User's Guide

WebShield SMTP for Solaris

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

Network Associates, McAfee, McAfee Associates, VirusScan, NetShield, and SiteMeter are registered trademarks of Network Associates, Inc. ScanPM, WebScan, WebScanX, SiteExpress, BootShield, ServerStor, ScreenScan, ScreemScan, WebCrypto, PCCrypto, NetCrypto, Remote Desktop 32, WebShield, WebShieldX, 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.

Solaris, 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

Network Associates 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: Network Associates, Inc., Documentation, 2805 Bowers Avenue, Santa Clara, CA 95051-0963, send e-mail to documentation@nai.com, or send a fax to Network Associates Documentation at (408) 970-9727.

Issued March 1998 / WebShield SMTP for Solaris v3.1.6

Table of Contents

1 Introducing WebShield SMTP for Solaris

What Is WebShield SMTP?

WebShield SMTP (Simple Mail Transport Protocol) protects your network against viruses by scanning inbound and outbound e-mail traffic at your Internet mail gateway. Installing WebShield SMTP between your internal networks and external e-mail sites allows you to reduce the risk of virus attack by detecting, cleaning, logging, and moving infected e-mail messages and attachments to a quarantine folder.

WebShield SMTP is an important element of a comprehensive security program that should include a variety of safety measures, such as regular backups, password protection, training, and awareness. Network Associates urges you to set up and comply with a security program with these elements as a preventive measure to protect your corporate enterprise.

Because electronic mail is now the primary source of virus infections, mainly from macro viruses embedded in e-mail attachments, network users unaware that a document or spreadsheet contains a macro virus can easily spread copies of the virus to hundreds of other computers.

E-mail attachments with macro viruses can travel through firewalls—and through many anti-virus scanners—undetected. Some viruses even propagate by mailing themselves. Until recently, the only defense against these viruses was powerful virus detection at the desktop. Now, with WebShield SMTP, you can stop e-mailed virus infections before they reach the desktop.

WebShield SMTP for Solaris features

- Scans all e-mail messages and attachments at the Internet mail gateway, inbound and outbound, in real time
- Detects known viruses embedded in files saved in the following MIME (Multi-purpose Internet Mail Extensions) and Uuencode (UNIX-to-UNIX encoding) formats, including combinations of these formats:
  - ZIP (Zip compressed archive)
  - tar (POSIX [Portable Operating System Interface for UNIX] Tape Archive)
  - ARJ (compressed Archive Robert Jung)
  - LHA 1.x / LZH (compressed archives)
  - UNIX compress (.Z extension compressed)
  - gzip (UNIX GNU Zip compressed)
  - zoo (compressed archive)

  ✍ *(excludes self-extracting archives)*
- Removes known viruses and probable macro viruses from MIME-encoded files
- Optionally notifies the mail administrator, message recipients, and mail sender if it detects a virus
- Logs messages that contain a virus, and reports how it has resolved each incident
- Offers a quarantine option so you can safely examine any mail that remains virus-infected
- Allows easy setup of and modifications to your internal e-mail routing
- Scans and processes e-mail addressed to virtual domains
- Configures easily from any point on your network via your favorite web browser

How To Contact Network Associates

Customer service

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

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

Technical support

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

World Wide Web	http://www.nai.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@nai.com
Network Associates 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 NAI
America Online	keyword NAI

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

For corporate-licensed customers:

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

For retail-licensed customers:

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

To provide the answers you need quickly and efficiently, the Network Associates 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 model and any additional hardware
- Specific steps to reproduce the problem

International contact information

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

Network Associates Canada
139 Main Street, Suite 201
Unionville, Ontario
Canada L3R 2G6
Phone: (905) 479-4189
Fax: (905) 479-4540

Network Associates Europe B.V.
Gatwickstraat 25
1043 GL Amsterdam
The Netherlands
Phone: 31 20 586 6100
Fax: 31 20 586 6101

Network Associates France S.A.
50 rue de Londres
75008 Paris
France
Phone: 33 1 44 908 737
Fax: 33 1 45 227 554

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

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

Network Associates 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

Network Associates 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

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

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

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

2 Using WebShield SMTP for Network Security

Security Policies

WebShield SMTP for Solaris is a powerful tool for implementing your e-mail traffic security policies. Although scanning e-mail messages for viruses can help prevent an attack on your system, you should rely on this tactic to provide only one part of your overall security strategy. You must have consistent and reliable security policies for WebShield SMTP to be fully effective. Areas to consider include:

- What services you need

  The first step in deciding what security policies to implement is to consider what traffic you want to allow into your network and under what conditions. Your company might require certain services from the Internet, but might see other services as posing unnecessary risks.

- What the risks are

  Different Internet services involve varying degrees and types of risk. Once you have determined the services your users require, study the risks involved, then decide on the appropriate level of security for handling them.

- Security procedures for users

  Communicating with people at your site and involving them in the security process can help prevent attackers from breaking into a system by relying on weaknesses in people rather than in software. Many successful attackers, for example, trick people into revealing passwords or other information that compromises a target system's security.

- Host security

  Deciding how to handle network traffic includes evaluating what security you should implement at the host level. You must consider how to secure hosts accessible from outside the network. For example, if you allow e-mail to go directly from external systems to an internal mail server, you would need additional security measures to protect tyhe host system from infection. If you route incoming e-mail traffic through WebShield SMTP first, you can ensure the protection you need without additional complex security measures.

Once you have determined your security policies, you can install and configure WebShield SMTP. As e-mail arrives, WebShield SMTP handles each message according to the configuration you have specified.

Fitting WebShield SMTP Into Your Network

WebShield SMTP communicates between external servers and internal mail servers on your network. Internal network users send and receive mail through WebShield SMTP, rather than contacting external servers directly. For outbound mail, WebShield SMTP can also act as a regular mail server itself; it forwards inbound mail to the internal mail hubs you specify. You could also install WebShield SMTP on a perimeter network, or as part of a firewall system.

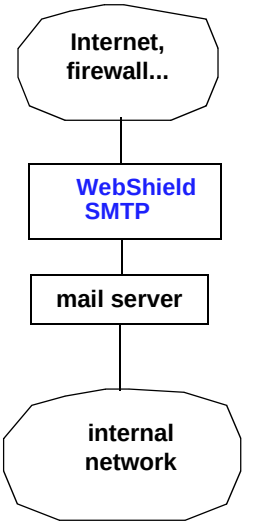


Figure 2-1. WebShield SMTP for Solaris logical diagram

✍ *This logical diagram (Figure 2-1) does not necessarily represent the physical architecture of your WebShield SMTP system.*

After you install WebShield SMTP on your mail server or a separate server, configure your internal hosts (mail clients) to direct all mail to your internal mail hubs. Configure your internal mail hubs to direct mail to WebShield SMTP. To direct inbound mail from the Internet to WebShield SMTP, modify your MX (mail exchanger) records for your domains and your mail hubs. See “Directing inbound mail to WebShield SMTP” on page 25 for more details. Doing so directs any inbound mail addressed to a recognized domain (or virtual domain) or the mail hubs first to WebShield SMTP, then onward to the internal mail server.

