User's Guide

WebShield SMTP for Windows NT

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

COPYRIGHT

Copyright © 1998 Network Associates, Inc. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Network Associates, Inc.

TRADEMARK NOTICES

McAfee, McAfee Associates, VirusScan, NetShield, and Site Meter are registered trademarks of Network Associates, Inc. ScanPM, WebScan, WebScanX, SiteExpress, BootShield, ServerStor, ScreenScan, ScreemScan, WebCrypto, PCCrypto, NetCrypto, Remote Desktop 32, WebShield, NetRemote, eMail-It, Hunter, PC Medic, PC Medic 97, and SecureCast are trademarks of Network Associates, Inc. All other products or services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

“SABRE” is a trademark of American Airlines, Inc. and is licensed for use to Network Associates. Saber Software is not affiliated with American Airlines, Inc. or SABRE Travel Information Network. All trademarks are the property of their respective owners.

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 January 1998 / WebShield SMTP v3.1.0

Table of Contents

Chapter 1. Introducing WebShield SMTP 6

What is WebShield SMTP? 6
Why use WebShield SMTP? 6
Main features 7

How To Contact McAfee 8
Customer service 8
Technical support 8
McAfee training 9
International contact information 10

Chapter 2. Installing WebShield SMTP 12

Before You Start 12

Installation Procedure 13

Post Installation Configuration 16
Single server configuration 16
Single server configuration using Microsoft Exchange 17
Multiple server configuration 25
Registering additional trusted clients 27
Optimizing WebShield SMTP performance 28

Chapter 3. Using WebShield SMTP 30

Starting the Administration Console 30

Using the Administration Console 31

Using the Servers Property Page 32
Loading and sending WebShield SMTP configurations 33
Adding a WebShield SMTP server 33
Removing a WebShield SMTP server 34
Setting a default WebShield SMTP server 34

Using the SMTP Property Page 34
Using the Scan tab 36
Using the Action tab 37
Using the Ports tab 39
Using the Exclude Recipient tab 41
Using the DNS tab 42
Using the Exclude Sender tab 43
Using the Block tab 45
Using the Relay tab 47
Using the Logs Property Page 51
Using the Quarantine Property Page 54
Viewing a quarantined file 55
Using the Alert Property Page 56
Displaying WebShield SMTP Information 58
Displaying Mail and Virus Statistics 59
Using the Content Filter Property Page 60
Shutting Down WebShield SMTP 61

Chapter 4. Virus Notification 62

Using Alert Manager 62
Summary window 63
Forwarding alerts to another computer 64
Sending a network message 65
Sending an alert to an e-mail address 66
Sending an alert to a pager 68
Sending an alert to a printer 70
Using SNMP 72

Appendix A. Updating WebShield SMTP 73

Detecting New and Unknown Viruses 73
Why would I need a new data file? 73
Updating your data files 74
Reporting new items for WebShield SMTP updates 75

Appendix B. McAfee Support Services 76

Customer Service Programs 77

Free 90-day introductory support program 77

Subscription maintenance and support program 78

Optional support plans 79

Professional Services Programs 80

Training 80

Consulting 80

Jump Start program 81

Enterprise Support 81

Optional Enterprise Support feature 82

Index 83

1 Introducing WebShield SMTP

What is WebShield SMTP?

WebShield SMTP (Simple Mail Transfer Protocol) 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—including compressed formats—protecting your network from harmful infections. Using the Java™-based Administration Console, you can configure and maintain WebShield SMTP either locally or remotely 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 gateway. It detects, cleans, logs, and quarantines infected file attachments, including compressed files. As a result, these tasks are handled at the point of entry before the virus proliferates to individual mail recipients.

Main features

- Scans e-mail attachments at the SMTP mail gateway
- Supports scanning of ZIP, LHA and CAB format compressed files
- 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
- Anti-virus scanning can be disabled for selected senders and recipients.
- Can be used to search e-mail messages for objectionable or sensitive content
- Can be used to block unwanted e-mail by recipient, sender, or server
- Implemented as a Windows NT Service
- Can be used to relay mail from a server or domain name to another server

How To Contact McAfee

Customer service

To order products or obtain product information, we invite you to contact our Customer Care department by calling (408) 988-3832 or by writing to 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 site on the World Wide Web a valuable resource for answers to technical support issues. 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 do not have the answers you need, contact McAfee at one of the following numbers 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 and model
- Any additional hardware or peripherals connected to your computer
- Operating system type and version numbers
- Network type and version, if applicable
- Contents of your AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script
- Specific steps to reproduce the problem

McAfee training

For information about scheduling on-site training for any McAfee product, call (800) 338-8754.

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
Canada L3R 2G6
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 S.A.
50 rue de Londres
75008 Paris
France
Phone: 33 1 44 908 737
Fax: 33 1 45 227 554

McAfee Deutschland GmbH
Industriestrasse 1
D-82110 Germering
Germany
Phone: 49 8989 43 5600
Fax: 49 8989 43 5699

McAfee (UK) Ltd.
Hayley House, London Road
Bracknell, Berkshire
RG12 2TH
United Kingdom
Phone: 44 1344 304 730
Fax: 44 1344 306 902

McAfee Japan Co, Ltd.
Toranomon 33 Mori Bldg.
3-8-21 Toranomon
Minato-Ku, Tokyo 105
Japan
Phone: 81 3 5408 0700
Fax: 81 3 5408 0780

McAfee Korea
135-090, 18th Fl., Kyoung Am Bldg.
157-27 Samsung-Dong, Kangnam-Ku
Seoul, Korea
Phone: 82 2 555-6818
Fax: 82 2 555-5779

McAfee South East Asia
7 Temasek Boulevard
The Penthouse
#44-01, Suntec Tower One
Singapore 038987
Phone: 65 430-6670
Fax: 65 430-6671

McAfee Latin America
150 South Pine Island Road, Suite 205
Plantation, FL 33324
USA
Phone: 954-452-1731
Fax: 954-236-8031

McAfee Australia
Level 1, 500 Pacific Highway
St. Leonards, NSW 2065
Australia
Phone: 61-2-9437-5866
Fax: 61-2-9439-5166

2 Installing WebShield SMTP

Before You Start

McAfee recommends that this product be installed by a mail administrator.

You have the option of installing WebShield SMTP on the same computer where your SMTP mail server is running, or on a separate computer. Regardless of which configuration you choose, the basic system requirements for installing WebShield SMTP are the same. You must have:

- A computer running Windows NT Server version 3.51 or later with the latest Microsoft Service Pack.

  ✍ *WebShield SMTP's server component cannot be installed on a computer running Windows NT Workstation software.*

  ✍ *If you are running WebShield SMTP and your SMTP mail server on separate computers, McAfee recommends using computers with similar hardware specifications.*

- 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.

- At least 64MB of memory.

- Java Runtime Environment (JRE) v1.3 or later.

  ✍ *To run the Java-based Administration Console, install the Java Runtime Environment. You can obtain the Java Runtime Environment from the WebShield SMTP installation CD, or by downloading it from http://www.Javasoft.com/products/.*

Installation Procedure

To install WebShield SMTP, follow these steps:

Step	Action

1. Log on to the Windows NT SMTP server. You must use a service account with Administrator security rights to the Windows NT domain or local computer.

✍ *If you are installing the WebShield SMTP Administration Console only, you may use a computer running either Windows NT Server or Windows NT Workstation.*

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 Welcome to Setup screen appears.

5. Click Next.

Response: The Setup Type screen appears.

6. If you want to change the destination directory for WebShield SMTP's program files, click Browse. Enter a directory and click OK.

7. Select the type of installation:

- To install all WebShield SMTP options including the Administration Console and Alert Manager, select Typical and click Next.
- To install only the WebShield SMTP Administration Console, select Compact and click Next.

  ✍ *Select this option when establishing a trusted client for the purpose of configuring WebShield SMTP remotely.*

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

Response: The Service Account Usage screen appears.

8. Review the information provided, then click Next to continue.

Response: The Service Account Information screen appears.

9. Specify the account type that will run WebShield SMTP's services by selecting Use System Account or Use Custom Account.Use Custom Account is the default account type.

10. Enter a user name with administrator rights and the appropriate password, then click Next. Do not use a password that will expire.

Response: The Confirm Installation Settings screen appears.

11. Review the installation options. If you want to make changes, click Back three times to reach the Setup Type screen. If the installation options are correct, click Next.

Response: WebShield SMTP files are copied to the server. The What's New in WebShield SMTP screen appears.

12. It is strongly recommended that you read the What's New in WebShield SMTP file. This file contains important last-minute information. Click Yes to read this file, or No to continue.

Response: If you click Yes, your computer's text editor is launched and What's New in WebShield SMTP appears.

13. After reading What's New in WebShield SMTP, close the file and the text editor.

14. Click Finish to complete the Setup process.

Response: WebShield SMTP is installed.

✍ *It is strongly recommended that you read the WebShield SMTP README.1ST file before continuing. README.1ST contains important information on registering and validating your software, McAfee contact information, and a product license agreement. To open the README.1ST file, click Start, point to McAfee WebShield SMTP, and click Read Me 1st.*

15. Configure your SMTP environment to transfer mail through WebShield SMTP. For detailed instructions, see "Post Installation Configuration" on page 16.

