User's Guide

WebShield LX

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

TRADEMARK NOTICES

McAfee, McAfee Associates, VirusScan, NetShield, and Site Meter are registered trademarks of McAfee 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 McAfee 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.

“SABRE” is a trademark of American Airlines, Inc. and is licensed for use to McAfee. 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 September 1997 / WebShield v1.2.0

Table of Contents

1 Introducing WebShield

What is WebShield?

WebShield is a comprehensive solution for virus protection at the Internet gateway. WebShield scans all inbound and outbound SMTP, FTP, and HTTP file transfers for viruses, protecting your network from harmful infections. Using the HTML-based WebShield Administration Console, you can remotely configure and maintain WebShield from a designated trusted host.

Main features

- Scans electronic mail (SMTP), file transfers (FTP) and World Wide Web (HTTP) traffic at the Internet gateway
- Transparent operation, no network changes necessary
- Offers secure remote management through an intuitive Web-based interface
- Provides dedicated operating system and virus scanning software for Intel architecture-based PCs
- Allows for filtering of potentially harmful Java applets
- Offers a quarantine option for infected files and e-mail messages
- Provides custom virus notification options for all scanning services
- Can use dual disk drives to optimize performance: one for file spooling and scanning, the other for WebShield and the operating system

How To Contact Us

Customer service

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

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

Technical support

McAfee is famous for its dedication to customer satisfaction. McAfee has continued this tradition by investing considerable time and effort to make our website a valuable resource for updating McAfee software and obtaining the latest news and information. For technical support information and issues, we encourage you to visit our website first.

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

If you do not find what you need or do not have access to the Web, try one of McAfee's automated services.

Automated Voice and Fax Response System	(408) 988-3034 24 hours
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
Microsoft Network (MSN)	MCAFEE

If the automated services did not solve your problem, you may contact McAfee Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time at one of the following numbers:

For corporate-licensed users:

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

For retail-licensed users:

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

To speed the process of helping you use our products, please note the following before you call:

- Product name and version
- Computer brand, model, and any additional hardware
- Network type and version
- Specific steps to reproduce the problem, if applicable

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
178 Main Street
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: (0) 31 20 586 6100
Fax: (0) 31 20 586 6101

McAfee France S.A.
50 rue de Londres
75008 Paris
France
Phone: 33 1 44 908733
Fax: 33 1 45 227554

McAfee Deutschland GmbH
Industriestrasse 1
D-82110 Germering
Germany
Phone: 49 89 8943560
Fax: 49 89 89435699

McAfee (UK) Ltd.
Hayley House, London Road
Bracknell, Berkshire
RG12 2TH
United Kingdom
Phone: 44 1344 304730
Fax: 44 1344 306902

McAfee Japan KK
4F Toranomon Mori Bldg. 33
3-8-12 Toranomon
Minato-Ku, Tokyo, 105
Japan
Phone: 81 3 3435 8246
Fax: 81 3 3435 1349

2 Installing WebShield

Before You Start

Please review the requirements outlined in this section before beginning the WebShield installation procedure.

Required network topology

The WebShield system must reside at a choke point at your network. If your network contains any alternate routes that allow traffic to bypass the WebShield system, WebShield may fail to function.

The WebShield system requires its own IP address. It does *not* replace your router, and no routes should point to it.

Required hardware

McAfee recommends the base configuration below as a starting point for a T-1 (1.5Mbps) Internet connection.

If the hardware you want to use is not listed here, please contact McAfee Technical Support or your McAfee sales representative before installing WebShield to ensure McAfee supports your hardware configuration.

✍ *For optimal performance, McAfee strongly recommends using all PCI devices.*

- Pentium 166 or better

- 32MB RAM
- One 2GB or larger disk drive, or
- For dual drive systems, one 2GB or larger disk drive and one 500MB or larger disk drive
- IDE or SCSI CD-ROM drive
- Two Network Interface Cards from the following list:
  - DEC DE 500 cards
  - Adaptec ANA-6901 or ANA-6911 cards
  - Other cards based on the DEC 21x4x series of chips
  - Western Digital 8013-based cards
  - AMD Lance cards
  - 3Com 3c509b cards
- An IDE adapter or a SCSI adapter from the following list:
  - BusLogic 445, 542, 545, 946, 948, 956, 958

    ✍ *McAfee recommends the BusLogic cards listed above.*
  - Adaptec 1542, 2940, and compatible

    ✍ *Adaptec SCSI controllers are sensitive to cable problems. If you have drive problems with these cards, reseat all the disk system components to ensure there are no bad connections.*
  - NCR 810-based cards

✍ *Sites with larger Internet connections, such as T-3s (45Mbps), should measure the amount of traffic permitted through their firewalls as opposed to traffic that is accessing a popular external Web server. WebShield can be configured in multiple serial systems. Therefore, system-1 could scan SMTP transfers while system-2 was scanning FTP and HTTP traffic.*

An up-to-date list of supported hardware can be obtained through McAfee's Automated Voice and Fax Response System. See "How To Contact Us" on page 6.

Required information

During the installation process, you will be asked to provide the details of your network configuration. For successful installation of the product, please gather the following data before proceeding:

- Host name
- Company-assigned domain name
- Company-assigned IP address

  ✍ *You need to provide the IP address for connection to the internal network. This address will be used for the internal connection only. The external connection does not have an IP address.*

- Trusted host

  ✍ *The trusted host is the system used for WebShield management and configuration, as well as logging of data. If you wish to use the UNIX syslog utility to remotely collect your WebShield logs, the trusted host must be a UNIX system.*

- Company name
- WebShield Administrator's e-mail address

  ✍ *The person at this address can receive WebShield alert notifications.*

- IP gateway (If using an interior gateway)
- Mail relay address

  ✍ *The mail relay must reside on the internal network.*

- Domain name server

  ✍ *This DNS must reside on the internal network for optimum WebShield performance. If your DNS is external, WebShield will function but will not provide host names in logs and alert notifications.*

- Network, Broadcast address, and Netmask

  ✍ *Network, Broadcast address, and Netmask are required only if your organization uses non-standard settings. WebShield will automatically generate standard default settings.*

- Time zone

Installation Procedure

WebShield is intended to scan all FTP, SMTP, and HTTP traffic entering and leaving a local area network (LAN). WebShield uses two network interfaces—an “external” interface and an “internal” interface. WebShield attempts to assign the interfaces at boot time by probing the network for the trusted host. If, after following the installation procedures outlined below, your WebShield system does not appear to work, McAfee recommends that you try to correct the problem by switching the network interface cables and rebooting.

