User's Guide

WebShield

McAfee, Inc.
2710 Walsh Avenue
Santa Clara, CA 95051-0963

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

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

FEEDBACK

McAfee appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligations whatsoever. Please address your feedback to: McAfee, Inc., Documentation, 2710 Walsh Avenue, Santa Clara, CA 95051-0963, or send a fax to McAfee Documentation at (408) 653-3143.

Issued September 1996/WebShield Version 1.0.0

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 Internet e-mail, file transfers, and Web-browsing traffic 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, file transfers and World Wide Web Traffic at the Internet gateway
- Offers secure remote management through an intuitive Web-based interface
- Provides dedicated operating system and virus scanning software for IBM-compatible systems
- 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 scanned services
- Uses 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 at the following address:

McAfee, Inc.
2710 Walsh 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.

Phone	(408) 988-3832
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
- Operating system type and version
- 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
Canada L3R 2G9
Phone: (905) 479-4189
Fax: (905) 479-4540

McAfee Europe B.V.
Orlyplein 81 - Busitel 1
1043 DS Amsterdam
The Netherlands
Phone: (0) 31 20 6815500
Fax: (0) 31 20 6810229

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

2 Installing WebShield

Before You Start

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

Required hardware

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

- Pentium 166 or better
- 32MB RAM
- 500MB disk drive, for WebShield and the operating system (set to SCSI ID 0 or 1)
- 2GB disk drive, for file and packet spooling (set to SCSI ID 2-6)
- CD-ROM drive

  ✍ *All drives MUST be SCSI devices.*

- Two Network Interface Cards from the following list:
  - SMC Etherpower cards

    ✍ *McAfee recommends the SMC Etherpower cards.*

  - Other cards based on the DEC 21x40 series of chips

- Western Digital 8013-based cards
- AMD Lance cards
- 3Com 3c509 cards

  ✍ *The 3Com 3c509 cards may require manual configuration to ensure proper operation. These are not recommended.*

- 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
  - 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.*

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
- Domain name
- IP address

  ✍ *You need to provide the IP address for connection to the internal network. This address will only be used tor the internal connection. 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 facility to remotely collect your WebShield logs, the trusted host must be a Unix system.*

- Mail relay address

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

- WebShield Administrator's e-mail address

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

- Company name

- Domain name server

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

- Timezone

- Netmask, Network, and Broadcast address

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

Installation Procedure

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**

✍ *WebShield is intended to scan all traffic entering and leaving a local area network. WebShield uses two network interfaces, an "external" interface and an "internal" interface. For proper operation, the external interface must be attached to only one other device, such as a router, gateway, or firewall. 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.*

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

   Response: The Set Up Variable Filesystem screen is displayed.

5. 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 by hand, highlight Customize Disk Layout and select OK. You may wish to partition by hand 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.*

6. When partitioning is complete, select OK.

Response: The WebShield Configuration Screen is displayed.

7. Enter the following data into the form provided:

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

8. Select Network.

Response: The Advanced 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.*

Action: Enter the Domain Name Server and Mail Relay Address. Review the default settings, and select OK.

9. Select Timezone.

Response: The Timezone screen is displayed.

Action: Select your timezone from the list provided, and press ENTER to return to the WebShield Configuration Screen.

10. Select 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.
- **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 space bar.

11. Select OK.

Response: The Review Current Settings screen is displayed. Use the arrow keys or PAGE UP and PAGE DOWN to scroll up and down.

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

Response: WebShield is installed and running.

✍ *After installation, WebShield is configured and managed remotely from the trusted host through the HTML-based WebShield Administration Console. See "Using the WebShield Administration Console" on page 18. If you wish to configure your system using a non-graphical interface on the WebShield machine, enter the root password at the prompt. The default password is* `webshield`.

Changing the Root Password

After 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 root password can be changed remotely using the Administration Console. See "Set administrative password" on page 33 for details. To change this password from the WebShield machine, 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 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. Note that 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 "Restart system" on page 40 and "Shut down system" on page 41 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 16.*

3. Type:

shutdown -h now

and press ENTER.

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

3 Using WebShield

Using the WebShield Administration Console

After initial installation, all WebShield configuration and management is handled from the trusted host, through an HTML-based WebShield Administration Console. From this console (Figure 3-1), you can scan the Quick Configuration Summary of WebShield's current settings or access control panels to customize your WebShield configuration.