When installation concludes, McAfee WebShield SMTP Mail Configuration, Scan, and Alert Manager services start 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 and your SMTP mail server are running on the same computer, see "Single server configuration" below. If WebShield SMTP and your SMTP mail server are installed on separate computers, see "Multiple server configuration" on page 25.

Single server configuration

Figure 2-1 shows a single-server configuration environment where WebShield SMTP and the SMTP mail server are running on the same computer.

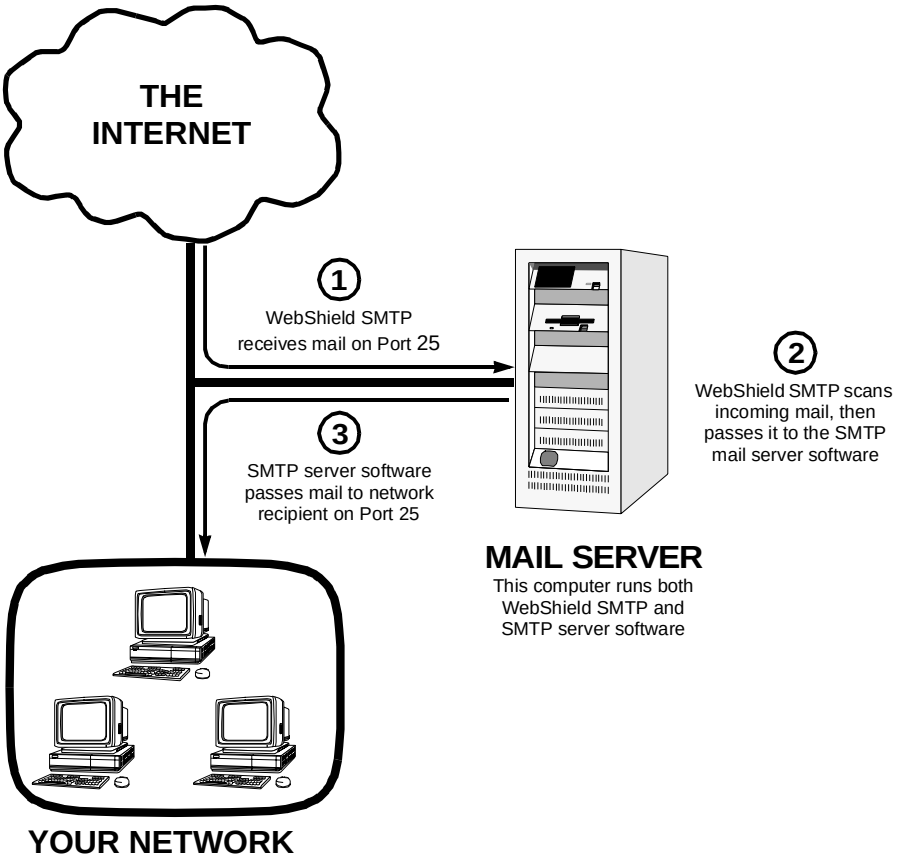

Figure 2-1. Single System Environment

If your SMTP mail environment resembles the environment displayed in Figure 2-1, you must modify ports in WebShield SMTP and your SMTP server. If you are using Microsoft Exchange as a mail server, skip the following procedure and go to "Single server configuration using Microsoft Exchange" below. If you are using a mail server other than Microsoft Exchange, follow these steps:

Step	Action

1. Start the Administration Console. See "Starting the Administration Console" on page 30 for instructions on starting and using the console.

2. Open the SMTP property page, then open the Ports tab. Select the following checkbox: WebShield and Mail Server on the Same System.

3. Click inside the Send text box, then enter any available port number other than 25 or 9999.

4. Open the Servers property page, then click Send Config to save the changes you made in the Ports tab.

5. Reconfigure the incoming mail port for your SMTP mail server to be consistent with WebShield SMTP's send port number.

6. Configure your SMTP mail server to forward all remote mail through the WebShield SMTP server. This will ensure that all outbound mail is scanned by WebShield SMTP.

   ✍ *The procedures to complete Steps 5 and 6 above will vary depending on the mail server software you are using.*

Single server configuration using Microsoft Exchange

If you installed WebShield SMTP and Microsoft Exchange on the same computer, you must make additional configuration changes to Windows NT, Microsoft Exchange, and WebShield SMTP. Complete the following four-part procedure in the exact order it appears below:

✍ *The configuration adjustments in this section are only required when WebShield SMTP and Microsoft Exchange are running on the same computer. If you are running WebShield SMTP and Microsoft Exchange on separate computers, skip this section.*

Part 1: Make the following changes in Windows NT:

Step	Action
1.	Using a text editor, open the following Windows NT file: `\(your Windows NT system directory)\system32\drivers\etc\services`
2.	Locate the following line: `smtp 25/tcp mail` ✍ *To locate this line quickly, open your text editor's search feature and find "smtp."*
3.	Replace the number 25 with the port number you want WebShield SMTP to use when sending mail after it has been scanned. You can use any available port number other than 25 and 9999. Example: `smtp 7192/tcp mail`.
4.	Save the change you made to `\services`

Part 2: Make the following changes in Microsoft Exchange:

Step	Action
1.	Start Microsoft Exchange Administrator.
2.	Browse through the tree view of your site to the Connections container, then double-click Internet Mail Service (In Microsoft Exchange 4.0, this connector is called Internet Mail Connector). **Response:** The Internet Mail Service Properties dialog box (Figure 2-3 on page 19) appears.
3.	Click the Connections tab, then click Advanced.

Response: The Advanced dialog box (Figure 2-2) appears..

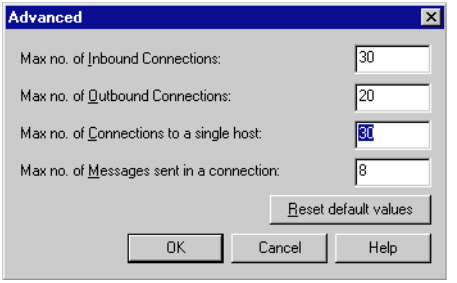

Figure 2-2. Microsoft Exchange Advanced dialog box

4. In the Maximum Number of Connections to a Single Host text box, enter the number displayed in the Maximum Number of Inbound Connections text box, then click OK.

Response: The Internet Mail Service Properties dialog box (Figure 2-3) appears.

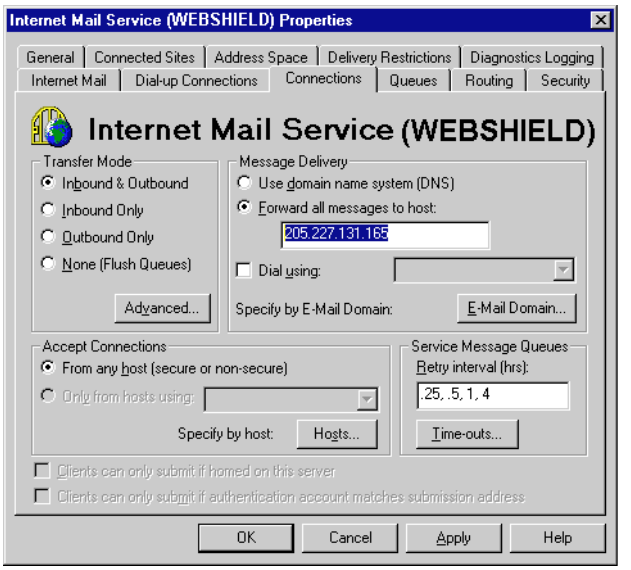

Figure 2-3. Microsoft Exchange Internet Mail Service Properties (Connections tab)

5. Select Forward All Messages To Host.

6. Enter the IP (Internet Protocol) address for your mail server in the text box below the Forward all Messages To Host radio button

If you are using Microsoft Exchange 5.0 or 5.5, complete steps 7 and 8. If you are using Microsoft Exchange 4.0, skip 7 and 8 and proceed to Step 9.

7. Click the Routing tab.

   Response: The Internet Mail Service Properties dialog box (Figure 2-4) appears with the Routing tab displayed.

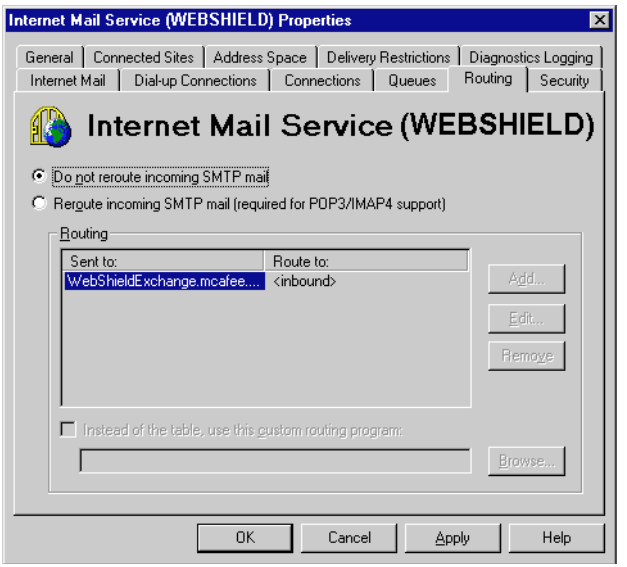

Figure 2-4. Microsoft Exchange Internet Mail Service Properties (Routing tab)

8. Select Do Not Reroute Incoming SMTP Mail

9. You must restart Microsoft Exchange Internet Mail so the changes you made will take effect. In Windows NT, do the following:

   - Click Start, point to Settings, then click Control Panel.
   - Double-click Services.