To install WebShield, carefully follow the procedure outlined below. To move from item to item on the installation screens, use the Tab key on your keyboard.

Step	Action
1.	With the computer turned off, insert the WebShield installation diskette into your floppy disk drive and place the WebShield compact disc into the CD-ROM drive.
2.	Start the computer. **Response**: The initial WebShield screen is displayed, verifying that you would like to begin the installation procedure and overwrite the data on the system’s hard disk drive. Select Yes to continue. ✍ *Selecting Yes will erase any information stored on this system’s hard disk drive. To cancel the installation, select No.*

3. Review the license agreement and product information, using the arrow keys or PAGE UP and PAGE DOWN to scroll up and down, and select Accept to continue with the installation procedure.

   Response: WebShield data is transferred to the hard drive.

4. The memory detection confirmation screen is displayed. If the amount of RAM automatically detected is correct, select Yes. If the amount is not correct, select No and you will have the opportunity to enter the correct amount.

   ✍ *The amount of RAM WebShield detects may be lower than the actual amount installed in the system by one or two megabytes. This is because some memory is reserved for system use. Similarly, if you manually enter the amount of memory available, you should under-report it by one or two megabytes to leave some memory for system use.*

5. When prompted, remove the WebShield installation floppy diskette. To continue the installation, select OK.

6. Do one of the following:

   - If you are installing to a machine with two hard disks, continue with step 6.
   - If you are installing to a single hard disk machine, continue with step 7.

   Response: The Set Up Variable Filesystem screen is displayed.

7. Select a method for partitioning your system.

   - To use WebShield default partitioning, highlight Use WebShield Defaults and select OK. You will be asked to confirm your selection.
   - To partition manually, highlight Customize Disk Layout and select OK. You may wish to partition manually if you are familiar with Linux.
   - To use existing partitions, highlight Use Existing Layout and select OK. You may wish to use existing partitions if you are upgrading the WebShield machine.

     ✍ *McAfee strongly recommends the default partitioning method.*

8. When partitioning and data transfer are complete, select OK to continue.

   Response: The WebShield Configuration Screen is displayed.

9. Enter the following data into the form provided:

   - Host name
   - Company domain name
   - Company-assigned IP address
   - Trusted host
   - Company
   - WebShield Administrator e-mail address

10. At the bottom of the WebShield Configuration Screen, click Network.

Response: The Network Configuration Screen is displayed.

✍ *The Network, Broadcast address, and Netmask are generated automatically. If your organization uses non-standard settings, you should change these defaults to the proper settings.*

11. Enter the Domain Name Server and Mail Relay Address. Review the default settings, and click OK.

12. Click Time Zone.

Response: The Time Zone screen is displayed.

13. Select your time zone from the list provided, and press ENTER to return to the WebShield Configuration Screen.

14. Click Logging.

Response: The System Logging Screen is displayed, with the following options listed:

- **Disk**, which will log data to the local system. These logs reside in /var/log and can be viewed using the WebShield Administration Console.
- **Console**, which will log data to an alternate console on the host. This alternate console can be accessed by pressing ALT+F7 on the keyboard. To exit the alternate console, press ALT+F1.
- **Trust**, which will log data to a UNIX trusted host.

✍ *By default, Disk and Console are selected.*

Action: Make any necessary changes to the logging configuration by highlighting the desired option and pressing the Spacebar.

15. Click OK.

Response: The Review Current Settings screen is displayed.

Action: To return to the WebShield Configuration Screen and make changes, press ESC. Press ENTER to accept settings.

Response: WebShield is installed and running.

When WebShield installation is complete, you should change the root password, which is used for both the WebShield system and the HTML-based WebShield Administration Console.

✍ *The default password is* `webshield`.

The root password can be changed remotely using the Administration Console. See "Set administrative password" on page 23 for details. To change this password directly from the WebShield machine, see "Changing the root password" on page 54.

After installation, WebShield is configured and managed remotely through the WebShield Administration Console. See "Using the WebShield Administration Console" on page 17. To configure your system using the command-line interface, see "Using the command-line interface" on page 54.

3 Using WebShield

Using the WebShield Administration Console

After initial installation, all WebShield configuration and management is handled from the trusted host, through the HTML-based WebShield Administration Console (Figure 3-1). WebShield offers Plain and Frames-based interfaces with which you can customize and manage your configuration settings.

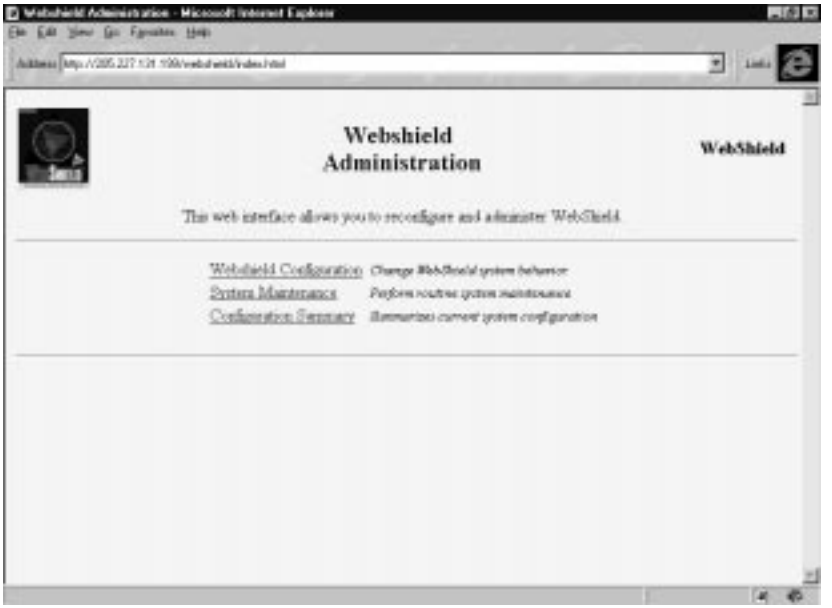

Figure 3-1. WebShield Administration Console Page

This chapter outlines the options that are available using the console and details how to configure your software. For instructions on using the command-line interface see Chapter 4, “Advanced Configuration.”