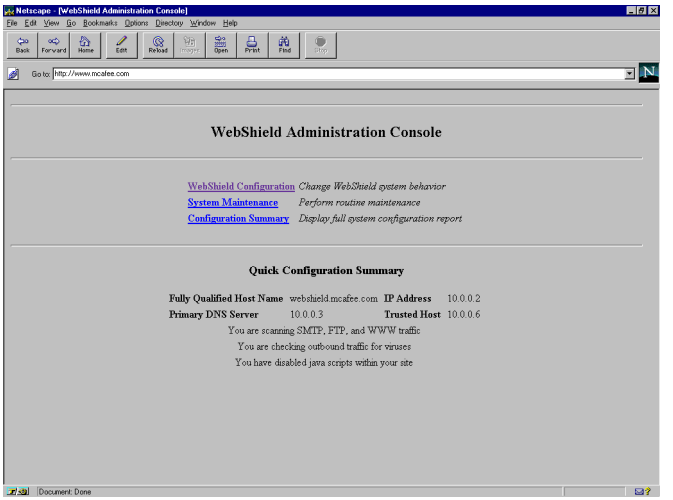

Figure 3-1. WebShield Administration Console Home Page

This chapter outlines the options that are available using the console and details the steps to take to configure your software.

From the WebShield Administration Console, you can link to three configuration and management pages. Using the forms provided in these pages, you can customize, manage, and maintain all aspects of WebShield. The pages 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 21.

- **WebShield System Maintenance**, which is used to update WebShield's virus definition data; export 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 34.

- **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 43.

Using the non-graphical administration tool

In most cases, WebShield will be administered from the HTML-based Administration Console described in this chapter. However, for direct configuration and management, a non-graphical administration tool is also available on the WebShield machine itself. This tool operates in much the same way as its HTML equivalent, and can be used to configure and manage your WebShield settings, including passwords and system shutdown.

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 character-based administration tool is /usr/sbin/wsadm.*

The company name and timezone can only be set during installation or by using this non-graphical interface.

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.

4. At the password prompt, enter the Webshield root password.

   ✍ *The default password is* `webshield`*. If you have not yet changed this password, McAfee recommends that you change it now. See "Changing the Root Password" on page 16 or "Set administrative password" on page 33 for more information.*

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

   ✍ *McAfee recommends that you bookmark this home page for easier access later.*

Using the Configuration Menu

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

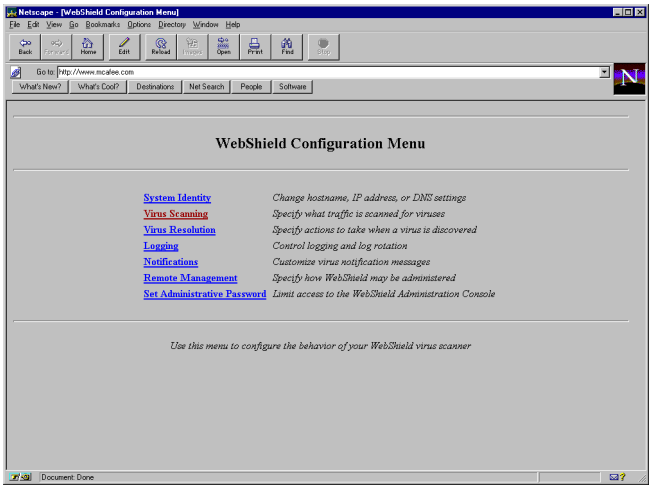

Figure 3-2. WebShield Configuration Menu

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

- System identity
- Virus scanning
- Virus resolution
- Logging
- Notifications
- Remote management
- Set administrative password