- The Services window appears. Highlight Microsoft Exchange Internet Mail Service, then click Stop. Wait until the service stops, then click Start.

Part 3: Make the following changes in WebShield SMTP:

Step	Action
1.	Start the Administration Console. See "Starting the Administration Console" on page 30 for instructions on starting and using the console.
2.	Open the SMTP property page, then click the Ports tab.
3.	In the Send text box, enter the port number you entered earlier in the Windows NT file: `\%winsysdir%\system32\drivers\etc\services`
4.	Select Enable WebShield and Mail Server on same System.
5.	Click the DNS tab.
6.	Select Enable DNS to enable domain name service resolution.
7.	Click inside the DNS Address text box, then enter the IP addresses of the domain name servers that provide service for your network. Click Add.

✍ *If you don't know the IP address of the domain name server for your network, you can obtain the address by doing the following:*

- Click Start, point to Settings, then click Control Panel.
- Double-click Network.
- The Network dialogue box appears. Double-click TCP/IP Protocol Properties, then click the DNS tab.
- The IP addresses for your network's domain name servers appear.

8.	Click the Servers tab, then click Send Config to save the changes you've made to WebShield SMTP.

Part 4: Make the following changes in Windows NT:

Step	Action

1. Open the Windows NT Registry Editor:

- If you are using Windows NT 3.51, click File, click Run, then enter: `REGEDT32.EXE`
- If you are using Windows NT 4.0, click Start, click Run, then enter: `REGEDIT.EXE`

2. Click OK.

3. Open this key: `HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\Web-Shield SMTP\MailScan`

4. Double-click the Registry key: `\SMTP_DIRECT_SEND_INTERNAL_DOMAIN.`

Response: The Edit String window appears.

5. Enter the domain name for your network, then click OK.

Example: mydomain.com

6. Double-click the Registry key: `\SMTP_DIRECT_SEND_ON.`

Response: The Value Data window appears.

7. Enter 1, then click OK.

8. To have your changes take effect, restart McAfee WebShield SMTP MailScan. In Windows NT, follow these steps:

- Click Start, point to Settings, then click Control Panel.
- Double-click Services.

- The Services window appears. Highlight McAfee WebShield SMTP MailScan, then click Stop. Wait until the service stops, then click Start.

Testing your configuration

After completing the configuration changes needed to run WebShield SMTP and Microsoft Exchange on the same computer, McAfee recommends you conduct the following three tests to verify that your system is working properly.

Test 1: To verify that WebShield SMTP's Mail Scan Service is running, use the Windows NT telnet feature:

Step	Action
1.	Click Start, then click Run.
2.	The Run text box appears. Enter: `telnet (server host and domain name) 25.` Example: `telnet mail.xyzcorp.com 25`
3.	Press Enter. **Response:** In the example above, the following text should appear: `220 mail.xyzcorp.com WebShield SMTP V3.1.0 McAfee & Assoc. Ready at Mon Dec 15 22:02:54 1997`

Test 2: To verify that Microsoft Exchange's Internet Mail Service is running, use the Windows NT telnet feature:

Step	Action
1.	Click Start, then click Run.
2.	The Run text box appears. Enter: `telnet (server host and domain name) (WebShield SMTP send port)` Example: `telnet mail.xyzcorp.com 7192`

3. Press Enter.

   Response: In the example above, the following text should appear:
   `220 mail.xyzcorp.com Microsoft Exchange Internet Mail Service 5.0.1457.7 ready`

Test 3: There are many ways to verify that WebShield SMTP and Microsoft Exchange are working together. McAfee recommends the following test, which will allow you to verify that both inbound and outbound mail is being delivered and received.

Step	Action

1. Send a message from a Microsoft Exchange client in your network to an e-mail address on the Internet that you have access to (your home e-mail address, for instance).

   Response: If your system is configured properly, Microsoft Exchange receives the outbound message from the client, then delivers it to WebShield SMTP on port 25. WebShield SMTP scans the message for viruses, cleans any infected components, then delivers the message to the Internet recipient.

2. Check the Internet recipient's e-mail account to verify that the message arrived, then send a reply message from that account to the Microsoft Exchange client from which the message originated.

   Response: If your system is configured properly, WebShield SMTP receives the reply message on port 25. WebShield SMTP scans the message for viruses, cleans any infected components, then delivers the message to Microsoft Exchange on the WebShield SMTP send port you specified. Finally, Microsoft Exchange delivers the reply message to the client from which the message originated.

Multiple server configuration

Figure 2-5 shows an environment where WebShield SMTP and the SMTP mail server are installed on separate computers.

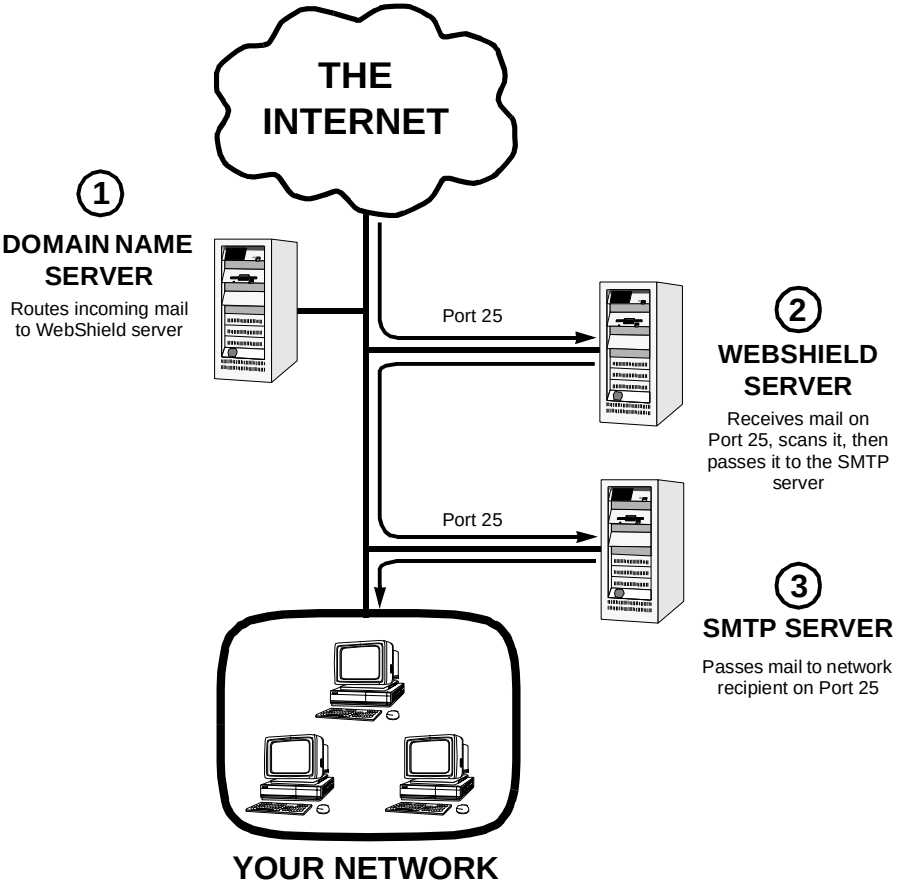

Figure 2-5. Multiple Server Environment

If your SMTP mail environment resembles the environment displayed in Figure 2-5, you must modify your network Domain Name Server (DNS) to forward e-mail messages to the WebShield SMTP server before they are sent to your SMTP server.

Follow these steps to modify your local DNS:

Step	Action

1. Start the Administration Console. See "Starting the Administration Console" on page 30 for instructions on starting and using the console.

2. Open the SMTP property page, then open the Ports tab. Clear the following checkbox: WebShield and Mail Server on the Same System.

3. Open the DNS tab, then select Enable DNS to enable domain name service resolution.

4. Click inside the DNS Address text box, then enter the IP addresses of the domain name servers that provide service for your network. Click Add.

   ✍ *If you don't know the IP address of the domain name server for your network, you can obtain the address by doing the following:*

   - Click Start, point to Settings, then click Control Panel.
   - Double-click Network.
   - The Network dialogue box appears. Double-click TCP/IP Protocol Properties, then click the DNS tab.
   - The IP addresses for your network's domain name servers appear.

5. Open the Servers property page, then click Send Config to save the changes you made in the Ports and DNS tabs.

6. At your local DNS server, edit the DNS table to substitute WebShield SMTP for your existing mail server.

   ✍ *Ensure that DNS and A resource records exist for the WebShield SMTP server.*

7. Locate the Mail Exchanger (MX) resource record entry used by your existing SMTP mail server.

8. 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.*

Registering additional trusted clients

You can configure the WebShield SMTP server from any computer within your network. To remotely configure the WebShield SMTP servers you must install WebShield SMTP's Administration Console on the remote computer, then register that computer as a trusted client by adding it to the WebShield SMTP Server List.

To install the Administration Console on the remote computer, see "Installation Procedure" on page 13. In Step 7, select Compact.

- System requirements for the WebShield SMTP Administration Console: a computer running Windows NT Server 4.0 or Windows NT Workstation 4.0.

To register the remote computer as a trusted client, log on to the WebShield SMTP server, then follow these steps:

Step **Action**

1. Do one of the following:

   - For Windows NT 3.51, choose File/Run and type `REGEDIT32`.
   - 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 clients. Separate each client name with a space.