Gateway installation

Figure 2-2 shows one type of installation that Network Associates recommends. Here, WebShield SMTP resides independently on a server that is closer than your internal mail server is to the perimeter of your network.

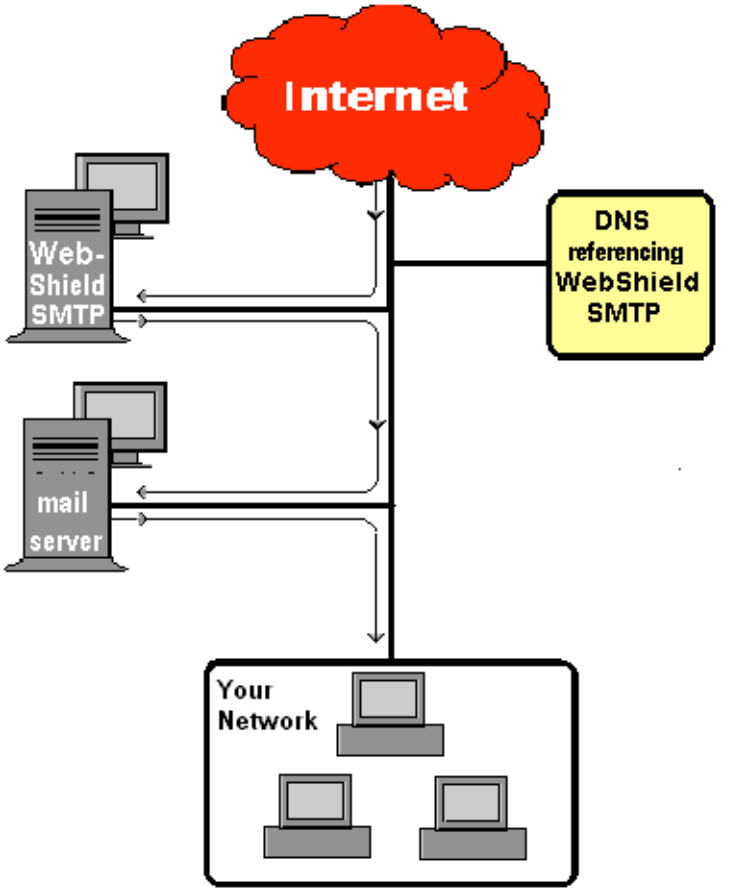


Figure 2-2. WebShield SMTP Gateway Installation

When you install WebShield SMTP at your mail gateway on a different machine from your internal mail server, WebShield SMTP will send scanned mail to the servers you specify.

Integrated installation

You may integrate WebShield SMTP with your existing mail server if your mail server runs on Solaris. After scanning for viruses, WebShield SMTP hands the mail to the mail server to deliver locally. Installing WebShield SMTP on your mail server results in the network architecture shown in Figure 2-3.

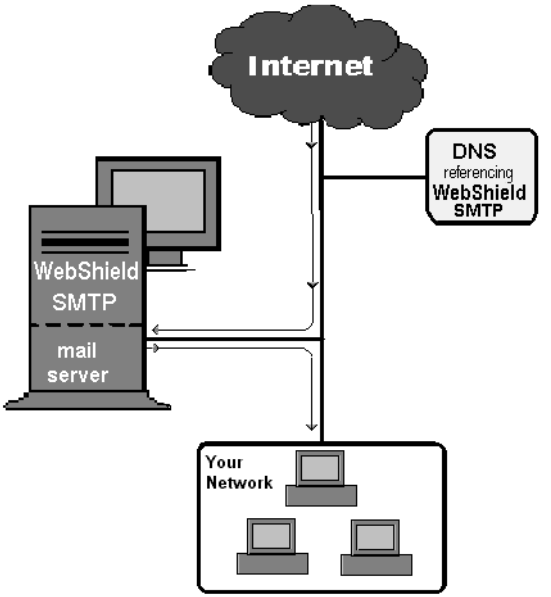


Figure 2-3. WebShield SMTP Integrated Installation

When you install it on your mail server, WebShield SMTP uses the mail server's sendmail utility for the final step in delivering inbound and outbound mail.

Virtual domains

WebShield SMTP understands how to route mail to virtual domains, but you must configure it to use all domains, including virtual domains, that you want it to recognize. If you neglect to enter a domain or virtual domain, WebShield SMTP will treat it as being outside your network and will not relay mail between it and any external address.

3 Installing WebShield SMTP for Solaris

Before You Begin

Network Associates distributes WebShield SMTP either on CD-ROM or via the Network Associates website. Review the system requirements shown below to verify that WebShield SMTP will run on the server you intend to use, then follow the steps for installation on page 20.

System requirements

- Sun Microsystems Solaris version 2.6 or 2.5.1, running on SPARC hardware

  You can install WebShield SMTP on your existing mail server as an Integrated installation, or you can install it on a separate machine as a Gateway installation.

- System swap space at least 2.5 times the size of physical memory

  Scanning files for viruses, especially compressed files, can require a large amount of virtual memory. To determine or modify the size of your system swap space, consult Sun Microsystems documentation. (See Appendix B, “Suggested Reading” on page 70.)

- `/var` partition large enough to accommodate mail queues

  WebShield SMTP expands compressed files while scanning them for viruses. Network Associates recommends 1GB per 1000 users for most organizations with large mail volumes.

- 7MB in `/opt` for the `NETAlib` package, 3MB in `/opt` for the `NETAsmtp` package, and additional space in `/var` for their queue directories

- `tmpfs` for your `/tmp` directory

  Note that systems with `tmpfs` can run out of inode space for `tmpfs` in kernel memory. Consult Sun Microsystems documentation noted in Appendix B, "Suggested Reading" on page 70 for more information. For Solaris version 2.6 in particular, be sure your `tmpfs` has enough inodes by inserting the following line into the file `/etc/system`

  `set tmpfs:tmpfs_maxkmem = 0x600000` (for example).

  Next, reboot your system.

- 20MB in `/opt` for the `NETAvil` package, the Network Associates Virus Information Library

  ✍ *Although Network Associates recommends installing the `NETAvil` package, WebShield SMTP does not require it. See "Online Manual and Virus Information" on page 65 for details.*

Default requirements for your mail server

The WebShield SMTP installer assumes that

- you are using sendmail
- your start-up script is `/etc/init.d/sendmail`
- this start-up script is hard-linked to `/etc/rc2.d/S88sendmail`
- you have made no changes to your sendmail start-up script.

✍ *If you have made changes, you must manually save a copy of your customized `/etc/rc2.d/S88sendmail` file. If you remove WebShield SMTP from your server, WebShield SMTP restores only the standard configuration.*

The next two subsections list information you must have available to install WebShield SMTP successfully.

