*

Step	Action

1. Open the Alert Manager Properties window.

2. Select the Network Message tab.

   Response: The Network Message window appears with a list of all systems configured to receive network messages.

3. To add a system to receive network message alert notifications, click Add.

4. Enter the computer to receive network messages or click Browse to locate the computer.

5. To test the connection, click Test.

   Response: The message recipient receives a test message.

6. To set the priority level of the messages this computer receives, click Priority Alerts.

   - To set the system to receive low, medium, and high priority alerts, select Low.
   - To set the system to receive medium and high priority alerts, select Medium.
   - To set the system to receive high priority alerts only, select High.

7. Click OK.

8. To add another system to receive network message alert notifications, click Add.

9. To configure other notification options, select another property window. To save the changes and exit, click OK. To cancel any changes, click Cancel.

Sending an alert to an e-mail address

The Alerts Manager supports the sending of e-mail messages. To send alert notifications via e-mail, complete the following procedure:

Step	Action

1. Open the Alert Manager Properties window.

2. Select the E-Mail tab.

   Response: The E-Mail window appears with a list of e-mail addresses configured to receive alert notifications.

3. To add an e-mail address, click Add.

   Enter an e-mail address. The format of the address is <user>@<domain> (e.g. johndoe@mcafee.com).

   Fill out the Subject line

   Fill out the From line.

   To configure SMTP settings, click Configure SMTP, enter the Domain name or IP address, Server name, and Login name.

4. To test the connection, click Test.

   Response: The message recipient receives a test message.

5. To set the priority level of the messages this e-mail address receives, click Priority Alerts.

   - To set the address to receive low, medium, and high priority alerts, select Low.
   - To set the address to receive medium and high priority alerts, select Medium.
   - To set the address to receive high priority alerts only, select High.

6. Click OK. To add another recipient to receive alert notifications, click Add.

7. To configure other notification options, select another property window. To save the changes and exit, click OK. To cancel any changes, click Cancel.

Sending an alert to a pager

The Alerts Manager supports the sending of alert notifications to alphanumeric and numeric pagers.

Alphanumeric pager

To send alert notifications to an alphanumeric pager, complete the following procedure:

Step	Action
1.	Open the Alert Manager Properties window.
2.	Select the pager tab. **Response**: The pager window appears with a list of all pagers configured to receive alert notifications.
3.	To add a pager, click Add.
4.	Select Alphanumeric pager.
5.	Enter the pager phone number, an ID or a PIN number (if applicable), and a password (if applicable).
6.	To use the standard alert message, click the Use Standard Alert Message option button. To use a custom message, click the Use Custom Alert Message option button and enter a message.
7.	Click Modem to configure the modem settings.
8.	To test the pager, click Test.

9. To set the priority level of alert notifications this pager receives, click Priority Alerts.

   - To set the address to receive low, medium, and high priority alerts, select Low.
   - To set the address to receive medium and high priority alerts, select Medium.
   - To set the address to receive high priority alerts only, select High.

10. Click OK.

11. To add another pager to receive notifications, click Add.

12. To configure other notification options, select another property window. To save the changes and exit, click OK. To cancel any changes, click Cancel.

Numeric pager

To send alert notifications to an numeric pager, complete the following procedure:

Step	Action

1. Open the Alert Manager Properties window.

2. Select the pager tab.

   Response: The pager window appears with a list of all pagers configured to receive alert notifications.

3. To add a pager, click Add.

4. Select Numeric pager.

5. Enter the pager phone number.

6. Enter a numeric message.

7. Enter the delay time between dialing and sending the alert message.

8. Click Modem to configure the modem settings.

9. To test the pager, click Test.

10. To set the priority level of alert notifications this pager receives, click Priority Alerts.

    - To set the address to receive low, medium, and high priority alerts, select Low.
    - To set the address to receive medium and high priority alerts, select Medium.
    - To set the address to receive high priority alerts only, select High.

11. Click OK.

12. To add another pager to receive notifications, click Add.

13. To configure other notification options, select another property window. To save the changes and exit, click OK. To cancel any changes, click Cancel.

Sending an alert to a printer

The Alerts Manager supports the sending of alert notifications to printers. To send alert notifications to printers, complete the following procedure:

Step **Action**

1. Open the Alert Manager Properties window.

2. Select the Printer tab.

   Response: The Printer window appears with a list of all systems currently configured to receive alert notifications.

3. To add a printer, click Add.

4. Enter a printer location or click Browse to locate the printer.

5. To test the connection, click Test.

   Response: The printer prints a test message.

6. To set the priority level of the messages this printer receives, click Priority Alerts.

   - To set the system to receive low, medium, and high priority alerts, select Low.
   - To set the system to receive medium and high priority alerts, select Medium.
   - To set the system to receive high priority alerts only, select High.

7. Click OK.

8. To add another printer to receive alert notifications, click Add.

9. To configure other notification options, select another property window. To save the changes and exit, click OK. To cancel any changes, click Cancel.