   Example: Allowed_Clients "localhost1 mailserver administration1"

4. Choose Exit from the Registry menu when complete.

Optimizing WebShield SMTP performance

You can increase WebShield SMTP's capacity to receive, scan, and send mail if the computer it is running on has more than 64MB of memory installed. Do this by increasing the maximum number of concurrent scan threads available to WebShield SMTP.

✍ *This procedure is not required as part of the installation process.*

Step	Action

1. Open the Windows NT Registry Editor, then go to HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\WebShield SMTP\MailScan. Double-click Scan_Max_Number_Threads.

   Response: The Edit DWORD Value window appears.

2. Enter a number greater than 50 (consider using 100) in the text box, then select Decimal. Click OK.

3. You must restart Microsoft Exchange Internet Mail so the changes you made will take effect. In Windows NT, do the following:

   - Click Start, point to Settings, then click Control Panel.
   - Double-click Services.

- The Services window appears. Highlight Microsoft Exchange Internet Mail Service, then click Stop. Wait until the service stops, then click Start.

✍ *Another method to increase WebShield SMTP's processing capacity is to install WebShield SMTP on one or more additional servers, and to add these servers to your local domain name server. This solution provides a means to load balance WebShield SMTP and adds redundancy to your mail environment.*

3 Using WebShield SMTP

Starting the Administration Console

After installation, all WebShield SMTP configuration and management is controlled through the Webshield SMTP Administration Console. Default configuration settings are established during the installation, but you'll probably want to customize them yourself. This chapter outlines the options that are available using the Administration Console and details the steps to take to configure your software.

The Webshield SMTP 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 27**.*

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

✍ *The Java Runtime Environment is not yet supported on 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 appears (see Figure 3-1 on page 31).

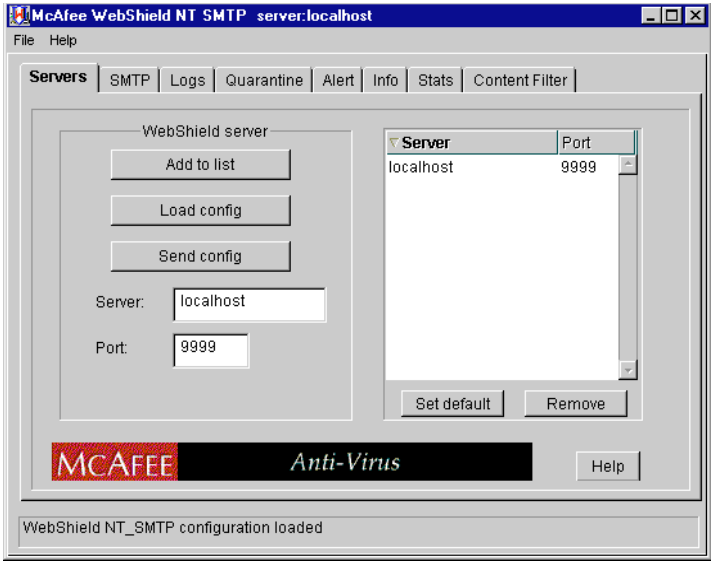

Figure 3-1. WebShield SMTP Administration Console (Servers property page)

Using the Administration Console

From the WebShield SMTP Administration Console (Figure 3-1 on page 31) you can select menu items for configuration and management. Use the property pages to customize, manage, and maintain all aspects of Webshield SMTP. 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 32.

- **SMTP.** Use this page to select virus scanning preferences, choose port and DNS configurations, block unwanted mail, and relay mail to alternative domains. To perform these actions, see "Using the SMTP Property Page" on page 34.

- **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 51.

- **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 54.

- **Alert.** Use this page to direct WebShield SMTP to send an alert message when it detects a virus. The message can be sent to various recipients in your organization via Alert Manager, and to the sender of the infected mail. To enable the Alert option, see "Using the Alert Property Page" on page 56.

- **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 58.

- **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 59.

- **Content Filter.** Use this page to direct WebShield SMTP to store duplicate copies of all mail messages passing through the SMTP server that contain a particular word or string of words in the header or body of the mail. For instance, you can use the Content Filter feature to find sensitive or objectionable text in mail messages. To activate content filtering, see "Using the Content Filter Property Page" on page 60.

Using the Servers Property Page

To use the WebShield SMTP Servers property page (Figure 3-1 on page 31), start the Administration Console and click Servers.

From this page, you can:

- Load and send Webshield SMTP configuration settings
- Add a WebShield SMTP server to Administration Console
- Remove a WebShield SMTP server from the Administration Console

- Set a default WebShield SMTP 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 Server list and click Load Config—or double-click the name you selected—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. The name of the server being configured appears in the WebShield SMTP title bar.
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 SMTP server

To add a WebShield SMTP server to the Administration Console, use the Servers property page (Figure 3-1 on page 31) 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 Server list.

Removing a WebShield SMTP server

To remove a WebShield SMTP server from the Administration Console, use the Servers property page (Figure 3-1 on page 31) and follow the instructions below.

Step	Action
1.	In the Server list, select the WebShield SMTP server name you want to remove.
2.	Click Remove. **Response**: The WebShield SMTP server and port number are removed from the Server list.

Setting a default WebShield SMTP server

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

Using the SMTP Property Page

The WebShield SMTP property page (Figure 3-2 on page 36) allows you to select virus scanning preferences, choose port and DNS configurations, block unwanted mail, and relay mail to alternative domains.

The SMTP property page contains eight tabs:

- **Scan.** Use the Scan tab to select the e-mail attachment types you want WebShield SMTP to scan**.**
- **Action.** Use the Action tab to choose how you want WebShield SMTP to respond to infected e-mail attachments and scan errors.

- **Ports.** Use the Ports tab to specify which read and send ports you want WebShield SMTP to use, and to select the configuration you are using WebShield SMTP in: single server or multiple server.

- **Excld Recpt.** Use the Exclude Recipient tab to allow e-mail sent to certain addresses or domains to pass through the WebShield SMTP server without being scanned for viruses.

- **DNS.** Use the DNS tab to add and remove domain name server addresses.

- **Excld Sndr.** Use the Exclude Sender tab to allow e-mail sent from certain addresses or domains to pass through the WebShield SMTP server without being scanned for viruses.

- **Block.** Use the Block tab to tell WebShield SMTP not to deliver mail sent from certain e-mail addresses and domains.

- **Relay.** Use the Relay tab to relay mail from any host to an alternative host.

To use the SMTP property page, start the Administration Console, then click the SMTP tab.

Response: The WebShield SMTP property page appears with the Scan tab open (Figure 3-2).

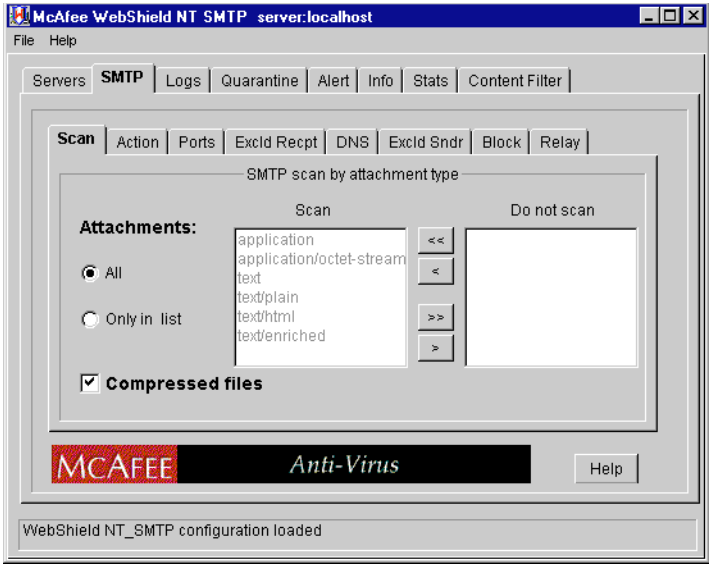

Figure 3-2. WebShield SMTP Administration Console (SMTP Scan tab)

Using the Scan tab

Use the Scan tab to select the types of e-mail attachments you want to scan.

1. At the SMTP property page, click the Scan tab.

   Response: The SMTP Scan tab (Figure 3-2) appears.

2. Do one of the following:

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

- To only scan certain file attachment types passing through the SMTP server, select the Only In List option. Choose 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 scan octet-stream applications.
  - **Text**. Select this option to scan all text files.
  - **Text/HTML**. Select this option to scan HTML text files.
  - **Text/Plain**. Select this option to scan plain text files.
  - **Text/Enriched**. Select this option to scan enriched text files.

  To move file attachment types between the Scan and Do not scan lists, To only scan certain file attachment types passing through the SMTP server, select the Only In List option. Choose the file attachments you want WebShield SMTP to scan. The options are listed below.

3. To scan compressed files passing through the SMTP server, select compressed files.

4. Click Send Config in the Servers property page to save the changes you've made, or select another tab or property page to further configure WebShield SMTP.

Using the Action tab

Use the Action tab to choose how you want WebShield SMTP to respond to infected e-mail attachments and scan errors.