Information you need during installation

- The CIDR (Classless Inter-Domain Routing) address of your network (A CIDR address is an IP address followed by a slash, then by the number of bits in the netmask; an example is 172.16.0.0/16 .)
- Your network mail administrator's e-mail address
- The domain name for your mail system
- The port number on the WebShield SMTP machine where your administration server should listen
- The IP (Internet Protocol) address for the primary network interface of the server that will host WebShield SMTP
- The device name of your primary network interface

  ✍ *Type `ifconfig -a` then press Enter to see the device names for your network interfaces. Examples include such Ethernet adapters as `le0, hme0, and qe1.` Find the name that corresponds to the IP address of the server that will host WebShield SMTP.*

- The port number on the WebShield SMTP machine where your certificate server software should listen
- Your company name

Information you need for setup after installation

- The MX (mail exchanger) resource record entry for your existing internal SMTP mail server

Installation Steps

To install WebShield SMTP, follow these steps:

1. On the computer you intend to use to host WebShield SMTP, change your working directory to a temporary directory by typing

   ```
   cd /tmp
   ```

2. Download the WebShield SMTP for Solaris package container into your temporary directory from the Network Associates website, www.nai.com, or insert the WebShield SMTP for Solaris CD-ROM into the CD-ROM drive.

   Response: `webshlss.316`, the package container for installing WebShield SMTP, loads into the temporary directory on your machine, or the WebShield SMTP CD-ROM mounts into the /cdrom directory.

3. Type the package add command followed by the path, then press Enter. (The required `-d` argument tells `pkgadd` to look in the directory specified, rather than in the default spool directory `var/spool/pkg`.) For example, type

   ```
   pkgadd -d /tmp/webshlss.316
   ```

   Response: A list of three packages appears.

   ```
   The following packages are available:
   1 NETAlib Network Associates Virus Scanning Library,
   release 3.1.6

   2 NETAsmtp Network Associates WebShield SMTP
   for Solaris, release 3.1.6

   3 NETAvil Network Associates Virus Information
   Library, Up-to-date 2-1-98

   Select package(s) you wish to process (or 'all' to
   process all packages). (default: all) [?,??,q]
   ```

4. Type either `1,2` or `all`, then press Enter. The virus scanning library and the WebShield SMTP for Solaris program packages are required. Network Associates recommends that you also install the virus information library. (See "Online Manual and Virus Information" on page 65.)

   ✍ *To accept the default option, simply press Enter.*

   Response: Your computer begins processing the virus scanning library package, then prompts you to create a base directory for the files.

```
Processing package instance <NETAlib> from
</tmp/webshlss.316> Network Associates
Virus Scanning Library, release 3.1.6
Copyright 1998 Network Associates

The selected base directory </opt/NETAlib> must
exist before installation is attempted.
Do you want this directory created now [y,n,?,q]
```

5. Type `y` to create the base directory shown, then press Enter.

   Response: As a precaution, the installer prompts you to continue before it executes scripts with super-user permission.

```
This package contains scripts which will be executed
with super-user permission during the process of
installing this package.
Do you want to continue with the installation of
<NETAlib> [y,n,?]
```

6. Type `y` to continue the installation, then press Enter.

   Response: Your machine tracks the progress of the installation, listing the files it installs, then notifying you when the installer finishes.

```
Installing Network Associates Virus Scanning Library
as <NETAlib>
```

   Your machine then begins to process the second package.

7. The installer next asks you to enter some information specific to your system. Reply by typing the correct answers for your network. Press Enter after each response.

✍ *The examples shown list default responses in brackets and italic type. The correct form for responses appears as a series of x's and dots.*

- `Please enter the CIDR address of your administration network: x.x.x.x/x`
- `Please enter the email address of your mail administrator: xxxxxx@xxxxx.xxx`
- `Please enter the DNS domain name of your mail system: xxxxx.xxx`
- `Please enter the port at which your admin server should listen [443]:`
- `Please enter the address of your primary interface: xxx.xxx.xxx.xxx`
- `Please enter the device name of your primary interface [le0]:`
- `Please enter the port at which your certificate server should listen [80]:`
- `Please enter your Company Name: xxxxxxx`

Next, the program asks you to type keys at random.

```
We are now going to generate the first part of your
secure administration server's cryptographic key.
Please type randomly on your keyboard until you hear
the beep:
```

8. Quickly type many keys at random until...

Response: ...you hear a beep and the following message appears.

```
* -Enough, thank you.
```

Package 2 processing continues with the following prompt:

```
The selected base directory </opt/NETAsmtp> must
exist before installation is attempted.
Do you want this directory created now [y,n,?,q]
```

9. Type y, then press Enter.

Response: Your machine creates the directory and lists the files it will install. `Pkgadd` then offers you this prompt:

```
Do you want to install these as setuid/setgid files
[y,n,?,q]
```

10. Type y. Although not essential for some programs, WebShield SMTP requires installation of these files as `setuid/setgid`.

✍ *You must answer Yes and install the files as set user and group ID files. Otherwise, the installation will complete, but WebShield SMTP will not work.*

Response: As a precaution, the installer prompts you to continue before it executes scripts with super-user permission.

```
This package contains scripts which will be executed
with super-user permission during the process of
installing this package.

Do you want to continue with the installation of
<NETAsmtp> [y,n,?]
```

11. Type y, then press Enter.

Response: Your machine tracks the progress of the installation.

```
Installing Network Associates WebShield SMTP
for Solaris, as <NETAsmtp>
```

Your computer does some further processing, including generating a private key (for encrypting certificate authorization security), then it notifies you when it has finished installing the second package.

If you chose not to install `NETAvil`, your installation is complete. Skip to the next section "Directing inbound mail to WebShield SMTP" on page 25.

The last package, the virus information library, begins installing as your computer reports

```
Processing package instance <NETAvil>
from </tmp/webshlss.316>

Network Associates Virus Information Library,
Copyright 1998 Network Associates

The selected base directory </opt/NETAvil> must
exist before installation is attempted.
Do you want this directory created now [y,n,?,q]
```

12. Type y, then press Enter.

Response: Your machine creates the directory and proceeds with installing the virus scanning library.

Your computer lists the files it installs, then notifies you when the installation is complete.

Congratulations! You have finished installing WebShield SMTP. Next you must configure your network mail routing architecture and set up secure network connections.

Directing inbound mail to WebShield SMTP

When you first set up WebShield SMTP, you must modify your DNS (domain name system) configuration so that incoming mail goes through WebShield SMTP before being delivered to your existing mail server. Follow these steps:

1. Locate the mail exchanger (MX) resource record entry that your existing SMTP mail server uses.

2. Change this record by substituting the fully qualified domain name (for example, wssmtp.yourcompany.com) of the host where you installed WebShield SMTP.

   ✍ *The modified MX record must point to WebShield SMTP with a higher priority (lower number—the lower the better) than the priority for external mail exchangers.*

Example
DNS Table

Name	Type	Priority Value (Preference)	Data
mail.yourcompany.com (mail server)	MX	10 (a low number)	wssmtp.yourcompany.com (WebShield SMTP)

In the example above, all incoming and outgoing mail intended for the host mail.yourcompany.com will be forwarded to wssmtp.yourcompany.com

✍ *The procedure you use to modify your DNS configuration will depend upon your network environment.*

Your incoming e-mail traffic will now go through WebShield SMTP, and then be delivered to the internal mail server or servers.

Directing outbound mail to WebShield SMTP

✍ *You may skip this section if WebShield SMTP is installed on your only internal mail server.*

To scan outbound mail for viruses, you must configure your internal mail servers to direct outbound mail to WebShield SMTP. The following sections describe the procedures for Microsoft Exchange servers, UNIX-based servers using sendmail, and other internal mail servers.