System identity

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

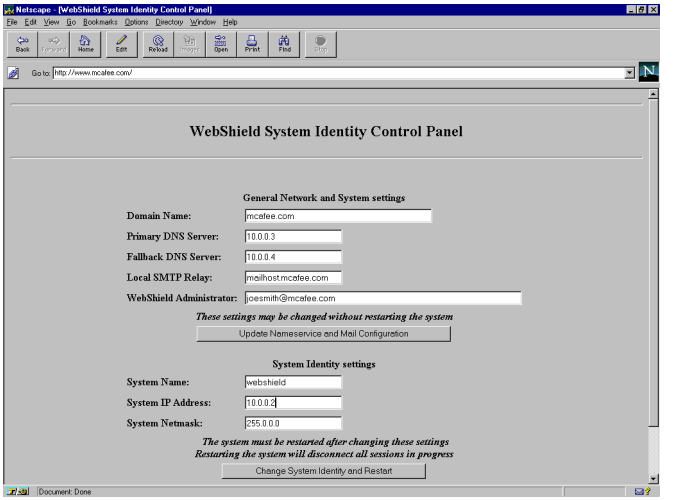

Figure 3-3. WebShield System Identity Control Panel

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.

   - If you change the Domain Name, Primary DNS Server, Fallback DNS Server, Local SMTP Relay, or WebShield Administrator E-mail Address, click Update Nameservice and Mail Configuration.

   - If you change the System Name, System IP Address, or System Netmask, click Change System Identity and Restart.

     ✍ *When you submit changes to the System Name, System IP Address, or System Netmask, the WebShield machine will be restarted, breaking all connections running through it.*

Response: A confirmation screen is displayed, and the WebShield system identity is updated to reflect your changes.

Virus scanning

The WebShield Virus Scanning Control Panel (Figure 3-4) is used to configure the scanning policies for your network.

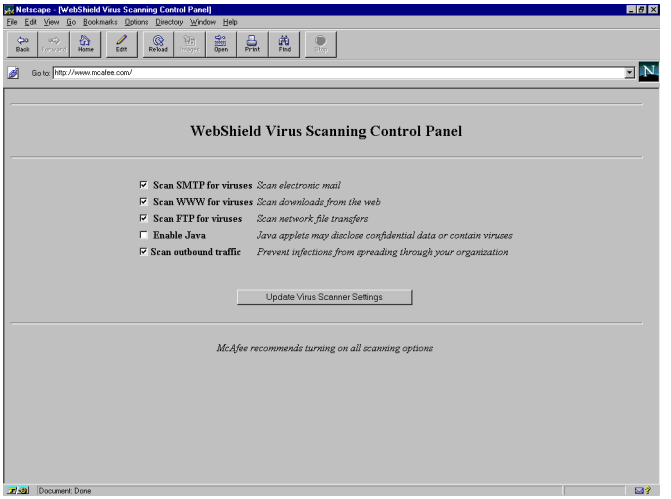

Figure 3-4. WebShield Virus Scanning Control Panel

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. Select your general scanning policies.

- **Scan SMTP for Viruses**: Check this box if you want WebShield to scan traffic using the Simple Mail Transfer Protocol, or SMTP. This protocol handles electronic mail exchange between mail servers.
- **Scan WWW for Viruses**: Check this box if you want WebShield to scan World Wide Web traffic.
- **Scan FTP for Viruses**: Check this box if you want WebShield to scan traffic using the File Transfer Protocol, or FTP. This protocol is designed for transferring files across networks.
- **Enable Java**: Check this box if you want to re-enable the transmission of Java applets. By default, WebShield filters Java applets, which may disclose confidential data or contain viruses.
- **Scan Outbound Traffic**: Check this box if you want WebShield to scan outbound traffic.

✍ *For maximum security, Enable Java should be OFF. All ither items should be ON.*

3. Click Update Virus Scanner Settings.

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

Virus resolution

The WebShield Virus Resolution Control Panel (Figure 3-5) allows you to configure the actions WebShield should take when a virus is detected during a transfer.