From the WebShield Administration Console, you can link to three configuration and management control panels. Using the forms provided in these control panels, you can customize, manage, and maintain all aspects of WebShield. The control panels include:

- **WebShield Configuration**, which allows you to customize your virus scanning and notification options, logging settings, system identity, and system management. To customize these options, see “Using the Configuration Menu” on page 22.

- **WebShield System Maintenance**, which is used to upgrade WebShield; update WebShield’s virus definition data; export and restore configurations, quarantined files, and logs; view the log files; and shutdown or restart the WebShield system. To perform these actions, see “Using the System Maintenance Menu” on page 38.

- **Configuration Summary**, which provides a detailed summary of your current WebShield settings and policies. To review your settings, see “Viewing the configuration summary” on page 53.

Using the non-graphical administration tool

For direct configuration and management, a non-graphical administration tool is also available. This tool operates in much the same way as its HTML-based equivalent, and can be used to configure and manage your WebShield settings, including passwords and system shutdown. The company name and time zone can be set only during installation or by using this interface.

To administer WebShield from a non-graphical interface, log in to WebShield directly or from an internal machine using telnet or rsh/rlogin.

✍ *The path to the non-graphical administration tool is /usr/sbin/wsadm.*

✍ *The default password is* `webshield`*. If you have not yet changed this password, McAfee recommends that you change it now. See* *"Set administrative password" on page 23**. To change the password from the command line, see* *"Changing the root password" on page 54* *for more information.*

Starting the Administration Console

The WebShield Administration Console can be accessed from the trusted host, which was named during the installation process. To start the Console, take the following steps:

Step	Action

1. Start your browser.

2. Type:

   `http://<IP address>`

   where `<IP address>` is the address of your WebShield machine.

3. Press ENTER.

   Response: The login screen is displayed.

   ✍ *McAfee recommends that you use your browser to bookmark this page for easier access later.*

4. From the login screen, click Plain Interface to view the WebShield Administration Console, or click Frames-based to view the WebShield Administration Console with frames.

   ✍ *The Frames-based option requires an HTML 3.2-compatible web browser.*

5. At the password prompt, enter user name and WebShield root password.

✍ *The default password is* `webshield`*. If you have not yet changed this password, McAfee recommends that you change it now. See* *"Set administrative password" on page 23**. To change the password from the command-line, see* *"Changing the root password" on page 54* *for more information.*

Response: The WebShield Administration console is displayed (Figure 3-2).

Using the Configuration Menu

To access the WebShield Configuration menu (Figure 3-2), start the Administration Console and click WebShield Configuration.

Figure 3-2. WebShield Configuration Menu

From this menu, you can customize the following WebShield settings and policies:

- Set Administrative Password
- Remote Management
- Virus Scanning
- Virus Resolution
- Logging
- Notification
- System Identity

Set administrative password

Using this form (Figure 3-3), you can change the password used to access both the WebShield machine and this Administration Console. This password can also be changed from the WebShield machine, as described in "Changing the root password" on page 54.

Figure 3-3. Set WebShield Administrative Password Control Panel

To change the password, take the following steps:

Step	Action
1.	Enter your current password in the space provided.
2.	Enter a new password, then enter it again for confirmation.
3.	To save the settings, click Accept Changes. To disregard new settings, click Clear Changes.

Remote management

The WebShield Remote Management Control Panel (Figure 3-4) allows you to change the ways in which WebShield is configured and managed.

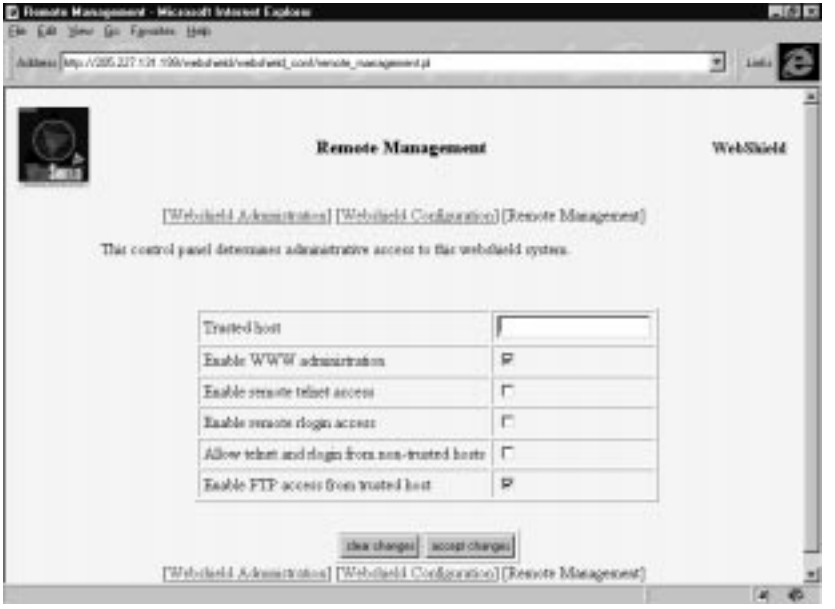

Figure 3-4. WebShield Remote Management Control Panel

Take the following steps to configure your remote management policies.

Step	Action
1.	Start the Administration Console, select WebShield Configuration, and click Remote Management. **Response**: The WebShield Remote Management Control Panel is displayed.

2. To change the trusted host, enter a new IP address in the space provided.

   ✍ *The trusted host is the system used for WebShield management and configuration, as well as logging of data. If you wish to use the UNIX syslog utility to remotely collect your WebShield logs, the trusted host must be a UNIX system.*

3. Select which remote administration modes you want to use for WebShield configuration and management.

   - If you want to use this HTML-based WebShield Administration Console, select the Enable WWW Administration checkbox.
   - If you want to use telnet to access the WebShield system, select the Enable Remote Telnet Access checkbox.
   - If you want to use the rlogin facility to access the WebShield system, select the Enable Remote Rlogin Access checkbox.
   - If you want to ftp from a trusted host to directly access files on the WebShield system, select the Enable FTP Access from Trusted Host checkbox.
   - If you wish to allow remote access to WebShield from hosts other than the trusted host, select the Allow Remote Access from Non-trusted Hosts checkbox.

4. To save the settings, click Accept Changes.

   Response: A confirmation screen is displayed, and WebShield's remote management settings are updated to reflect your changes.