Microsoft Exchange servers

Make the following changes in Microsoft Exchange:

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 appears.

3. Click the Connections tab, then click Advanced.

   Response: The Advanced dialog box appears.

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 appears.

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 appears with the Routing tab displayed.

8. Select Do Not Reroute Incoming SMTP Mail

9. You must restart Microsoft Exchange Internet Mail so the changes you made will take effect. 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.

UNIX-based servers using sendmail

For internal mail servers using sendmail, set the default mail relay value in your `sendmail.cf` file to the name of your WebShield SMTP server. For example, change the lines

```
# 'Smart' relay host
#DS
# major relay host
#DR
#CR
```

to

```
# 'Smart' relay host
DSwssmtp.yourcompany.com
# major relay host
DRwssmtp.yourcompany.com
CRwssmtp.yourcompany.com
```

where `wssmtp` is the name of the server where WebShield SMTP is installed.

Other internal mail servers

For other types of internal mail servers, configure your mail server to relay all outbound mail through WebShield SMTP. This option is often called “default mail relay.”

To administer WebShield SMTP, set up the WebShield SMTP Administration Console as the next section of this chapter describes.

Setting Up Access to the WebShield SMTP Administration Console

Administering WebShield SMTP for Solaris is convenient and secure through the HTML-based WebShield SMTP Administration Console. WebShield SMTP will not allow arbitrary hosts to connect to the Administration Console; it will accept requests only from the administration hosts you specify during the installation process.

✍ *You can use the WebShield SMTP Administration Console to change your administration hosts later.*

First you must initialize your web browser by downloading the certificate file from the WebShield SMTP host, then connect to the console securely through SSL (secure sockets layer, an Internet security protocol). The next sections describe the procedures.

Initializing your web browser

The first time you connect to the Administration Console from an administration host, you must initialize your web browser. This ensures that your web browser will recognize WebShield SMTP for Solaris as a secure server that you have permission to use. To do this, you must download the certificate file to your browser.

To initialize your web browser on the secure administration host, follow these steps:

1. Start your browser.

2. In the address or the location field, type

   `http://<IP address>:<port number>`

   where `<IP address>` is the internal interface address of your WebShield SMTP for Solaris machine, and `<port number>` is the certificate server port.

✍ *The default port number for the certificate server is 80. If you chose this default port during installation, you do not have to type this number or the colon.*

3. Press Enter.

Response: The WebShield SMTP Administration Console asks if you want to download the key to your browser.

4. Click Setup CA Key to download the certificate authority key.

✍ *If you reinstall WebShield SMTP for Solaris, you must remove the earlier certificate authority key from your browser and set up a new secure connection. Otherwise, your browser might send you an error message, and you will not be able to administer WebShield SMTP for Solaris.*

5. Follow the prompts your browser displays to download and initialize the key.

6. Click Go to SMTP Administration.

7. At the user prompt, enter `root`.

8. At the password prompt, enter WebShield SMTP's password.

✍ *The default password is `webshield`. Change this on the Administration Console as soon as possible.*

Response: You are now connected to the secure server. You can configure WebShield SMTP from the secure server using the WebShield SMTP Administration Console.

Starting the WebShield SMTP Console Securely

After you have initialized your web browser, you must connect to the WebShield SMTP Administration Console with an SSL-compatible browser. Follow these steps:

1. Start your browser.

2. In the address or location field, type

   `https://<IP address>:<port number>`

   where `<IP address>` is the address of your WebShield SMTP host, and `<port number>` is the port of your SSL administration server. (Note that this address includes “s” after “http”, and is a different port number from the address for initializing the web browser in the previous section.)

   ✍ *The default port number of the administration host is 443. If you chose the default port during the install, you do not need to enter this number or the colon.*

3. Press Enter.

4. At the user prompt, enter `root`.

5. At the password prompt, enter the WebShield SMTP password. If you have not changed the administrative password, the default password is *`webshield`*. Change this on the Administration Console as soon as possible.

   Response: The WebShield SMTP Administration Console appears (Figure 4-1 on page 34). You might want to bookmark this page on your browser for easier access later.

   ✍ *The console’s graphical user interface appears best on screens with resolution of at least 800 x 600.*

You have successfully installed WebShield SMTP for Solaris, configured its required network architecture, and set up its secure network connections. The next chapter describes how to configure WebShield SMTP to perform e-mail routing and virus scanning.

4 Using the WebShield SMTP Administration Console

WebShield SMTP Administration Console Overview

After installing WebShield SMTP, and establishing a server connection to the Administration Console, you can manage your e-mail traffic and set up virus scanning, reporting, and response options for your mail system.

✍ *Do not attempt to administer one WebShield Solaris product while installing another on the same machine.*

Use the property pages provided in the WebShield SMTP Administration Console to configure and manage all program functions. The following summary describes the property pages available.

- **Configure WebShield SMTP**. Use this page to set your parameters for system management, virus scanning and resolution (the core of the software), mail and virus logging, and mail hubs. See "WebShield SMTP Configuration" on page 35 for descriptions of the options available.

- **System Maintenance**. Use this page to change your administration password, to start or stop the mail gateway, to export quarantined files, and to update virus data (DAT) files. See "WebShield SMTP System Maintenance" on page 52 for descriptions of these tasks.

- **Reports and Statistics**. Use this page to generate detailed mail gateway usage information and to specify how to view and export log files. See "WebShield SMTP Reports" on page 59 for more information and examples of these features.

- **Show Full Configuration**. Use this page to view a complete report of your current WebShield SMTP settings and policies. See "Show Full Configuration" on page 64 for details.

- **WebShield SMTP for Solaris Manual**. Use this page to open a new browser window that displays this *User's Guide* in PDF (portable document format) with Adobe Acrobat. You can consult this guide while also looking at the WebShield SMTP Administration Console, or print it.

- **Virus Information Library.** Use this page to link to the Network Associates Virus Information Library. If you installed the package `NETAvil`, WebShield SMTP displays your local copy in a new browser window. If you did not install `NETAvil`, WebShield SMTP connects to the library on the Network Associates website.

  ✍ *The User's Guide and Virus Information Library might not be available if you use a text-only browser.*

WebShield SMTP Configuration Summary

After you install WebShield SMTP and connect to the WebShield SMTP Console (see "Setting Up Access to the WebShield SMTP Administration Console" on page 29), you can set options and manage your e-mail traffic (Figure 4-1).

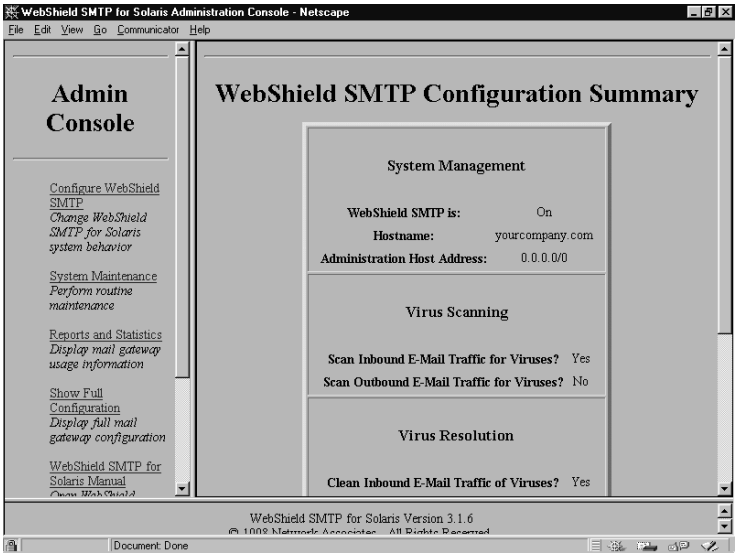


Figure 4-1. WebShield SMTP Administration Console Configuration Summary

The console opens with its six menu options listed as links in the left pane and a summary of the Webshield SMTP for Solaris current configuration displayed in the right pane (Figure 4-1). Click a link in the left pane to see the corresponding page.