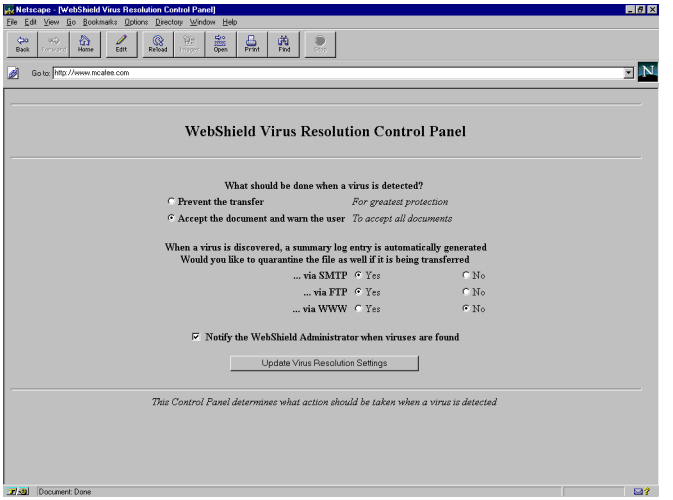

Figure 3-5. WebShield Virus Resolution Control Panel

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

Step	Action
1.	Start the Administration Console, select Webshield Configuration, and click on Virus Resolution. **Response**: The WebShield Virus Resolution Control Panel is displayed.
2.	Select an action for WebShield to take upon virus detection: ▪ **Prevent the Transfer**: If you want to prevent the transfer from taking place when a virus is detected, click this button. ▪ **Accept the Document and Warn the User**: If you want to allow the transfer but notify the user that it is infected, click this button.

3. When a virus is discovered, a summary log entry is generated automatically. The suspect file can also be saved in quarantine on the WebShield machine for later retrieval. Select your quarantine options, based on the protocol used for the transfer:

   - SMTP, or e-mail
   - FTP, or file transfer
   - HTTP, or the protocol used by the World Wide Web

   ✍ *McAfee recommends that you quarantine suspect files that are transferred using SMTP.*

4. If you want your WebShield Administrator to receive a notification message when WebShield discovers a virus, select Yes by clicking the box provided.

5. Click Update Virus Resolution Settings.

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

Logging

The WebShield Virus Logging Control Panel (Figure 3-6) allows you to customize your logging setup to meet your network's needs.

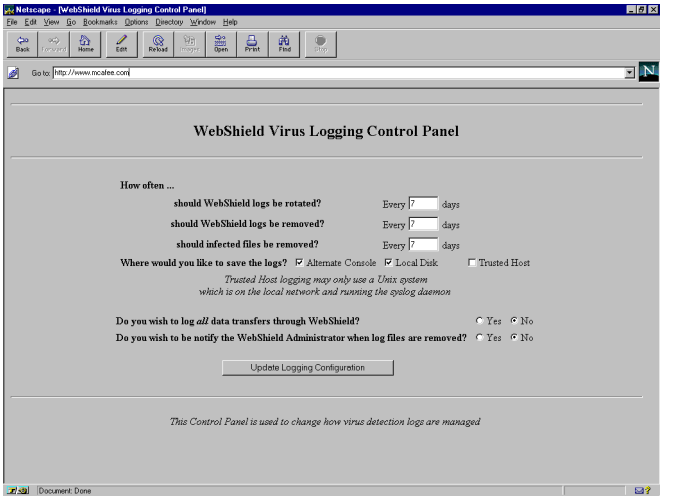

Figure 3-6. WebShield Virus Logging Control Panel

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

Step	Action
1.	Start the Administration Console, select WebShield Configuration, and click on Logging. **Response**: The WebShield Virus Logging Control Panel is displayed.
2.	Select how often WebShield logs should be rotated, by entering a number of days between log rotations. ✍ *By rotating the logs frequently, you reduce the size of the log files and make them more accessible for viewing.*
3.	Indicate how often old logs should be removed, by entering a number of days between log removal.

4. WebShield will store infected files for a specified number of days. Indicate how often infected files should be removed, by entering a number of days between file removal.

5. Select where you want WebShield to log data:

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

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

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

6. You can log all transfers passing through WebShield, regardless of whether they are infected. If you wish to reconfigure your logging options to activate this option, click Yes when asked if you wish to log all transfers.

7. WebShield can notify the WebShield Administrator when files are removed. If you wish for the Administrator to receive an e-mail notification, click Yes.

8. Click Update Logging Configuration to submit these changes.

   Response: A confirmation screen is displayed, and WebShield logging configuration is updated to reflect your 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 3-7).