   To disregard new settings, click Clear Changes.

Virus scanning

The main services that lead to the spread of viruses are electronic mail, file transfers, and web browsing communications. Use the WebShield Virus Scanning Control Panel (Figure 3-5) to customize WebShield's scanning options and protect your system while on the Internet and other TCP/IP-based networks.

✍ *WebShield supports the following archiving and encoding formats: GZIP, MIME, LZEXE, PKLITE, TAR, UUENCODE, ZIP, and ZOO.*

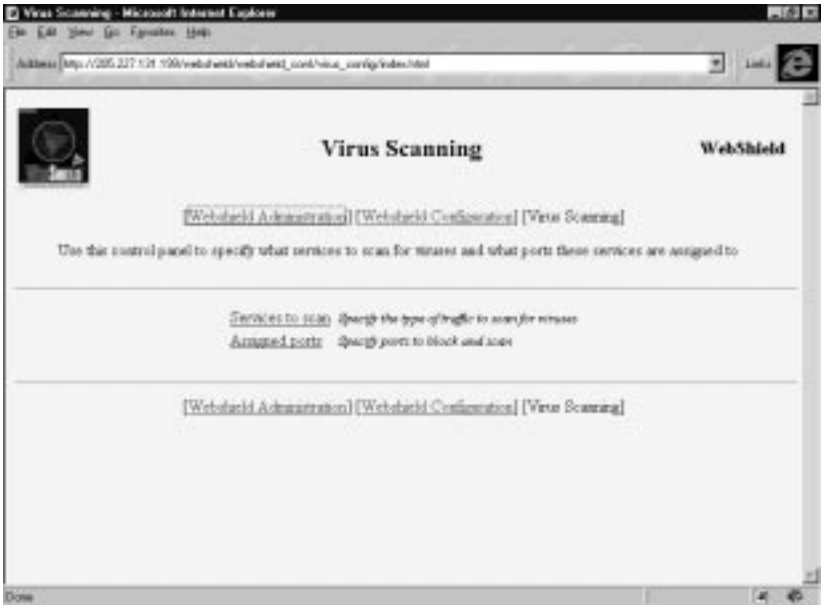

Figure 3-5. WebShield Virus Scanning Control Panel

Take the following steps to customize your scanning options:

Step	Action
1.	Start the Administration Console, select WebShield Configuration, and click on Virus Scanning.
	Response: The WebShield Virus Scanning Control Panel is displayed.

2. To customize your scanning options, click Services to Scan.

   Response: The Services to Scan Control Panel is displayed.

3. Select your general scanning policies. For maximum security all items should be ON.

   ✍ *Because of the nature of encryption, WebShield cannot scan encrypted files. McAfee recommends running VirusScan in conjuction with WebShield for complete virus protection.*

   - **Disable Execution of Java Binaries**: Check this box if you want to disable the transmission of Java applets. By default, WebShield filters Java applets, which may disclose confidential data or contain viruses.
   - **Scan Outgoing FTP and WWW Traffic for Viruses**: Check this box if you want WebShield to scan outbound FTP and WWW traffic to prevent infections from spreading from your local network.
   - **Scan Incoming Mail for Viruses**: Check this box if you want WebShield to scan incoming mail for viruses.
   - **Scan Outgoing Mail for Viruses**: Check this box if you want WebShield to scan outgoing mail for viruses.
   - **Scan Incoming WWW Traffic for Viruses**: Check this box if you want WebShield to scan World Wide Web traffic.
   - **Scan Incoming FTP Traffic for Viruses**: Check this box if you want WebShield to scan FTP traffic

4. To save the settings, click Accept Changes.

   Response: A confirmation screen is displayed, and WebShield's virus scanning policies are updated to reflect your changes.

   To disregard new settings, click Clear Changes.

5. Select Assigned Ports from the Virus Scanning Control Panel to determine which ports to scan for possible virus transmissions.

   Response: The Assigned Ports Control Panel is displayed.

6. To deny connections to any port, enter the port number or range in the Deny Connections box.

   ✍ *Separate individual ports with commas. Designate a port range with a dash. For example, to block all ports from 1 to 10 and port 15, enter* `1-10,15` *in the Deny Connections box.*

7. Enter the SMTP, FTP, and WWW port numbers and port ranges you want to scan for possible virus transmissions in the appropriate boxes.

8. To save the settings, click Accept Changes.

Virus resolution

The WebShield Virus Resolution Control Panel (Figure 3-6) allows you to configure the actions WebShield should take when a virus is detected during a transfer.

Figure 3-6. WebShield Virus Resolution Control Panel

Take the following steps to configure your policies for virus resolution:

Step	Action
1.	Start the Administration Console, select Webshield Configuration, and click Virus Resolution. **Response**: The WebShield Virus Resolution Control Panel is displayed (Figure 3-6).

2. Select an action for WebShield to take upon virus detection:

   - **Allow Transfers of Infected Documents:** If you want to allow the document to transfer but notify the user that it is infected, select this checkbox.

     ✍ *Some Web browsers and FTP clients do not properly notify the user when a virus is detected. When such a browser or FTP client is being used and a virus is detected, the file will not be transferred, but the user may receive a blank Web page or a 0-byte file.*

   - **Preserve Infected Mail Messages:** If you want to quarantine infected mail messages, select this checkbox.

   - **Preserve Infected FTP Documents:** If you want to quarantine infected FTP documents, select this checkbox.

   - **Preserve Infected WWW Pages:** If you want to quarantine infected WWW files, select this checkbox.

   - **Notify the WebShield Administrator when Viruses are Discovered:** If you want your WebShield Administrator to receive a notification message when WebShield discovers a virus, select this checkbox.

3. When a virus is discovered, a summary log entry is generated automatically. You can configure WebShield to save the suspect file in quarantine on the WebShield machine for later retrieval.

4. To save the settings, click Accept Changes.

   Response: A confirmation screen is displayed, and WebShield's virus scanning policies are updated to reflect your changes.

   To disregard new settings, click Clear Changes.

Logging

The WebShield Virus Logging Control Panel (Figure 3-7) allows you to customize your logging setup to meet your network's needs.

Figure 3-7. WebShield Virus Logging Control Panel

Take the following steps to configure WebShield's log files:

Step	Action
1.	Start the Administration Console, select WebShield Configuration, and click Logging.
	Response: The WebShield Virus Logging Control Panel is displayed.