✍ *On some browsers, e.g., Internet Explorer version 3.0, you might have to double-click on links to make them work.*

The configuration summary you see when you start the Administration Console shows the initial configuration options you chose during installation. As you change your configuration options in the other available pages, the summary changes to reflect your choices. You cannot edit the information displayed on this page directly.

WebShield SMTP Configuration

The Configuration window (Figure 4-2) appears when you click Configure WebShield SMTP on the left pane of the console.

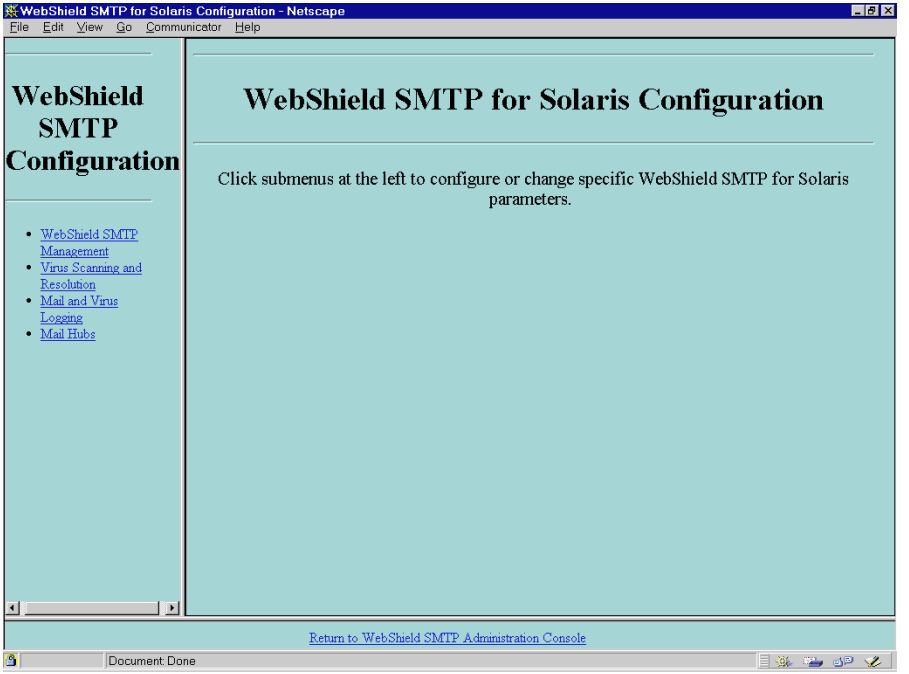


Figure 4-2. WebShield SMTP Configuration page

The WebShield SMTP Configuration menu page has four submenus:

- WebShield SMTP Management
- Virus Scanning and Resolution
- Mail and Virus Logging
- Mail Hubs

Click the menu item you want to see; the options available appear to the right, as in the example, Figure 4-3.

WebShield SMTP Management

Use the WebShield SMTP Management page (Figure 4-3) to enter or change the administration host machine's address and the mail administrator's e-mail address (the address that will receive administrator notification messages).

Select or delete the previous settings, then enter the new information in the text boxes provided. The Administration Host IP or CIDR address (see "Information you need during installation" on page 19) is the address of the machine from which you administer WebShield SMTP.

The Administration Server Port and the Certificate Authority Port are on the server where WebShield SMTP is installed. These port numbers can be any port available, although conventionally there are certain port numbers assigned to certain tasks. SSL-based web servers generally use port 443, and non-SSL web servers use port 80. WebShield SMTP uses these values by default (Figure 4-3).

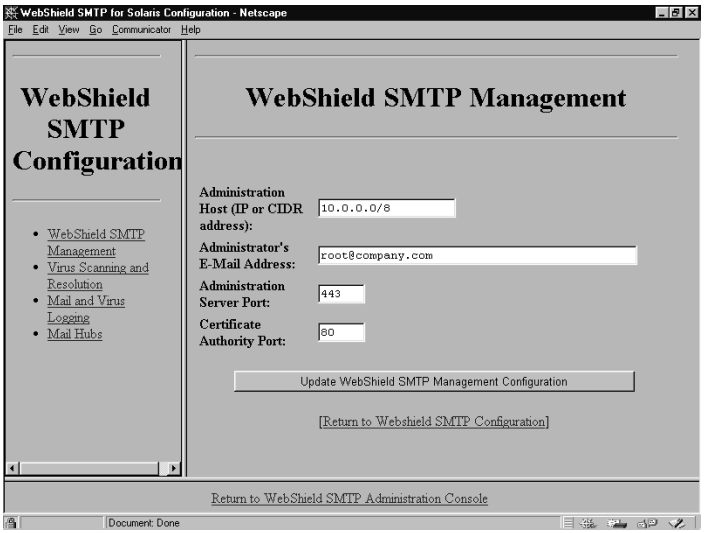


Figure 4-3. WebShield SMTP Management control panel

To see which ports your server is using, open or return to a command-line window, then type `netstat -a | grep -i listen` at the prompt. Solaris will display a list of active ports. Each active port listing consists of two parts: a machine name, which can consist of a fully qualified domain name, a simple machine name, or an asterisk; and a port number, which follows the name. The asterisk indicates that the port is listening on all of the system's network interfaces. If the port listing has a name but no number, look in the `/etc/services` directory to determine which number corresponds to the name.

Click Update WebShield SMTP Management Configuration to save your changes.

Throughout the console, you will know that your changes were saved when the page reappears displaying your new entries. WebShield SMTP displays an error message if your changes cannot be saved. (See "Error handling" on page 67 for more details.) To configure other WebShield SMTP options, click a different link.

Virus Scanning and Resolution

Use the Virus Scanning and Resolution page (Figure 4-4 on page 39) to set options for

- Scanning inbound and/or outbound mail for viruses. See "Virus Scanning" for details.
- Notifying the mail administrator and/or users about virus-infected messages, and specifying the contents of the notification message. See "Notification of Virus Activity" for details.
- Saving copies of virus-infected e-mail messages so you can analyze them later. See "Preservation of Detected Viruses" for details.
- Removing viruses from infected e-mail messages. See “Cleaning Infected Mail” for details.
- Transferring virus-infected e-mail messages to intended recipients even if WebShield SMTP cannot remove the virus. See “Forwarding of Infected Mail” for details.