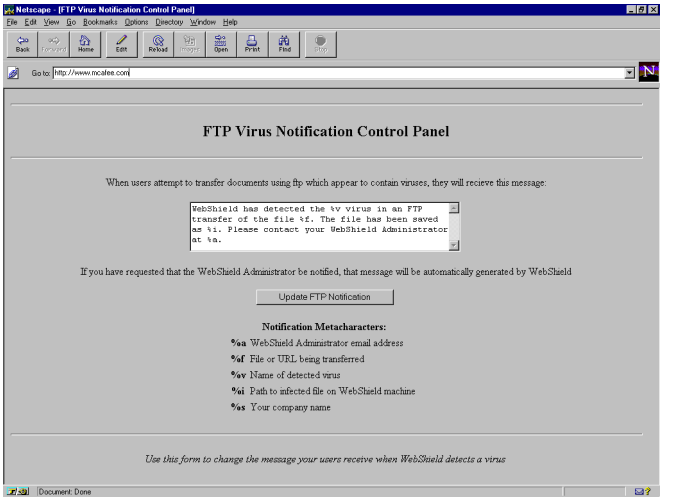

Figure 3-7. FTP Virus Notification Control Panel

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.
- **SMTP Bounce Message**: When WebShield detects a virus in electronic mail, it can notify the sender.
- **FTP Virus Detection**: When WebShield detects a virus in an FTP transfer, it can notify the client attempting to download.
- **WWW Virus Detection**: When a virus is detected while browsing the Web, WebShield can notify the browser attempting to access the site.
- **Java Detection**: When a Java applet is detected while browsing the Web, WebShield can notify the browser.

✍ *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 meta-characters 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 Update Notification button on that form.

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

Remote management

The WebShield Remote Management Control Panel (Figure 3-8) allows you to change the ways in which WebShield is configured and managed.

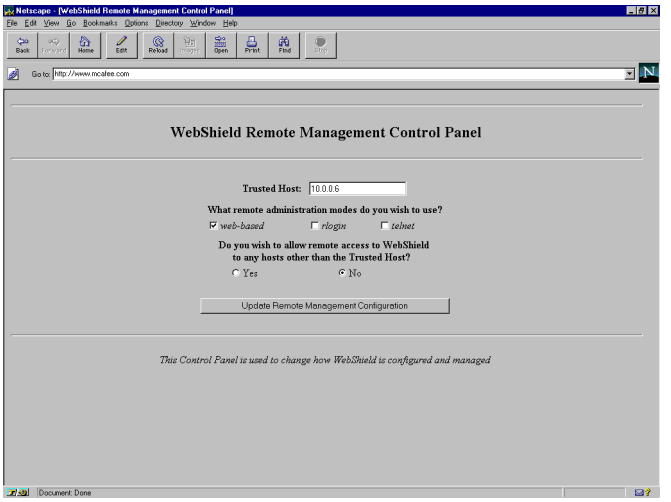

Figure 3-8. WebShield Remote Management Control Panel

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 into the form 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 facility 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, click the Web-based checkbox.
   - If you want to use the rlogin facility to access the non-graphical WebShield administration tool, click the rlogin checkbox.
   - If you want to use telnet to access the non-graphical WebShield administration tool, click the telnet checkbox.

4. If you wish to allow remote access to WebShield from hosts other than the trusted host, click Yes.

5. Click Update Remote Management Configuration.

   Response: A confirmation screen is displayed, and your WebShield remote management configuration is updated to reflect your changes.

Set administrative password

Using this form (Figure 3-9), you can change the password used to access both the WebShield machine and this Administration Console. This password also can be changed from the WebShield machine, as described in “Changing the Root Password” on page 16.

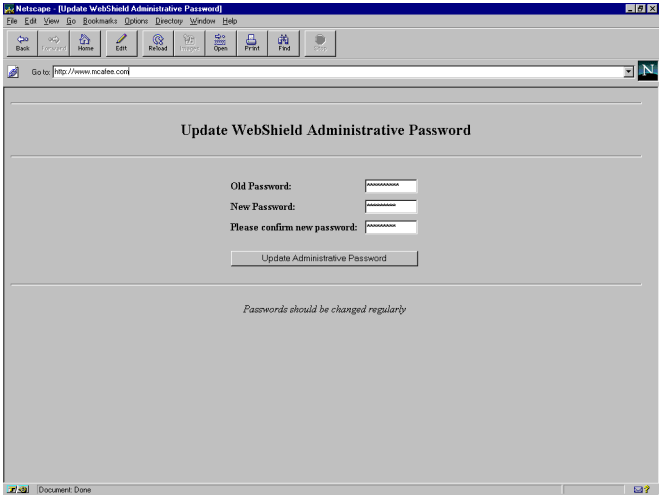

Figure 3-9. Update WebShield Administrative Password Page

To change the password, take the following steps:

Step	Action
1.	Enter your current password into the space provided.
2.	Enter a new password.
3.	Enter your new password again for confirmation.
4.	Click Update Administrative Password.