1. At the SMTP property page, click the Action tab.

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

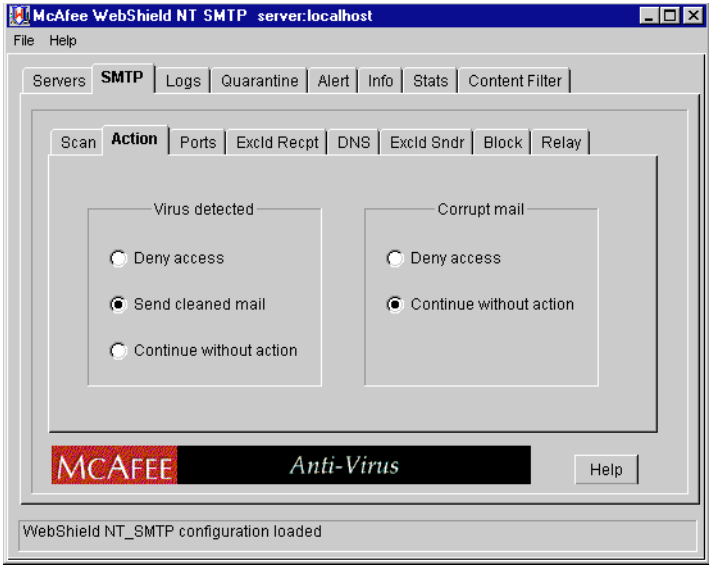

Figure 3-3. WebShield SMTP Administration Console (SMTP Action tab)

2. Specify the 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 text file containing the name of the infected file, the virus name, and the sender's address.*

   - **Continue without action.** Select this option if you want WebShield SMTP to 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 54, for more information about the Quarantine option and "Using the Logs Property Page" on page 51, for information about logging.*

3. 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.

4. Click Send Config in the Servers property page to save the changes you've made, or select another tab or property page to further configure WebShield SMTP.

Using the Ports tab

Use the Ports tab to specify the port you want WebShield SMTP to use to receive mail prior to scanning it, and the port you want it to use to send mail after it scans it. You can also use this tab to specify whether you are using WebShield SMTP and your SMTP server in a single server or multiple server configuration.

1. At the SMTP property page, click the Ports tab.

Response: The SMTP Ports tab appears (Figure 3-4).

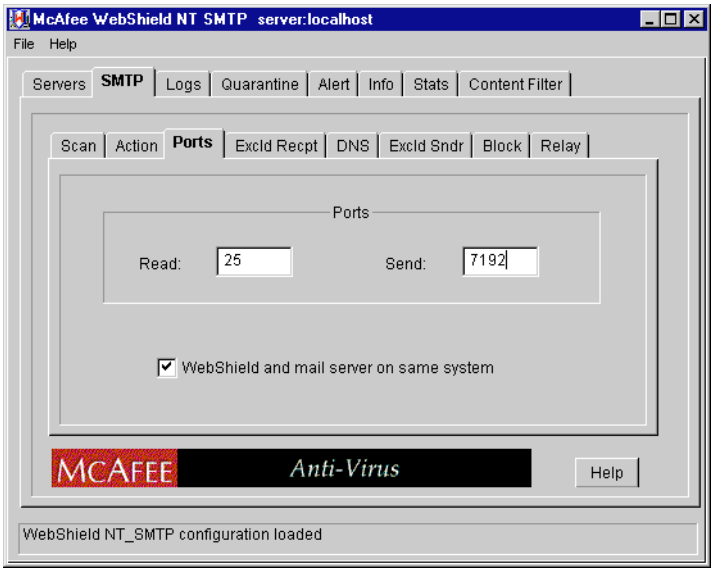

Figure 3-4. WebShield SMTP Administration Console (SMTP Ports tab)

2. In the Read text box, enter the port number you want WebShield SMTP to use to receive mail prior to scanning it.

3. In the Send text box, enter the port number you want WebShield SMTP to use to send mail to mail servers after it scans it.

4. If your are operating WebShield SMTP and your SMTP mail server on the same computer, select WebShield and Mail Server on the Same System. For more information, see "Single server configuration" on page 16.

   If you are operating WebShield SMTP and your SMTP mail server on separate computers, clear the WebShield and Mail Server on the Same System checkbox. For more information, see "Multiple server configuration" on page 25.

5. Click Send Config in the Servers property page to save the changes you've made, or select another tab or property page to further configure WebShield SMTP.

Using the Exclude Recipient tab

In special circumstances you may want to allow e-mail sent to certain addresses or domains to pass through the WebShield SMTP server without being scanned for viruses. To do this, use the Exclude Recipient tab.

1. At the SMTP property page, click the Exclude Recipient tab.

   Response: The SMTP Exclude Recipient tab appears (Figure 3-5).

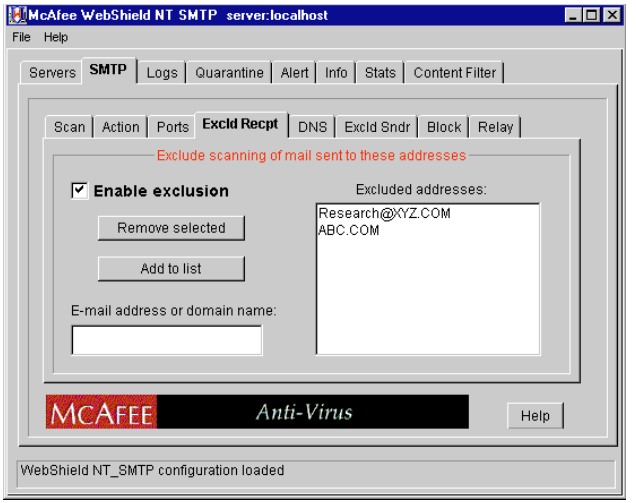

Figure 3-5. WebShield SMTP Administration Console (SMTP Exclude Recipient tab)

2. Select the Enable exclusion checkbox.

   ✍ *If this checkbox is selected, WebShield SMTP will not clean mail sent to the addresses in the Excluded addresses list.*

3. Enter the e-mail address or domain name you want to exclude from incoming mail scanning in the text box provided. Click Add to list.

4. To re-enable cleaning of messages sent to an e-mail address or domain name, select the address and click Remove selected.

5. Click Send Config in the Servers property page to save the changes you've made, or select another tab or property page to further configure WebShield SMTP.

Using the DNS tab

WebShield SMTP requires valid domain name server addresses for mail delivery. Use the DNS tab to add and remove domain name server addresses.

✍ For more information on entering domain name server addresses, see "Post Installation Configuration" on page 16.

1. At the SMTP property page, click the DNS tab.

   Response: The SMTP DNS tab appears (Figure 3-6).

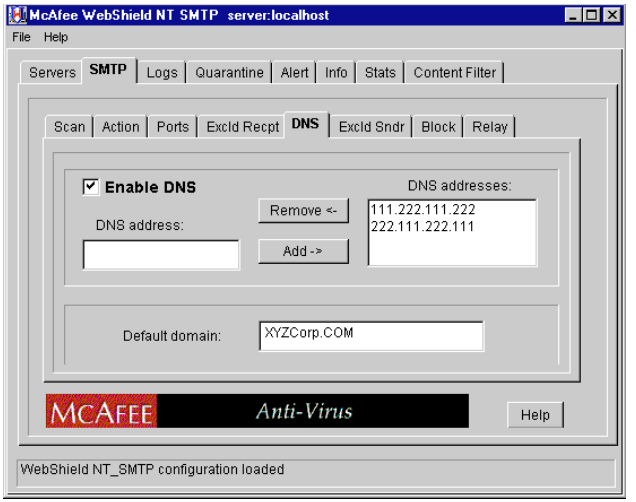

Figure 3-6. WebShield SMTP Administration Console (SMTP DNS tab)

2. Select the Enable DNS checkbox to allow WebShield SMTP to query the local domain name server to deliver remote mail (i.e., mail delivered via the Internet).

3. Enter the IP address for the domain name server that provides service for your network in the DNS Address text box. Click Add.

4. Click inside the Default domain text box and enter your network domain name.

5. Click Send Config in the Servers property page to save the changes you've made, or select another tab or property page to further configure WebShield SMTP.

Using the Exclude Sender tab

You may want to allow mail sent from certain addresses or domains to pass through the WebShield SMTP server without being scanned for viruses. For instance, you may want to disable scanning for all of your network's outgoing mail. In special circumstances, you may want to disable scanning for mail sent into your network from selected addresses or domain names.

To disable scanning for mail sent from a particular address or domain name, use the Exclude Sender tab.

1. At the SMTP property page, click the Exclude Sender tab.

Response: The SMTP Exclude Sender tab appears (Figure 3-7).

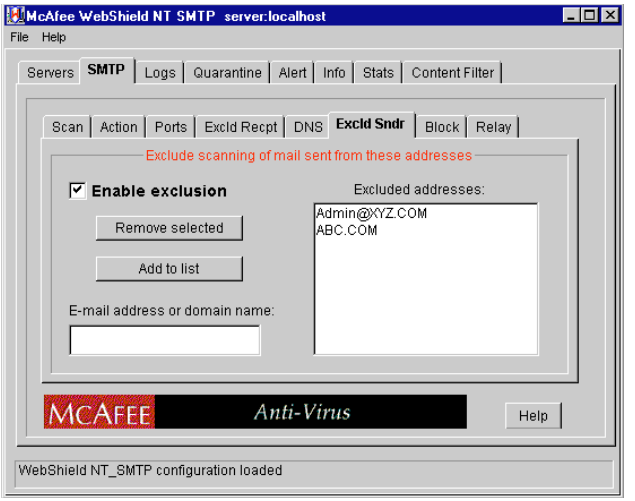

Figure 3-7. WebShield SMTP Administration Console (SMTP Exclude Sender tab)

2. Select the Enable exclusion checkbox.

   ✍ *If this checkbox is selected, WebShield SMTP will not clean mail sent from the addresses in the Excluded addresses list.*

3. Enter the e-mail address or domain name you want to exclude from outgoing mail scanning in the text box provided. Click Add to list.