Virus Scanning

The core of WebShield SMTP’s value lies in its ability to detect and remove viruses from your e-mail traffic. To enable this function, select Yes beneath the Scan Inbound Mail for Viruses label (Figure 4-4 on page 39). Selecting No disables virus scanning for inbound mail.

✍ *When first configuring your mail system, you might want to select No simply to test your mail flow.*

To see an explanation of this function online, click the Explain checkbox, then click Redraw at the top of the page.To see explanations for all functions on this page, select the Show Explanations checkbox, then click Redraw.

✍ *WebShield SMTP does not detect viruses in Microsoft Mail .msg archives.*

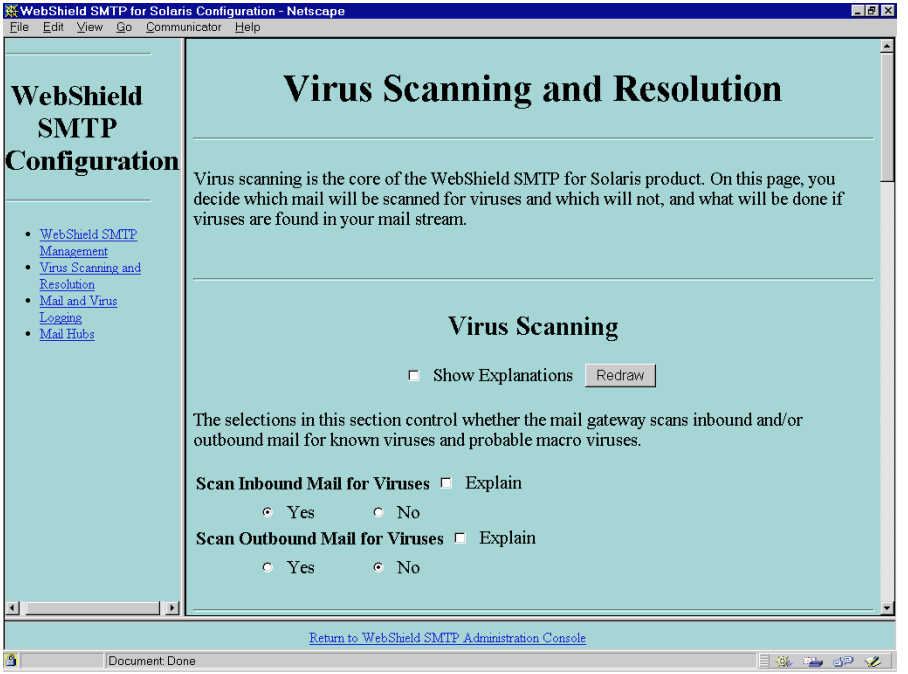


Figure 4-4. Virus Scanning and Resolution control panel Virus Scanning section

Network Associates also recommends that you choose to scan your outbound mail for viruses. Although scanning inbound mail protects your network from viruses brought in from the Internet, your network might get infected from some other source. If so, your users could inadvertently spread the virus to associates, clients, and customers. Scanning outbound mail allows you to detect and quickly trace a virus—before it can spread inside or outside your network.

To continue choosing options for virus detection and response, scroll down the configuration page to Notification of Virus Activity.

Notification of Virus Activity

Although you can configure WebShield SMTP to detect and respond to virus infections automatically, you might want to track incidences of infection, or choose how WebShield SMTP responds on a case-by-case basis. To help you with this task, you can tell WebShield SMTP to inform you, message senders, message recipients, or others whenever it finds a virus.You can accept the message (Figure 4-5 on page 40) that WebShield SMTP sends by default, or you can compose your own text for the message and specify what particular details you want to include. You can do the same for users inside or outside your network.

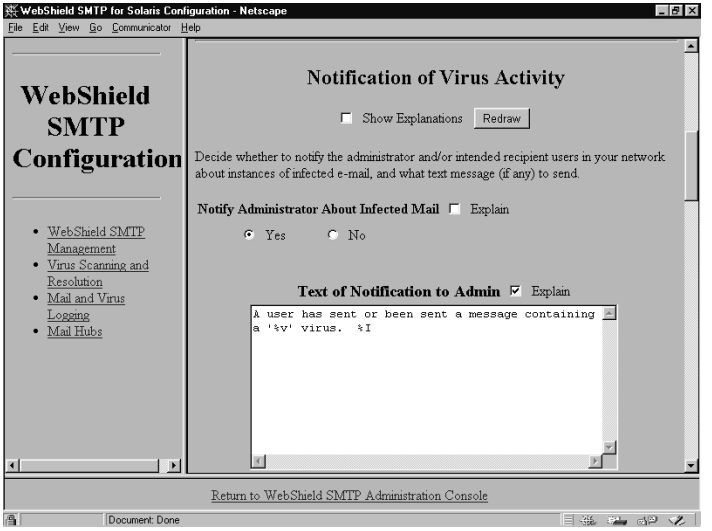


Figure 4-5. Virus Scanning and Resolution control panel Notification of Virus Activity section (Administrator options)

To have WebShield SMTP notify you when it finds a virus, select Yes beneath the Notify Administrator About Infected Mail label. To compose your own alert message, enter your text in the space provided.

When composing your own messages, you may use the shortcut symbols, or metacharacters shown below. WebShield SMTP also uses these characters in default messages.

- %a — These characters insert the mail gateway administrator's e-mail address that you specified during installation.
- %v — These characters insert the name of the detected virus.
- %i — These characters insert the Reference ID of the virus-infected file found on the mail gateway. To tell WebShield SMTP to assign a reference ID to use here, select the Preservation of Detected Viruses option (see page 43 for more details). If you do not choose to preserve viruses, WebShield SMTP displays N/A (not applicable) in your message.
- %I — [uppercase i] These characters expand into the text “The Reference ID is ‘%i.’” To tell WebShield SMTP to assign a reference ID for use here, select the Preservation of Detected Viruses option (see page 43 for more details). Otherwise, WebShield SMTP removes this text from your message.
- %s —These characters insert your company name, which you specified during the installation steps (see page 22).

When WebShield SMTP processes these metacharacters with your message text, it replaces the symbols with the specified data as it sends each notification. To see the metacharacter definitions, select the Explain checkbox beneath the Text of Notification to Admin label, then click Redraw at the top of the page. See “Online help text” on page 68 for more about WebShield SMTP’s online help.

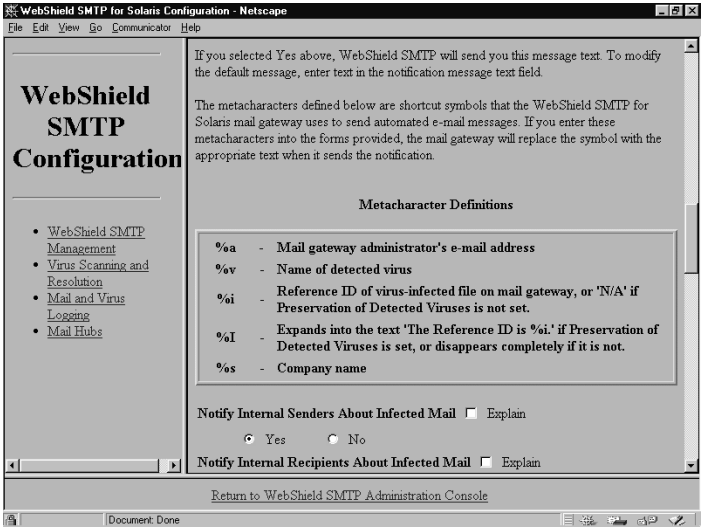


Figure 4-6. Virus Scanning and Resolution control panel Notification section (cont.)