Response: A confirmation screen is displayed, and your WebShield password is updated.

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:

- Update virus definition data
- Export configuration
- Export logs
- Export quarantined file
- View current log
- Restart system
- Shutdown system

Update virus definition data

Every month more than 100 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. 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 Web Site 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 Definition Data.

   Response: The Update Virus Definition Data page is displayed (Figure 3-10).

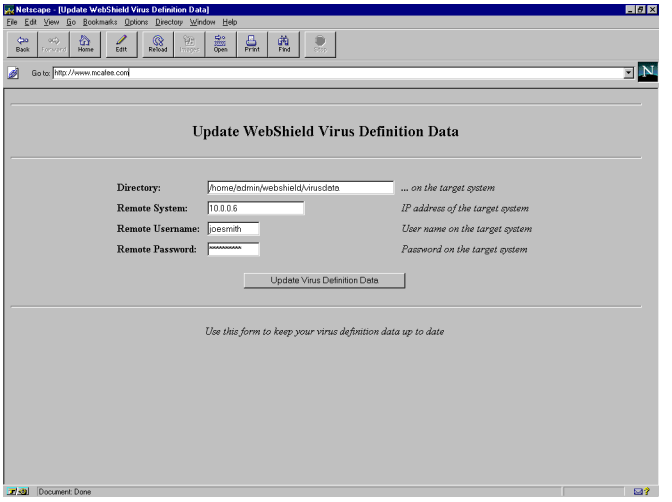

Figure 3-10. Update Virus Definition Data Page

5. Enter the full path of the directory containing the virus definition data into the space provided.

6. Enter the name of the remote system where the files are saved.

7. Enter the remote system's user name and password.

8. Click Update Virus Definition Data.

   Response: A confirmation screen is displayed, and WebShield's virus definition data are updated.

Export configuration

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 page is displayed (Figure 3-11).

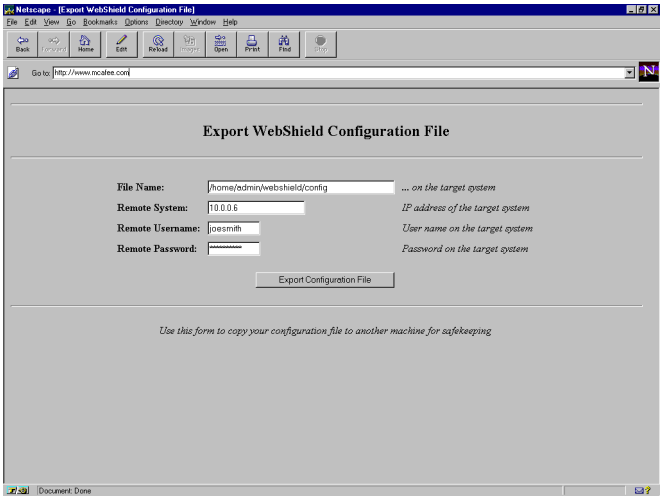

Figure 3-11. Export WebShield Configuration File Page

3. In the space provided, enter the name of the file to which you want to export the configuration, including the path.

4. Enter the name of the remote system to which you want to save the file.

5. Enter the remote system's user name and password.

6. Click Export Configuration File.

Response: A confirmation screen is displayed, and WebShield's Configuration File is exported to the remote system.

Export WebShield system log

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 Logs.

Response: The Export WebShield System Log page is displayed (Figure 3-12).