   Response: The address you entered appears in the Excluded addresses text box.

4. To re-enable scanning of messages sent from an e-mail address or domain name, select the address and click Remove selected.

5. Click Send Config in the Servers property page to save the changes you've made, or select another tab or property page to further configure WebShield SMTP.

Using the Block tab

Use the Block tab to stop the delivery of mail sent from certain e-mail addresses and domains. Mail sent from the addresses you specify is not delivered to the intended recipient. Instead, it's stored in the Webshield SMTP subdirectory \BLOCKED.

✍ *This feature is useful for intercepting unsolicited bulk e-mail from senders outside your network—spammers, in other words. The Block tab can also be used to intercept mail from senders within your network.*

1. At the SMTP property page, click the Block tab.

   Response: The SMTP Block tab appears (see Figure 3-8 on page 45).

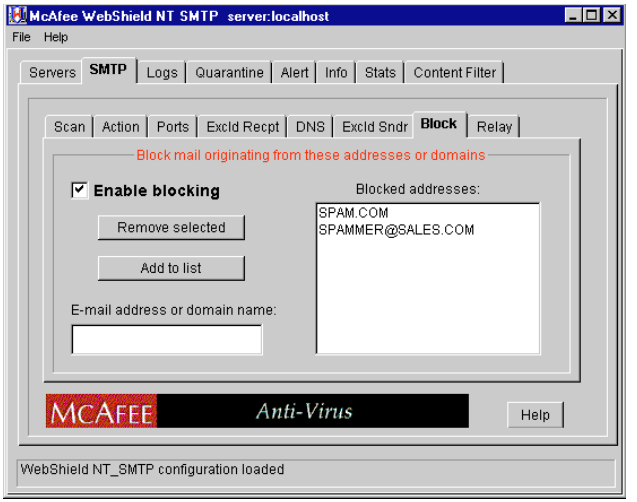

Figure 3-8. WebShield SMTP Administration Console (SMTP Block tab)

2. Select the Enable blocking checkbox.

3. Enter the e-mail address or domain name you want to block in the text box provided. Click Add to list.

Response: The address you entered appears in the Blocked addresses text box.

4. To remove blocking for an e-mail address or domain name, select the address and click Remove selected.

5. Click Send Config in the Servers property page to save the changes you've made, or select another tab or property page to further configure WebShield SMTP.

Using the Relay tab

Use the Relay tab to divert mail from the mail server or domain it is addressed to an alternative mail server.

Reasons to use Relay:

- You want to establish backup mail servers that can be used when your primary mail servers are overloaded or down. Figure 3-9 shows the Relay feature configured to use two backup mail servers.
- You want to enhance the security of your network by concealing the true names of your mail servers. Figure 3-10 shows the Relay feature configured to conceal the identity of three mail servers within a network.
- Your SMTP server does not support domain naming service protocol, or your domain name server is down.

The diagrams on the following pages give two examples of typical uses for WebShield SMTP's Relay feature.

In this first example, a network administrator uses the Relay feature to relay incoming mail to a backup mail server if the network's primary mail server is overloaded or down. If the backup mail server is also overloaded or down, mail is sent to a second backup server. The precedence among these mail servers is established by the order they appear in the Relay Tab list.

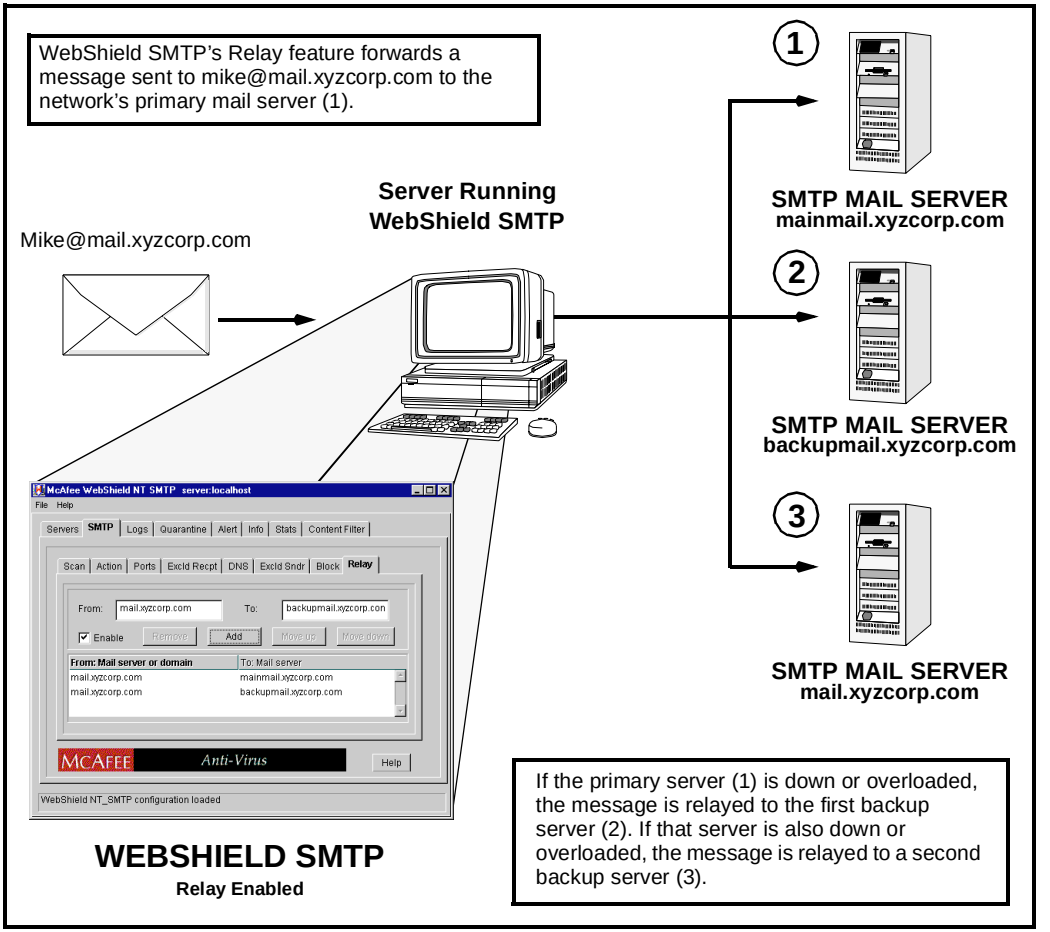

Figure 3-9. Using Relay to establish backup mail servers

In this second example, the network administrator uses WebShield SMTP's Relay feature to conceal the actual domain names of three mail servers on the network. The domain name mail1.xyzcorp.com serves as an alias for the actual mail server accounting.xyzcorp.com. Likewise, mail2.xyzcorp.com and mail3.xyzcorp.com serve as aliases for engineering.xyzcorp.com and sales.xyzcorp.com. The true names of the servers remain secret, reducing the potential for security breaches, while also ensuring proper mail delivery.