Notifying the person who sent an infected message can reduce the likelihood of another infection from that source. Notifying message recipients can alert them to look for infected messages, particularly if you choose to forward messages with viruses that WebShield SMTP cannot remove.

You can notify any combination of senders within your network or outside your network, or recipients within your network or outside your network. Click Yes beneath the label corresponding to your choices (Figure 4-7 on page 43).

To compose your own message to internal or external users, enter the text you want to send in the space provided. You can use the same metacharcters available for messages to the mail administrator. See page 42 for details.

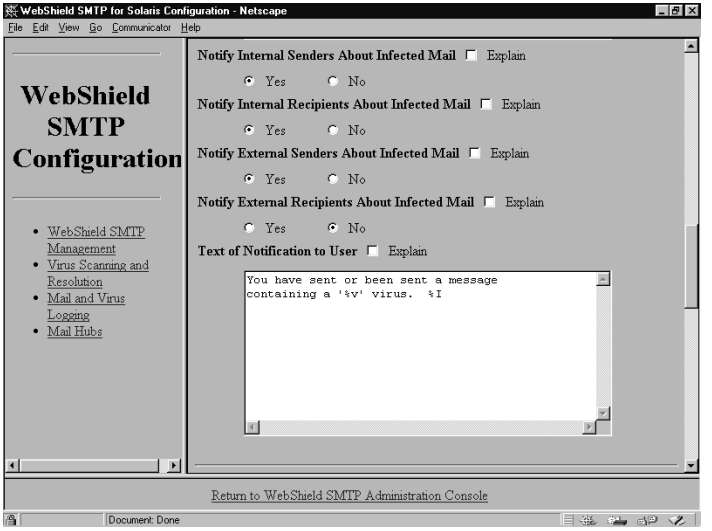


Figure 4-7. Virus Scanning and Resolution control panel User Notification options

Preservation of Detected Viruses

To save copies of infected files in a quarantine directoryyou can examine later, select Yes beneath the Preserve Infected Mail label (Figure 4-8). he third section of the Virus Scanning and Resolution control panel appears in .

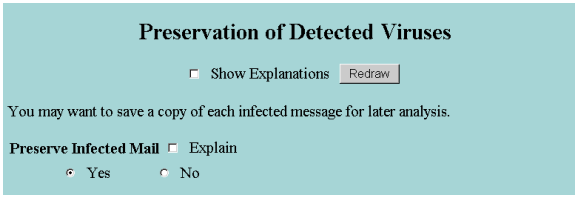


Figure 4-8. Virus Scanning and Resolution control panel Preservation of Detected Viruses section (detail)

WebShield SMTP will quarantine these copies in the directory `/var/infections` on the WebShield SMTP server. To retrieve them, use the Export Quarantined Files function described on page 55.

Cleaning and Forwarding Infected Mail

Preserving infected files in a quarantine directory allows you to send unusual virus types to Network Associates for analysis, or to determine if you have a pattern of virus infections in certain file types or from particular origination points. Figure 4-9.

Figure 4-9. Virus Scanning and Resolution control panel Cleaning Infected Mail and Forwarding of Infected Mail sections

To clean infected files that WebShield SMTP finds in your inbound or outbound mail, click Yes beneath the appropriate label. WebShield SMTP will use the information available in its data (DAT) files to scan all messages and attachments it can unpack while still providing optimal mail gateway transfer rates.

WebShield SMTP can remove most of the viruses that it finds in e-mail attachments. Removing a virus usually restores the infected file to its original state, without viral code. A small number of viruses, however, resist cleaning. If WebShield SMTP cannot remove an infection from a file, by default it deletes the infected file from the server unless you have chosen to preserve infected files. See “Preservation of Detected Viruses” on page 43 for details.

Most administrators will not select Forward Infected Mail. However, if your intention is merely to track viruses, or if messages are so important that they must be transferred even though they contain a virus, select this option. WebShield SMTP can still log the occurrence of known viruses. (See “Mail and Virus Logging” on page 46.)

Update Page, Default Values, and Redraw Page commands

When you have finished making changes on the Virus Scanning and Resolution control panel, click Update Page (in the lower right corner) to enter your changes. Verify that WebShield SMTP saved your changes by making sure the page reappears with the correct information.

Other useful commands available at the bottom of this page are

- Default Values—click this button to see the default values for this page. To return to these values, click Update Page.
- Redraw Page—click to refresh the page view, especially to view the Explain and Show Explanation text. (See “Online help text” on page 68 for details.)

Mail and Virus Logging

WebShield SMTP keeps a thorough record of its scanning operations, noting in two separate log files when it detected a virus, what action it took to respond to the infection, and a number of related statistics. Because these log files accumulate a substantial amount of information, you might want to limit their size and the length of time WebShield SMTP retains them. To learn how to view or export the log files WebShield SMTP generates, see "WebShield SMTP Reports" on page 59.

Click Mail and Virus Logging in the left pane under WebShield SMTP Configuration to display the Mail and Virus Logging control panel (Figure 4-10).

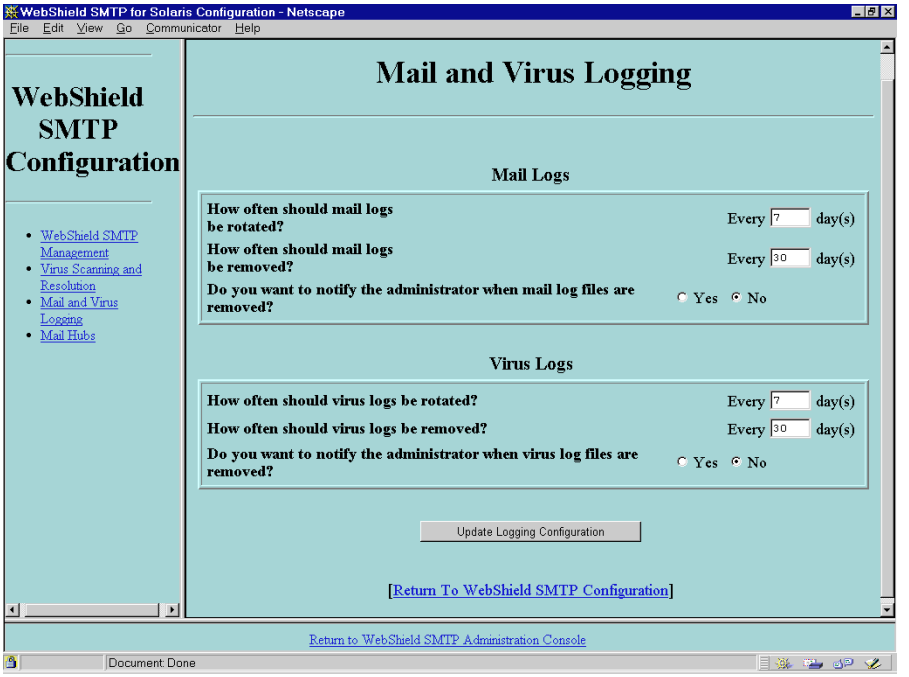


Figure 4-10. Mail and Virus Logging page

Mail and virus logs accumulate entries for the number of days that you enter in each Rotate field. WebShield SMTP then closes the log file and opens a new log in which it starts accumulating entries. That log file closes and a new log begins every *n* day(s).