✍ *The printer must be configured by the Print Manager prior to configuring this notification option.*

Using SNMP

WebShield SMTP supports SNMP (Simple Network Management Protocol). To enable SNMP, complete the following procedure:

Step	Action
1.	Open the Alert Manager Properties window.
2.	Select the SNMP tab. **Response**: The SNMP window appears.
3.	Select the Enable SNMP checkbox.
4.	To configure SNMP services, click Configure. **Response**: The Microsoft NT Network Settings property window appears.
5.	To complete configuration of SNMP services, refer to the Windows NT documentation.
6.	To configure other notification options, select another property window. To save the changes and exit, click OK. To cancel any changes, click Cancel.

A Updating WebShield SMTP

Detecting New and Unknown Viruses

The best way for you to deal with new and unknown viruses that might affect your system is to update your WebShield SMTP virus definition (.DAT) files.

To offer the best virus protection possible, McAfee continually updates the definition files WebShield SMTP uses to detect viruses. For maximum protection, you should update these files on a regular basis.

✍ *The term "update" refers only to the virus definition files; the term "upgrade" refers to product version revisions, executables, and definition files. McAfee offers free online virus signature file updates (.DATs) for the life of your product. We cannot, however, guarantee backward compatibility of the signature files with previous versions' executable files. By upgrading your software to the latest product version and updating to the latest .DAT files regularly, you ensure complete virus protection for the term of your software subscription or maintenance plan.*

Why would I need a new data file?

New viruses appear at a rate of more than 200 per month. Often, older data files cannot assist WebShield SMTP in detecting these new variations. The data files that came with your copy of WebShield SMTP, for example, may not detect a virus that was discovered after you bought the product.

McAfee's virus researchers are working constantly to update these data files with more and better virus definitions. New data files are released monthly.

✍ *McAfee cannot guarantee that the WebShield SMTP .DAT files included with this release will work with previous WebShield SMTP versions.*

Updating your data files

You can use any of these methods to update your data files for WebShield SMTP:

- **Connect to the McAfee Web Site.** Start your favorite browser software, then go to http://www.mcafee.com to download the latest data files and read up-to-the-minute news.
- **Connect to McAfee's FTP server.** Open a connection to ftp.mcafee.com. Use anonymous as your user name and your e-mail address as your password to gain access. Look for WebShield SMTP .DAT files in the directory pub/anti-virus.
- **Connect to the McAfee Bulletin Board System (BBS).** Use your preferred communications software to dial (408) 988-4004.

To update your virus definition data (DAT) files, follow these steps:

Step	Action
1.	Create a new directory for the downloaded file.
2.	Download the file into the new directory.
3.	Decompress the WebShield SMTP data files. ✍ *If you do not have a software decompression utility, you can download one from McAfee's online services.*
4.	Copy the files into the McAfee WebShield SMTP directory. **Response:** The next time WebShield SMTP runs, it uses the new data files to scan for viruses.

Reporting new items for WebShield SMTP updates

McAfee is committed to providing you with effective and up-to-date tools you can use to protect your system. To that end, we invite you to report any new viruses that WebShield SMTP does not now detect. Please note that McAfee reserves the right to use any information you supply as it deems appropriate, without incurring any obligations whatsoever. Send your suggestions to:

AVResearch@McAfee.com	Use this address to report new virus strains.

B Virus Information Library

McAfee Virus Information Library

The McAfee Virus Information LIbrary is a comprehensive database containing more than 250 technical documents and information about more than 1000 viruses. The library offers detailed information concerning computer viruses, their methods of infection, their effect on computers, instructions on removing viruses, and methods to prevent virus infection.

The McAfee Virus Information Library is available through the McAfee Web Site.

The Virus Information Library is continuously being updated to offer the most comprehensive, up-to-date information available. For more information on reaching the McAfee Web Site, see “How to Contact McAfee” on page 7.

C McAfee Support Services

McAfee is pleased to offer many different types of technical assistance to customers. These flexible support programs are designed to meet the needs of individuals and businesses at any level. By offering support solutions that range from a complimentary 90-day introductory technical support program to an optional one-year personal support plan, McAfee helps to ensure that you receive the level of technical assistance you require.

McAfee also offers a variety of technical assistance plans designed to meet the needs of business customers, including training, consulting, enterprise support, and a Jump Start program. Please review each of the different support service plans and benefits listed in this appendix and pick the one best suited for you.

✍ *The term update refers only to the virus definition files; the term upgrade refers to product version revisions, executables, and definition files. McAfee offers free online virus signature file updates (.DATs) for the life of your product. However, we cannot guarantee backward compatibility of the signature files with previous versions' executable files (.EXEs). By upgrading your software to the latest product version and updating to the latest .DAT files regularly, you ensure complete virus protection for the term of your software subscription or maintenance plan.*

Customer Service Programs

Free 90-day introductory support program

All registered owners of single-node products are entitled to online virus updates (new .DAT files), one free online product upgrade (product version revision) with the newest features and virus protection (if applicable), and the free support services listed below during the first 90 days of software ownership.