2. Select where you want WebShield to log data:

   - If you want to log data to the local system, select the Log to Local Disk in /var/log/messages checkbox. These logs can be viewed using the WebShield Administration Console.

   - If you want to log data to an alternate console on the host, select the Log to Alternate Console Host checkbox. This alternate console can be accessed by pressing ALT+F7 on the WebShield keyboard. To exit the alternate console press ALT+F1.

   - If you want to log data to a UNIX trusted host, select the Log to Trusted Host checkbox.

     ✍ *Data cannot be logged to a Windows 95 or Windows NT trusted host.*

3. You can log all transfers passing through WebShield, regardless of whether they are infected. If you wish to activate this option, check the Log All Data Transfers Passing Through WebShield checkbox.

4. WebShield can notify the WebShield Administrator when files are deleted. If you want the Administrator to receive an e-mail notification, select the appropriate checkbox.

5. Select how often WebShield logs should be rotated by entering a number of days between log file rotations.

   ✍ *By rotating the logs frequently, you reduce the size of the log files and make them more accessible for viewing.*

6. Indicate the number of days to keep the log files by entering a number of days between log removal.

7. WebShield will store infected files for a specified number of days. Indicate the number of days to keep infected files by entering a number of days between file removal.

8. To save the settings, click Accept Changes.

Response: A confirmation screen is displayed, and WebShield's virus logging policies are updated to reflect your changes.

To disregard new settings, click Clear Changes.

Notifications

The WebShield Notification Control Panels are used to customize the messages WebShield sends when it detects a virus. The FTP Virus Notification Control Panel is shown below (Figure 3-8).

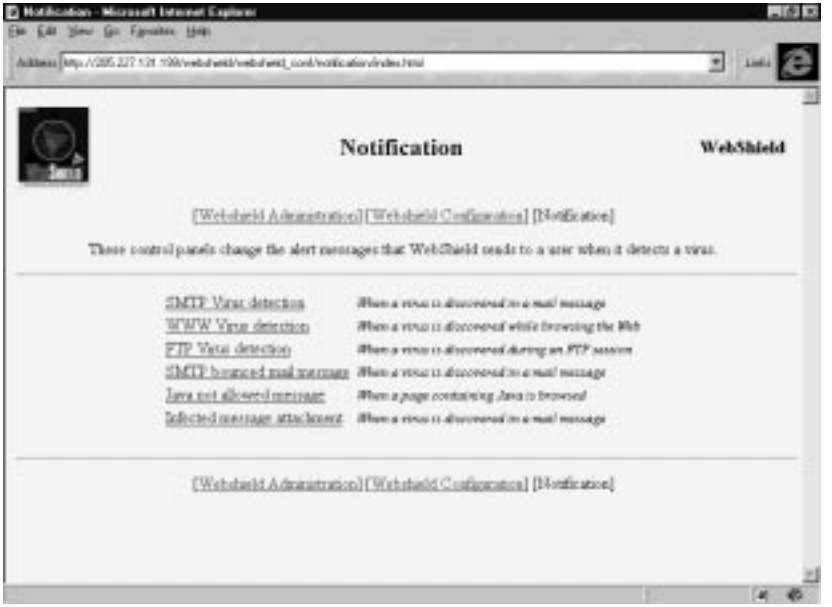

Figure 3-8. FTP Virus Notification Control Panel

Using these notification forms and the set of metacharacters described in this section, you can customize messages to be sent upon virus detection.

- **SMTP Virus Detection**: When WebShield detects a virus in electronic mail, it can notify the intended recipient.
- **WWW Virus Detection**: When a virus is detected while browsing the Web, WebShield can notify the browser attempting to access the site.
- **FTP Virus Detection**: When WebShield detects a virus in an FTP transfer, it can notify the client attempting to download.
- **SMTP Bounce Mail Message**: When WebShield detects a virus in electronic mail, it can notify the sender.
- **Java Not Allowed Message**: When a Java applet is detected while browsing the Web, WebShield can notify the browser.
- **Infected Message Attachment:** When a virus is detected in a mail message attachment, it can notify the intended recipient.

✍ *If you selected the WebShield Administrator notification option from the Virus Resolution Control Panel, the Administrator also will be notified.*

To customize these messages, take the following steps:

Step	Action
1.	Start the Administration Console, select WebShield Configuration, and click Notifications. **Response**: The WebShield Notification Menu is displayed.
2.	Select a session type. **Response**: A notifications form is displayed, including a list of metacharacters and their definitions.

3. Metacharacters are shortcut symbols WebShield uses to send automated e-mail messages. If you enter these metacharacters into the forms provided, WebShield will replace the symbol with the appropriate text when it sends notifications. Review the metacharacters below:

   - %a = WebShield Administrator's e-mail address
   - %v = Name of detected virus
   - %f = File or URL being transferred
   - %i = Path to infected file on WebShield machine
   - %s = Company name

4. Use the metacharacters and forms provided to write customized messages. Header information is automatically generated.

5. As you update the message for each type of transfer, click the Accept Changes button on that form to save the changes.

   Response: A confirmation screen is displayed, and the WebShield notification settings are updated.

System identity

The WebShield System Identity Control Panel (Figure 3-9) allows you to reconfigure WebShield's system identity after the initial installation.

Figure 3-9. WebShield System Identity Control Panel

To change these settings, take the following steps:

Step	Action
1.	Start the Administration Console, select WebShield Configuration, and click System Identity. **Response**: The WebShield System Identity Control Panel is displayed.
2.	Make any necessary changes.
3.	To save the settings, click Accept Changes. To disregard new settings, click Clear Changes.

Using the System Maintenance Menu

To access the WebShield System Maintenance Menu, start the Administration Console and click System Maintenance. From this menu, you can perform the following actions:

- View Current Log
- Export Log Files
- Rotate Log Files
- Export Quarantined Files
- Update Virus Identification
- Export Configuration
- Restore Configuration
- Upgrade WebShield
- Restart System
- Shutdown System

Viewing the current log file

You can view the current log file from the trusted host, using this page.

To view the WebShield System Log file, take the following steps:

Step	Action
1.	Start the Administration Console and select System Maintenance. **Response**: The WebShield System Maintenance Menu is displayed.
2.	Click View Current Log. **Response**: The current log file is displayed.