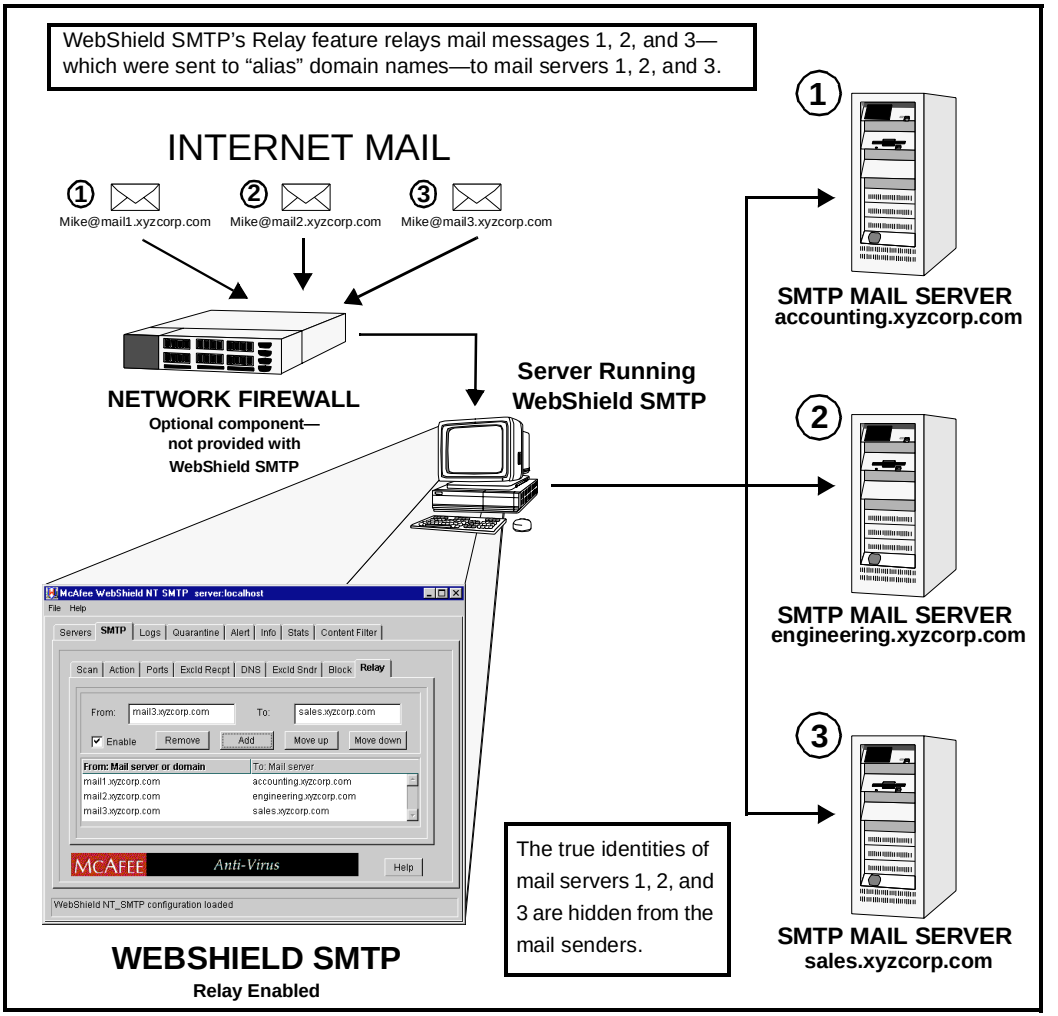

Figure 3-10. Using Relay to conceal the identity of mail servers

To configure WebShield SMTP to use the Relay feature, follow these steps:

Step	Action

1. At the SMTP property page, click the Relay tab.

Response: The SMTP Relay tab appears(Figure 3-11).

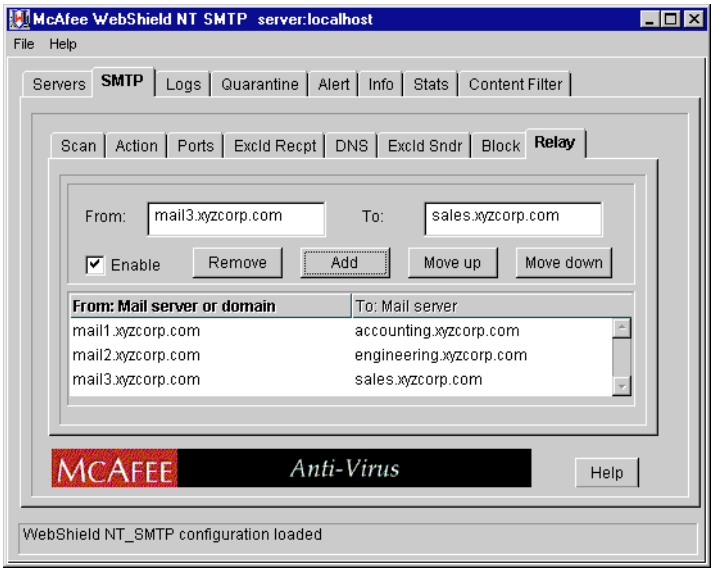

Figure 3-11. WebShield SMTP Administration Console (SMTP Relay tab)

2. Select Enable to use the Relay feature.

3. Enter the mail server or domain name from which you want to relay mail in the From text box.

4. Enter the mail server to which you want to relay mail in the To text box.

5. Click Add to List.

Response: The information you entered appears in the From Mail Server or Domain/To Mail Server list.

You can establish more than one "To" mail server for each "From" mail server or domain in the list. To do so, repeat steps 4 and 5. WebShield SMTP will use the first "To" mail server in the list in its first attempt to relay mail. If that connection fails, WebShield SMTP will relay the mail to the next "To" mail server in the list. If the connections fail to all the "To" servers you listed, WebShield SMTP will deliver the mail to the "From" server.

6. To remove an entry from the list, select it, then click Remove From List.

7. To more an entry list up or down in the list (which increases or decreases the precedence WebShield SMTP assigns to it), select it, then click Remove From List.

8. Click Send Config in the Servers property page to save the changes you've made, or select another tab or 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 SMTP installation directory. You can view these files to examine the network's mail and virus history.*

Step	Action

1. At the Administration Console click Logs.

   Response: The WebShield SMTP Logs property page appears with the Mail tab on top (see Figure 3-12 on page 52).

Figure 3-12. 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 SMTP mail server (incoming and outgoing) is logged in the MAIL.LOG file. The following information is noted in this log file:

- Date and time of mail received
- Date and time of mail sent
- Sender and recipient's e-mail addresses
- Size of the message
- Webshield SMTP-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 log file:

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

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

MAIL.LOG → mail_(date and time).log

VIRUS.LOG → virus-(date and time).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. To examine the log files, click View mail logs.

7. Click Send Config in the Servers property page to save the changes you've made, or select another property page to further configure WebShield SMTP.

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 Administration Console click the Quarantine property page.

   Response: The WebShield SMTP Quarantine property page (Figure 3-13) appears.

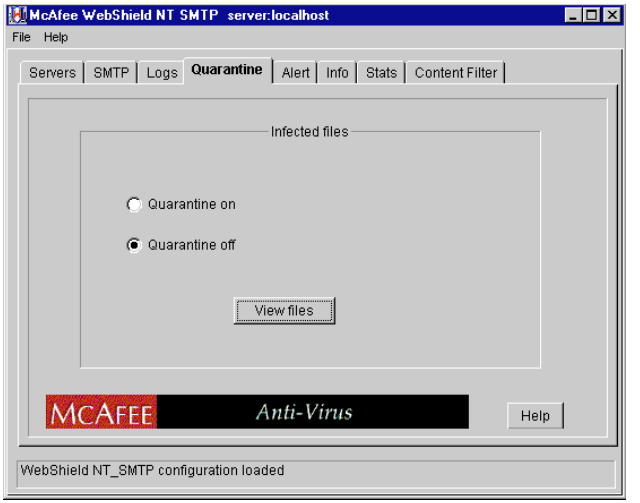

Figure 3-13. WebShield SMTP Administration Console (Quarantine property page)

2. Select Quarantine on if you want WebShield SMTP to automatically quarantine each infected mail it detects, and each mail that caused a scan error. Select Quarantine off if you do not want to use this option.

3. Click Send Config in the Servers property page to save the changes you've made, or select another property page to further configure WebShield SMTP.

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 SMTP 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 3-14) appears.

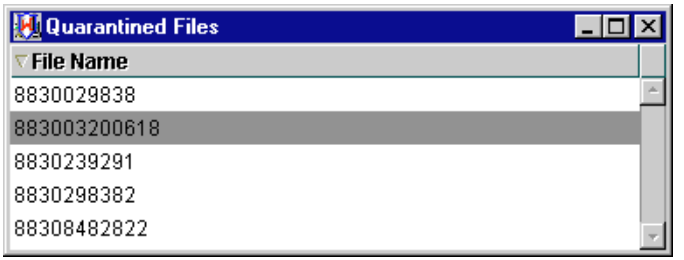

Figure 3-14. Quarantined Files List

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 SMTP's /log directory.*

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

Response: The message appears.

Using the Alert Property Page

Use this property page to direct WebShield SMTP to send an alert message when it detects a mail virus. You can use Webshield SMTP's default message or create your own message. The message can be sent various recipients in your organization via Alert Manager, and to the sender of the infected mail.

Step	Action

1. At the Administration Console click Alert.

Response: The WebShield SMTP Alert property page (Figure 3-15) appears.

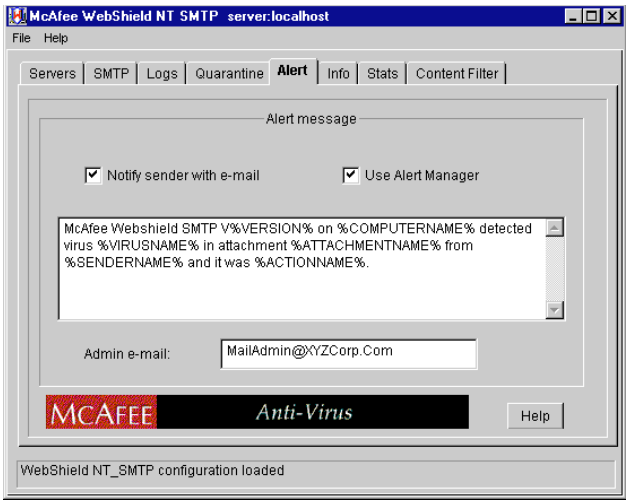

Figure 3-15. WebShield SMTP Administration Console (Alert property page)

2. To send an alert message to the sender of the infected mail, click Notify Sender with E-mail.

3. Enter your mail administrator's e-mail address in the Admin E-mail text box. This address is used as the "author" when WebShield SMTP sends alert messages to senders of infected mail.