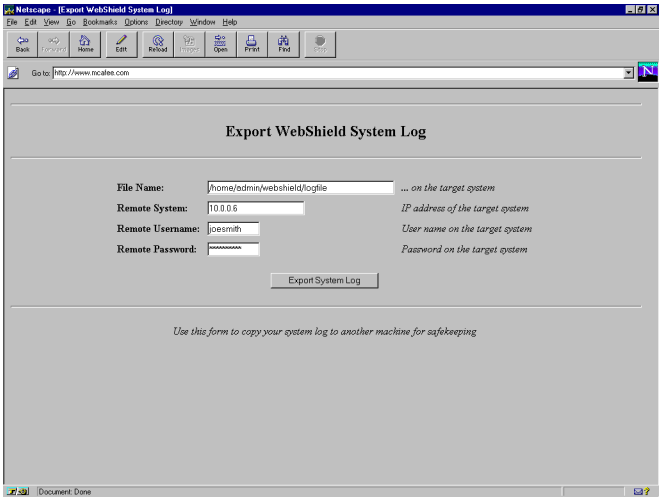

Figure 3-12. Export WebShield System Log Page

3. In the space provided, enter the name of the file to which you want to export the log file, including the path.

4. Enter the name of the remote system to which you want to save the file.

5. Enter the remote system's user name and password.

6. Click Export System Log.

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

Export 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 3-13).

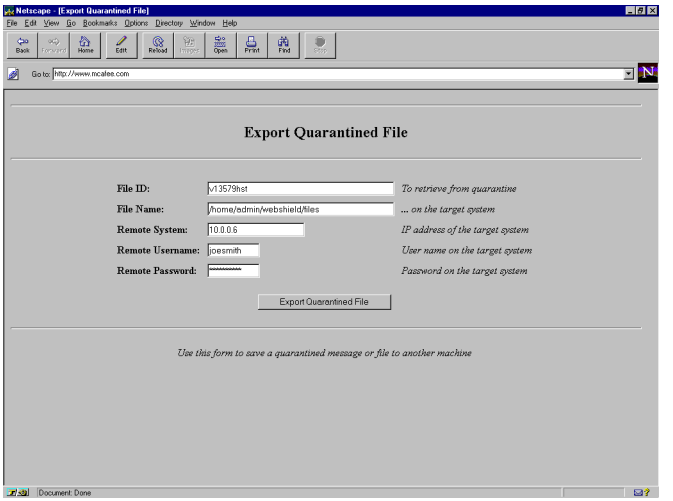

Figure 3-13. Export Quarantined File Page

3. To retrieve the file, enter the File ID in the space provided.

4. Enter the name of the remote system to which you want to save the file.

5. Enter the remote system's user name and password.

6. Click Export Quarantined File.

   Response: A confirmation screen is displayed, and the quarantined file is exported from the WebShield machine to the remote system.

View current log

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

To view the 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.
3.	Click your browser's Back button to return to the System Maintenance Menu.

Restart system

In some cases, it may become necessary to restart the WebShield system. Using the System Restart page from the WebShield System Maintenance Menu (Figure 3-14), you can reboot the WebShield system from the trusted host.

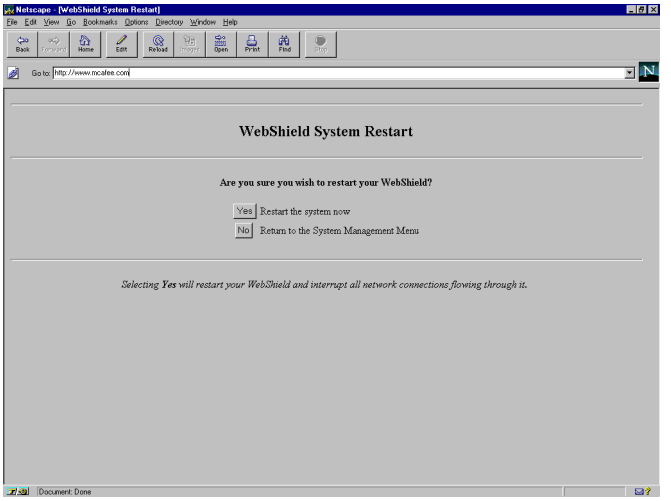

Figure 3-14. WebShield System Restart Page

To restart 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 Restart System.
3.	Click Yes to restart the WebShield system. **Response**: A confirmation screen is displayed, and the WebShield machine is restarted.

Shut down system

You may also need to shut down the WebShield system in some instances. Using the System Shutdown page from the WebShield System Maintenance Menu (Figure 3-15), you can remotely shut down the WebShield system from the trusted host.

Figure 3-15. WebShield System Shutdown Page

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 Shutdown System.

3. Click Yes 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 provides a 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 18. As changes are submitted, the Configuration Summary will be updated.

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

T

V

W