Exporting WebShield system log files

Using this page, you can export your WebShield log files to another system on the network for safekeeping. To complete this task, take the following steps:

Step	Action
1.	Start the Administration Console and select System Maintenance. **Response**: The WebShield System Maintenance Menu is displayed.
2.	Click Export Log Files. **Response**: The Export Log Files Control Panel is displayed (Figure 3-10 on page 40).

Figure 3-10. Export Log Files Control Panel

3. Select a method for exporting the system log files:

   - **Via FTP to Another System:** To export the log files via FTP to another system, choose this option. Enter the remote system information and password in the form provided.

   - **To a DOS-Formatted Diskette:** To export the log files to a diskette, choose this option. Insert a DOS-formatted diskette into the appropriate drive and enter the drive letter in the Drive box.

   - **To a Directory on the WebShield Machine:** To export the log files to the WebShield machine, choose this option. Enter the file destination directory in the space provided.

   - **As a WWW document:** To export log files through a browser, choose this option.

     ✍ *This option does not export log files as HTML documents.*

4. Select the files you want to export from the Export Log Files menu.

5. Click Export System Log.

   Response: A confirmation screen is displayed, and the WebShield system log file is exported to the target system.

Rotating log files

Using this page, you can rotate the system log files. When rotating the system log files, the current log files are saved and the log screen is cleared.

To view the WebShield Rotate Log File page, take the following steps:

Step	Action

1. Start the Administration Console and select System Maintenance.

   Response: The WebShield System Maintenance Menu is displayed.

2. Click Rotate Log Files.

   Response: The Rotate Log File page is displayed.

3. Click the Rotate Log File button to rotate log files.

Exporting quarantined files

Using this page, you can retrieve files that WebShield has quarantined. To complete this task, take the following steps:

Step	Action

1. Start the Administration Console and select System Maintenance.

   Response: The WebShield System Maintenance Menu is displayed.

2. Click Export Quarantined Files.

   Response: The Export Quarantined File page is displayed (Figure 3-11).

Figure 3-11. Export Quarantined File Control Panel

3. Select a method for exporting the quarantined files:

   - **Via FTP to Another System:** To export quarantined files via FTP to another system, choose this option. Enter the remote system information and password in the form provided.

   - **To a DOS-Formatted Diskette:** To export quarantined files to a diskette, choose this option. Insert a DOS-formatted diskette into the appropriate drive and enter the drive letter in the Drive box.

   - **To a File on the WebShield Machine:** To export quarantined files to the WebShield machine, choose this option. Enter the destination directory in the space provided.

   - A**s a WWW Document:** To export quarantined files through a browser, choose this option.

     ✍ *This option does not export quarantined files as HTML documents.*

4. Select the files you want to export from the Quarantine Files menu.

5. Click Export Files.

Updating virus identification files

Every month more than 200 new viruses enter the worldwide viral pool and put your network at risk. To combat these new viruses, McAfee provides monthly updates to its virus definition data files. Take the following steps to update WebShield's virus identification and protect against new viruses.

Step	Action
1.	Download the current compressed data file from McAfee's website or BBS and save it on a local system. For contact information, see "How To Contact Us" on page 6.
2.	Unzip the file into a directory on the local system.

3. Start the Administration Console and select System Maintenance.

   Response: The WebShield System Maintenance Menu is displayed.

4. Click Update Virus Identification.

   Response: The Update Virus Identification Control Panel is displayed (Figure 3-12).

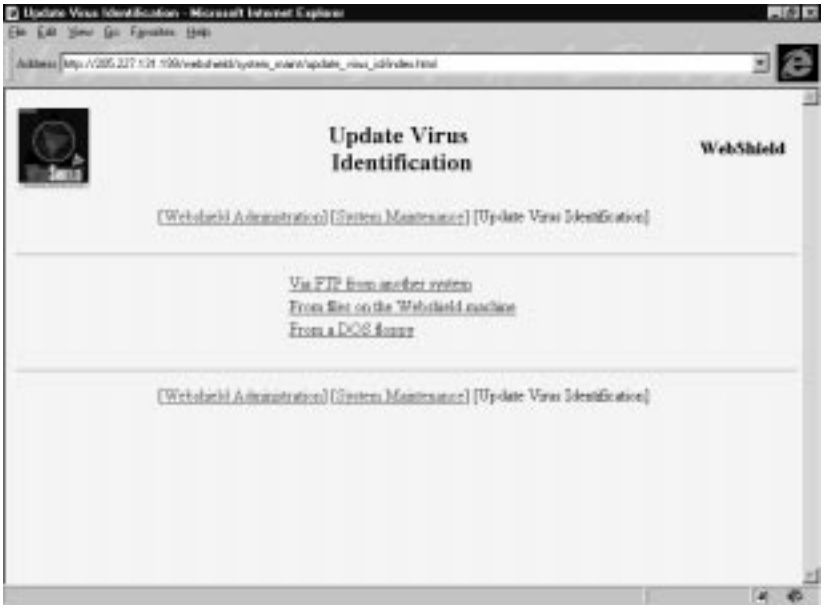

Figure 3-12. Update Virus Identification Control Panel

5. Select the method by which you want to install the update:

   - **FTP Host:** To install the update from an FTP host, choose this option. Enter the remote system information and password.

   - **Local File:** To install the update from a local file, choose this option. Enter the filename and source directory of the file.

6. Click Update Data. A confirmation screen is displayed, and WebShield's virus definition data are updated.

Exporting your configuration file

Using this page, you can export your WebShield configuration file to another machine on the network for safekeeping.

To export your WebShield configuration file, take the following steps.

Step	Action

1. Start the Administration Console and select System Maintenance.

   Response: The WebShield System Maintenance Menu is displayed.

2. Click Export Configuration.

   Response: The Export Configuration Control Panel is displayed (Figure 3-13).

Figure 3-13. Export WebShield Configuration File Control Panel

3. Select a method by which to export configuration files:

   - **Via FTP to Another System:** To export configuration files to another system via FTP, choose this option. Enter the remote system information and password.

   - **To a DOS-formatted Diskette:** To export configuration files to a DOS-formatted diskette, choose this option. Insert a DOS-formatted diskette into the appropriate drive and enter the drive letter in the Drive box.

   - **To a File on the WebShield Machine:** To export configuration files to the WebShield machine, choose this option. In the spaces provided, enter the name of the file to which you want to export the configuration and the destination directory.