- Electronic and online support available 24 hours a day, seven days a week on each of the forums listed below:
  - Automated voice and fax system: (408) 988-3034
  - McAfee BBS (electronic bulletin board system): (408) 988-4004
  - World Wide Web site: http://www.mcafee.com
  - CompuServe: GO MCAFEE
  - America Online keyword: MCAFEE
- Technical support phone assistance during regular business hours, 6:00 A.M.– 6:00 P.M. Pacific time, Monday through Friday, from our professionally trained support representatives at (408) 988-3832.

To receive your free one-time online upgrade please contact our Sales Support department at (408) 988-3832. Please supply your proof of purchase when you request the upgrade. You will be given a password to the upgrade area on either the McAfee BBS, FTP site, or World Wide Web site so that you can download a registered version of the latest product. This password is valid for one access only.

Subscription maintenance and support program

McAfee offers all registered owners of licensed multiple-node subscription products the following free support services and maintenance during the two-year term of the software subscription:

- Electronic and online support available 24 hours a day, seven days a week on each of the forums listed below:
  - Automated voice and fax system: (408) 988-3034
  - McAfee BBS (electronic bulletin board system): (408) 988-4004
  - World Wide Web site: http://www.mcafee.com
  - CompuServe: GO MCAFEE
  - America Online keyword: MCAFEE
- Technical support phone assistance during regular business hours, 6:00 A.M.–6:00 P.M. Pacific time, Monday through Friday, from our professionally trained support representatives at (408) 988-3832.
- Two years of free online product upgrades with the newest features and virus protection (if applicable). If you upgrade your operating system, you can also upgrade your McAfee product to the new platform (for example, from Windows 3.1 to Windows 95).

Optional support plans

✍ *Contact McAfee for current pricing structures.*

Option 1—one-year personal online maintenance and support program

For registered owners of single-node products who want to extend their support coverage, this plan allows you to call in for unlimited technical support, download the latest virus protections updates each month, and periodically download upgrades from any of McAfee's registered online services—all for a full year. If you upgrade your operating system, you can also upgrade your product program to the new platform.

Option 2—one-year quarterly disk/CD maintenance and support programs

This plan is for registered owners of either single- or multiple-node subscription products. It offers all the features of Option 1, while adding a quarterly mailing of software upgrade diskettes or CDs (depending on the product) and a quarterly update newsletter. With this option, you can update your product to include the latest features and virus updates without having to download files from an online service.

Each optional support plan begins as soon as you purchase the product and is good for one year, at which time you can renew your support program through McAfee's Sales Support department at (408) 988-3832.

✍ *McAfee reserves the right to change part or all of its customer service programs at any time without notice.*

Professional Services Programs

McAfee Professional Services provide a wide range of on-site services. Whether for short-term assistance or long-term strategic planning, a highly qualified consultant can help you achieve positive results. McAfee consultants are trained on NetWare, Microsoft NT Advanced Server, Windows 95, and a multitude of desktop applications.

Before work begins, a project manager discusses the project scope and objective with you and comes to a mutual agreement on the job objective. When the consultant leaves the site, you can be sure that the objective has been achieved. For current prices, contact McAfee.

✍ *McAfee reserves the right to change part of all of its professional services program at any time without notice.*

Training

McAfee's expertise and experience is available to your personnel, allowing an organization to take full advantage of computing resources. McAfee offers on-site training on all McAfee products, network management seminars, anti-virus seminars, customized curriculums for site-specific applications as well as product and personnel certification. McAfee's consultants provide extensive training with curriculum tailored to your organization's needs.

Consulting

McAfee Professional Services offer a number of hourly and daily consulting services including:

- Troubleshooting an existing installation
- Writing PowerScript or SaberBASIC scripts
- Planning and designing networks
- Installation and configuration
- Windows 95 configuration
- One-on-one consulting

McAfee Professional Services are available on a quotable time and materials basis to perform project management, product research, and a number of other consulting services.

Jump Start program

This fixed-fee consulting program is designed to get clients up and running on McAfee products as soon as possible. It includes training, installation, and configuration services as needed on a single server. It is designed to demonstrate how to connect various PCs to the LAN, train administrators how to use the program, and master the roll-out process.

Enterprise support

McAfee's Enterprise Support Program provides customers with the highest level of support possible. This fee-based program is designed for those customers who need a higher level of personal service.

The Enterprise Support Program offers the following features:

- Direct pager number to your assigned senior Enterprise Support Program analyst
- Extended support hours: 7:00 A.M. to 7:00 P.M. central time, Monday through Friday
- Five designated McAfee contacts
- Proactive support, providing updated company and product information as it becomes available
- On-site services at a 25% discount
- VIP issues review list
- Beta site (if desired)

Each Enterprise Support Representative calls clients each week. This phone call is used to forward any information such as technical notes and application anomalies of which you should be aware. This call also ensures that you have no unresolved problems or complications with the product. Enterprise Support representatives will return your page on the day it is received.

Optional enterprise support feature

7 X 24 support

Frequently, customers are responsible for their own LANs, which run 24 hours a day, seven days a week. This feature offers round-the-clock support for clients requiring support outside normal business hours.

Index