4. To send an alert message within your organization, click Use Alert Manager.

   ✍ *In addition to choosing the Use Alert Manager checkbox, you must configure Alert Manager if you want this message to be forwarded to people in your organization. The message can be forwarded through a variety of methods, including e-mail, pager, fax and printer. To configure Alert Manager see* *"Using Alert Manager" on page 62**.*

5. A default alert message appears in the text box. The default message uses six message variables that provide details about the virus detection:

   - **%VERSION%.** Displays the version number of the WebShield SMTP software you are using.
   - **%COMPUTERNAME%.** Displays the name of the computer where WebShield SMTP was running when it detected a virus.
   - **%VIRUSNAME%.** Displays the name of the virus that was detected.
   - **%ATTACHMENTNAME%.** Displays the name of the attachment in which the virus was found.
   - **%SENDERNAME%.** Displays the name of the person who sent the infected mail.
   - **%ACTIONNAME%.** Displays the action WebShield SMTP took (cleaned, deleted, quarantined, etc.) after finding the virus.

6. You can customize the alert message by editing the default message or deleting it and entering your own message. You can incorporate any of the six message variables into the message you create.

7. Click Send Config in the Servers property page to save the changes you've made, or select another property page to further configure WebShield SMTP.

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.

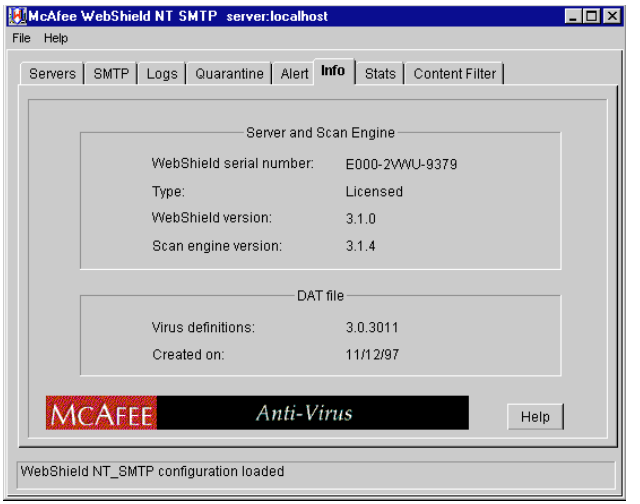

Figure 3-16. WebShield SMTP Administration Console (Info property page)

✍ *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 3-17) 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. This report is automatically updated when the Stats property page is opened, and every five seconds thereafter.

Click Stats in the Administration Console to view this information (Figure 3-17).

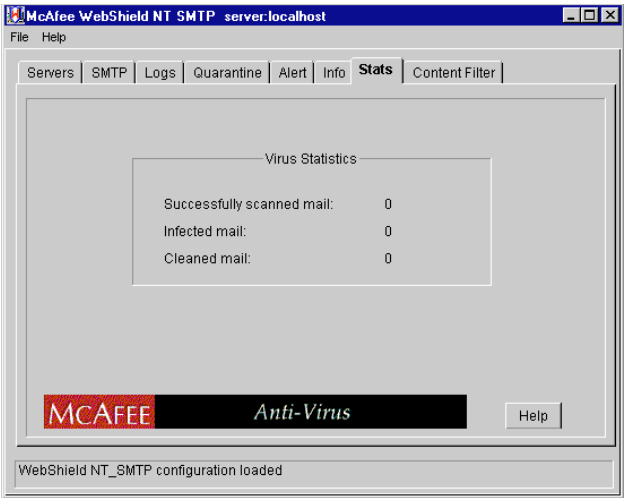

Figure 3-17. WebShield SMTP Administration Console (Statistics property page)

Using the Content Filter Property Page

Use this property page to search mail for content. You can search the body or the header of each mail message that passes through the mail server. WebShield SMTP will copy any mail file that contains the word, or string of words, you are searching for. Follow these steps:

Step	Action

1. At the Administration Console click Content Filter.

Response: The WebShield SMTP Content Filter property page appears (Figure 3-18).

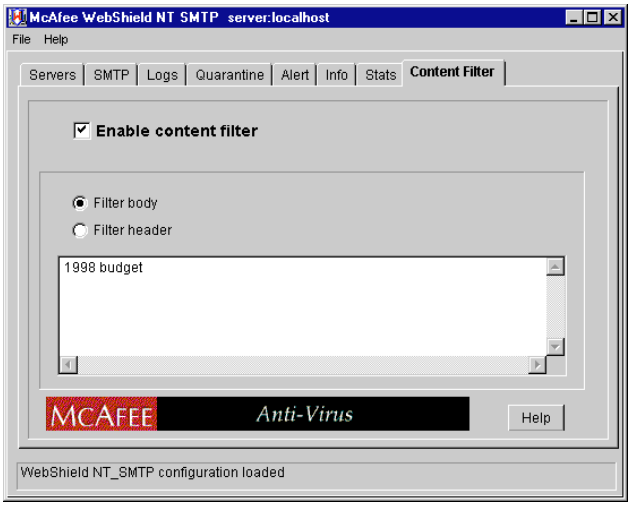

Figure 3-18. WebShield SMTP Administration Console (Content Filter page)

2. Click Enable Content Filter.

3. Enter the word, or string of words, you want WebShield SMTP to search for in the text box. When WebShield SMTP finds this text within a mail message, it stores a copy of the message in the WebShield SMTP subdirectory: \FILTER.

4. Click Send Config in the Servers property page to save the changes you've made, or select another property page to further configure WebShield SMTP.

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 Windows NT 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 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 Level. ▪ 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 Level.

   - 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 Mail Settings, then enter the server name and login name. Click OK.

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 Level.

   - 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 Settings, then enter the settings you want to use and click OK.
8.	To test the pager, click Test.

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

   - 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 Settings, then enter the settings you want to use and click OK.

9. To test the pager, click Test.

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

    - 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 and select a printer from the list that appears. Click OK.

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 Level.

   - 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 Traps checkbox.
4.	To configure SNMP services, click Configure SNMP. **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 website.** 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 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

A

Action Tab 37–39
Administration Console
  Alert Property Page 56–57
  Configuration Tab 40
  Content Filter Property Page 60–61
  Info Property Page 58
  Logs Property Page 51–53
  port settings 40
  property pages described 31–32
  Quarantine Property Page 54–55
  Servers Property Page 32–34
  SMTP Property Page 34–51
    Action Tab 37–39
    Block Tab 45–46
    DNS Tab 42–43
    Exclude Recipient Tab 41–42
    Exclude Sender Tab 43–44
    Ports Tab 39–41
    Relay Tab 47–51
    Scan Tab 36–37
    tabs described 34
  starting 30
  Stats Property Page 59
Alert Manager 62
  e-mail page 66
  forward page 64
  network message page 65
  pager page 68
  printer page 70
  summary page 63
Alert options 62
Alert Property Page 56–57
alphanumeric pager 68

B

Block Tab 45–46
Bulletin Board System (BBS) 8

C

compressed files, scanning 7
configuration
  DNS 25
  from a remote computer 27–28
  port settings 17, 40
  running WebShield SMTP and a mail server on one computer 16–24
    Microsoft Exchange 17–24
  running WebShield SMTP and a mail server on separate computers 25–27
  server settings 32–34
Content Filter Property Page 60–61
Customer Care, contacting 8
customer service 8

D

Data (.DAT) file, updating 73
DNS Tab 42–43
DNS, spelled out 25

E

electronic services
- McAfee BBS 74
- McAfee FTP server 74
- McAfee website 74

Exclude Recipient Tab 41–42
Exclude Sender Tab 43–44

F

features 7

H

hardware requirements 12

I

Info Property Page 58
installation 12–29
- post installation configuration 16–29
- procedure 13–15

J

Java Runtime Environment, where to obtain it 12

L

logging
- mail log 51
- MAIL.LOG 53
- virus log 51
- VIRUS.LOG 53

Logs Property Page 51–53

M

McAfee
- consulting 80
- contacting
  - BBS 8
  - Customer Care 8
  - outside the United States 10
  - via America Online 8
  - via CompuServe 8
  - within the United States 9
- customer service programs 77
- enterprise support 81
- Jump Start program 81
- professional services programs 80
- support services 76
- training 9, 80

Microsoft Exchange
- using it on the same computer as WebShield SMTP 17–24

N

notification 62
numeric pager 69

P

pager
- alphanumeric 68
- numeric 69

Ports Tab 39–41
processing capacity, increasing WebShield SMTP's 28–29

Q

Quarantine Property Page 54–55
Quarantine, enabling 54–55
Quarantine, viewing a file 55

R

Relay Tab 47–51
reporting new virus strains 75
rotating log files 51

S

Scan Tab 36–37
scanning
  allowing selected mail to go unscanned 41–42, 43–44
  scan settings 36
Servers Property Page 32–34
SMTP
  spelled out 6
SMTP Property Page 34–51
  tabs described 34
statistics
  mail 59
  viewing 59
  virus 59
Stats Property Page 59

T

technical support
  e-mail address 8
  information needed from user 9
  McAfee Bulletin Board System (BBS) 8
  online 8
training for McAfee products
  scheduling it 9
trusted clients, registering them 27–28

U

updating
  .DAT files 73
  definition 73
  methods 74
upgrade, definition 73

V

version numbers
  engine, verifying 58
  virus definition files, verifying 58
virus
  notification 62
  reporting a new 75

W

WebShield SMTP
  action settings 37
  increasing its processing capacity 28–29
  installing it 12–29
  introducing 6
  reporting items not detected 75
  scan settings 36
  shutting it down 61
  system requirements 12
  updating it 73
  updating methods 74
  what is WebShield SMTP? 6
  why use it? 6