   - **As a WWW Document:** To export configuration files through a browser, choose this option.

     ✍ *This option does not export configuration files as HTML documents.*

4. Click Export Files.

   Response: A confirmation screen is displayed, and WebShield's Configuration File is exported, with a filename of `configuration`.

   ✍ *The filename of the exported configuration may be truncated to* `configur` *or* `config~1` *if the operating system to which the configuration was exported does not support long filenames.*

Restoring configuration files

The WebShield Restore Configuration Control Panel is used to restore previously configured files from a saved file.

To restore your WebShield configuration files, take the following steps.

Step	Action

1. Start the Administration Console and select System Maintenance.

   Response: The WebShield System Maintenance Menu is displayed.

2. Click Restore Configuration.

   Response: The Restore Configuration Control Panel is displayed. (Figure 3-10).

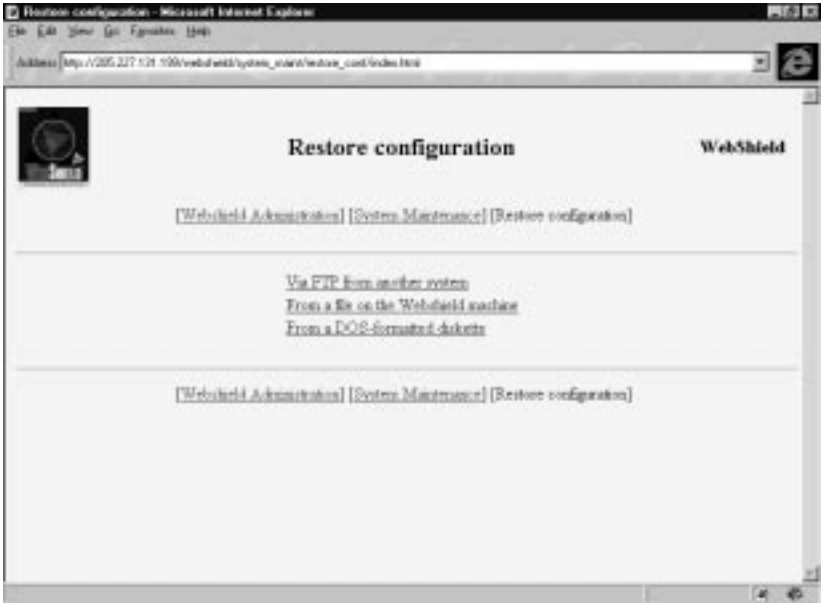

Figure 3-14. Restore Configuration Control Panel

3. Select a method in which to restore configuration files:

   - **From FTP Host:** To import system configuration from FTP host, choose this option. Enter the remote system information and password.

   - **From Local File:** To import system configuration from local file, choose this option. Enter the filename and source directory of the file.

   - **From DOS Floppy Disk:** To import configuration from a DOS floppy disk, choose this option. Insert the DOS floppy diskette into the appropriate drive and enter the filename and drive letter in the appropriate box.

Upgrading WebShield

WebShield can be upgraded by installing software updates listed in this control panel. To upgrade WebShield, follow the instructions outlined below.

Step	Action

1. Start the Administration Console and select System Maintenance.

   Response: The WebShield System Maintenance Menu is displayed.

2. Click Upgrade WebShield.

   Response: The Upgrade WebShield page is displayed (Figure 3-15).

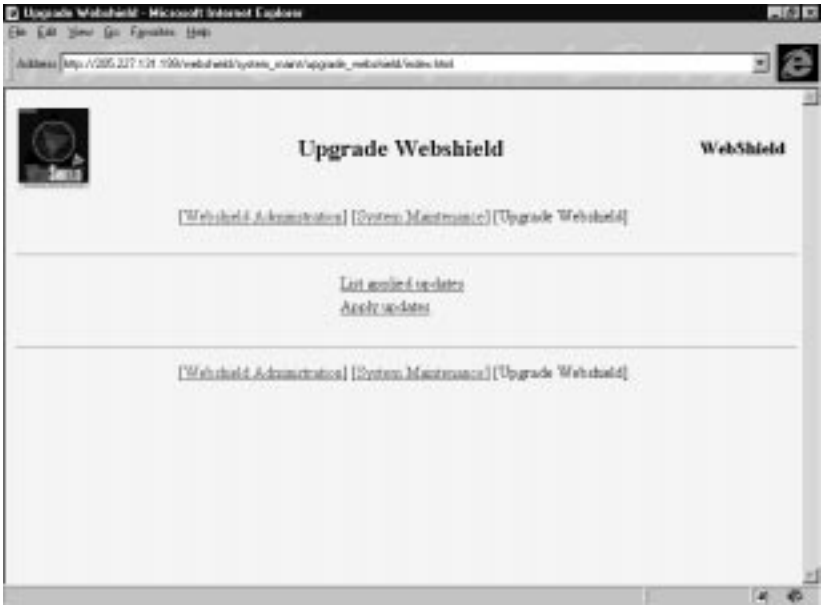

Figure 3-15. Upgrade WebShield Control Panel

3. To view a list of updates already applied, click List Applied Updates.

   Response: A list of applied updates is displayed.

   Action: Click your browser's Back button to return to the main menu.

4. Click Apply Updates.

   Response: The Apply Updates page is displayed.

5. Do one of the following:

   - To install a software update from an FTP host, click Install Update from FTP Host.

     Response: The Install Update from FTP Host page is displayed.

   - To install a software update from a local file, click Install Update from Local File.

     Response: The Install Update from Local File page is displayed.

6. Enter the required information in the spaces provided.

7. To save the settings, click Accept Changes.

   Response: A confirmation screen is displayed, and the updates are installed.

   To disregard new settings, click Clear Changes.

Restarting the WebShield system

In some cases, such as when your network configuration has been changed or when the WebShield trusted host has been changed, it may become necessary to restart the WebShield system. Using the Restart System page from the WebShield System Maintenance Menu (Figure 3-16), you can reboot the WebShield system from the trusted host.

Figure 3-16. WebShield Restart System Control Panel

To reboot the system, take the following steps:

Step	Action
1.	Start the Administration Console and select System Maintenance.
	Response: The WebShield System Maintenance Menu is displayed.

2. Click Reboot Now.

   Response: A confirmation screen is displayed, and the WebShield machine is restarted.

Shutting down WebShield

You may also need to shut down the WebShield system in some instances. Using the System Shutdown Control Panel (Figure 3-17) from the WebShield System Maintenance Menu, you can remotely shut down the WebShield system from the trusted host. To shut down the WebShield system directly, see "Shutting down the WebShield system" on page 55.

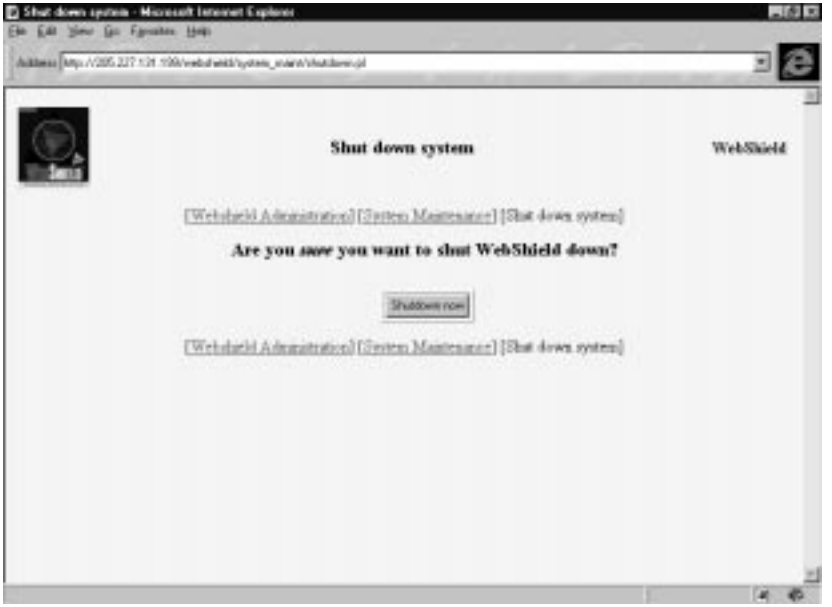

Figure 3-17. WebShield Shut Down System Control Panel

To shut down the system, take the following steps:

1. Start the Administration Console and select System Maintenance.

   Response: The WebShield System Maintenance Menu is displayed.

2. Click Shut Down System.

3. Click Shut Down Now to shut down the WebShield machine.

   ✍ *This will break all connections running through WebShield.*

   Response: A confirmation screen is displayed, and the WebShield machine is shut down.

Viewing the configuration summary

The Configuration Summary page provides an in-depth report of your current WebShield settings and policies. To review your settings using this summary, take the following steps:

Step	Action

1. Start the Administration Console and select Configuration Summary.

   Response: The Configuration Summary is displayed.

2. Review your current WebShield settings.

3. To change settings, go to the appropriate menu within the WebShield Administration Console and make necessary changes. See “Using the WebShield Administration Console” on page 17. As changes are submitted, the Configuration Summary will be updated.

4 Advanced Configuration

Using the command-line interface

Advanced users may prefer working directly from the WebShield machine to using the HTTP-based interface. This chapter provides instructions for changing the root password and shutting down WebShield from a command-line interface.

To administer WebShield from the command-line interface, log in to WebShield directly using ALT+ F2, or from an internal machine.

Changing the root password

To change the root password from the WebShield machine, follow the steps outlined below.

Step	Action
1.	Press ALT+F2 on the WebShield machine. **Response**: A login prompt is displayed.
2.	At the login prompt, enter the user name `root` and default password `webshield`.
3.	Type the command: `passwd` and press ENTER.

4. At the prompt, enter a new password.

5. Enter the password again for verification.

   Response: The root password is changed.

6. Type `exit`.

Shutting down the WebShield system

If it becomes necessary to turn off the WebShield machine, you must first shut down the system.

✍ *You should never turn off the WebShield machine without first following these shutdown procedures. Shutting down the system will break all connections running through WebShield.*

The WebShield system can be shut down or restarted remotely using the WebShield Administration Console. See "Restarting the WebShield system" on page 51 and "Shutting down WebShield" on page 52 for details. To shut down or restart the WebShield machine directly, follow these steps:

Step	Action

1. Press ALT+F2 on the WebShield machine.

   Response: A login prompt is displayed.

2. At the login prompt, enter the user name `root` and the root password.

   ✍ *The default root password is* `webshield`*. If you have not yet changed this password, you should change it now. See "Changing the root password" on page 54.*

3. Type:

   ```
   shutdown -h now
   ```

   and press ENTER. Wait a few moments while the system shuts down. When shutdown is complete, you can reboot or turn off the machine.

Moving a client workstation from the internal or external network

Since WebShield assigns a network interface to workstations within the local area network on boot up, the WebShield system may need to be reset after relocating a workstation.

After relocating an internal network workstation to an external network area or relocating an external network workstation to an internal network area, you must reset the WebShield box. WebShield will not recognize the newly relocated system until the WebShield box is reset and WebShield assigns the appropriate network interface to the system.

A Additional References

For More Information

The McAfee BBS and CompuServe McAfee Virus Help Forum are excellent sources of information on virus protection. Independent publishers, colleges, training centers, and vendors also offer information and training on virus protection and computer security.

We especially recommend the following publications:

- Ferbrache, David. *A Pathology of Computer Viruses*. London: Springer-Verlag, 1992. (ISBN 0-387-19610-2)
- Jacobson, Robert V. *The PC Virus Control Handbook*, 2nd Ed. San Francisco: Miller Freeman Publications, 1990. (ISBN 0-87930-194-0)
- Jacobson, Robert V. *Using McAfee Associates Software for Safe Computing*. New York: International Security Technology, 1992. (ISBN 0-9627374-1-0)

For more information on firewalls and network security, McAfee recommends the following additional resources:

- Chapman, D. Brent and Zwicky, Elizabeth D. *Building Internet Firewalls*. Sebastopol: O'Reilly & Associates, 1995. (ISBN 1-56592-124-0)
- Cheswick, William and Bellovin, Steven. *Firewalls and Internet Security*. Reading: Addison-Wesley, 1994. (ISBN 0-201-633-57-4)
- Garfinkel, Simson and Spafford, Gene. *Practical Unix and Internet Security*, 2nd Ed. Sebastopol: O'Reilly & Associates, 1996. (ISBN 1-565-92-148-8)

Index

N

P

Q

R

S

T

U

V

W