Each closed log file remains on disk for the number of days that you enter in the Remove field. After that, WebShield SMTP deletes it.

Select Yes in reply to the Notify Administrator question if you want WebShield SMTP to notify you when it deletes a log file.

When you finish, click Update Logging Configuration to enter your settings. Verify that WebShield SMTP saved your changes by making sure the page reappears with the correct new information.

To configure other WebShield SMTP options, click a different link in the pane to the left.

Mail Hubs

After you install WebShield SMTP, you must configure it to deliver mail to and from your internal mail servers. Use this page (Figure 4-11) to specify how and where WebShield SMTP will send e-mail it has examined for viruses.

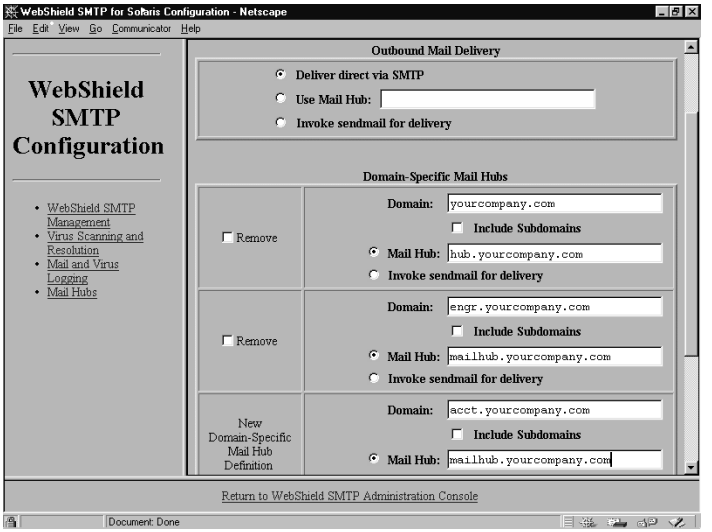


Figure 4-11. Mail Hubs control panel

Outbound Mail Delivery

You can choose to have WebShield SMTP send mail it has examined to recipients outside your network in one of three ways:

- If the existing sendmail configuration is standard, not customized, can mail reach the Internet directly? If so, select the 'Deliver direct via SMTP' button (Figure 4-12). This tells WebShield SMTP to use its native mail-handling utility to deliver mail to recipients outside your network.

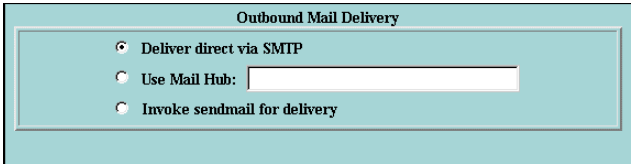


Figure 4-12. Outbound Mail Delivery detail (Deliver direct via SMTP)

- If you relay mail outside your network through a specific mail hub, and you have not customized your existing sendmail configuration, select the Use Mail Hub button and enter the domain name for the hub you want to use (Figure 4-13). This tells WebShield SMTP to use its native mail-handling utility to forward outbound mail directly to this hub.

Figure 4-13. Outbound Mail Delivery detail (Default relay)

- Is the WebShield SMTP server using a sendmail routing configuration that you have customized? If so, select the 'Invoke sendmail for delivery' button (Figure 4-14). This tells WebShield to use the sendmail utility already installed on your mail server to deliver mail outside your network.

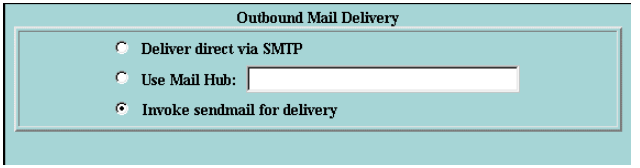


Figure 4-14. Outbound Mail Delivery (Invoke sendmail for delivery)

Defining Domain-Specific Mail Hubs for WebShield SMTP's internal network mail delivery

For mail that you route within your network, use the options provided in the Domain-Specific Mail Hubs area to specify where WebShield SMTP should forward mail it has scanned. You must enter the name of every domain in your network for which WebShield SMTP should accept mail. If WebShield SMTP does not recognize a domain to which mail is addressed, it will treat the mail as if outbound.

WebShield SMTP accepts but then discards mail if neither the sender's nor the recipient's domain is listed in this section. If it discards mail for this reason, WebShield SMTP will not log it and will not issue an error message to the sender.

To add a domain to this list, enter its name in the Domain text box at the top of each domain definition stanza, and then specify how WebShield SMTP should deliver mail for that domain.

Click Update Mail Hubs at the bottom of the page to save your changes and display a new domain-specific definition stanza. Continue entering domains until you have listed every domain, including virtual domains, for which you want WebShield SMTP to handle mail.

Specifying how mail is delivered for a domain

- Is the sendmail routing configuration for this subdomain or domain customized?
  - If yes, select Invoke sendmail for delivery.
  - If no, is WebShield SMTP the mail server for this subdomain or domain?
    - — If yes, then select Invoke sendmail for delivery.
    - — If no, then enter the name of the mail hub for the subdomain or domain, and select Mail Hub.

✍ *In the Domain-Specific Mail Hubs section, WebShield SMTP prefers the name of the mail hub, but it also allows the mail hub's IP address.*

If subdomains within a domain use the same routing as the parent domain, select the Include Subdomains checkbox beneath the parent domain name entry. You do not have to enter individual subdomains unless they use a different mail routing path. If a subdomain has a mail routing configuration different from its parent domain, however, you must enter the name of the subdomain in the Domain text box of a new domain-specific definition form.

- Does this domain have any subdomains for which mail is handled differently?
  - If no, select the Include Subdomains checkbox. You do not need to list the subdomains individually.
  - If yes, you must enter each subdomain in a new stanza.

✍ *See "Suggested Reading" on page 70 for more details about mail routing.*

After entering a stanza, click Update Mail Hubs again to save your changes. WebShield SMTP will display an error message if your changes cannot be saved. You will know that your changes were saved when the page reappears displaying your new entries and no error message. (See "Error handling" on page 67 for more details.)

Continue entering stanzas until you have entered each internal domain and virtual domain which WebShield SMTP should handle.

To choose other WebShield SMTP options, click a different link in the pane to the left. To go to any other page in the console, click Return to WebShield SMTP Administration Console at the bottom of the console window.

WebShield SMTP System Maintenance

WebShield SMTP groups a number of common maintenance functions in the WebShield SMTP Maintenance page. To display this page, first click the Return to WebShield SMTP Administration Console link to display the initial Administration Console page, then click the System Maintenance link in the pane to the left. The WebShield SMTP Maintenance page tells you whether the program is active and lists the data (DAT) file version it is using (Figure 4-15). To perform on of the administration functions listed, click the corresponding link to the left.

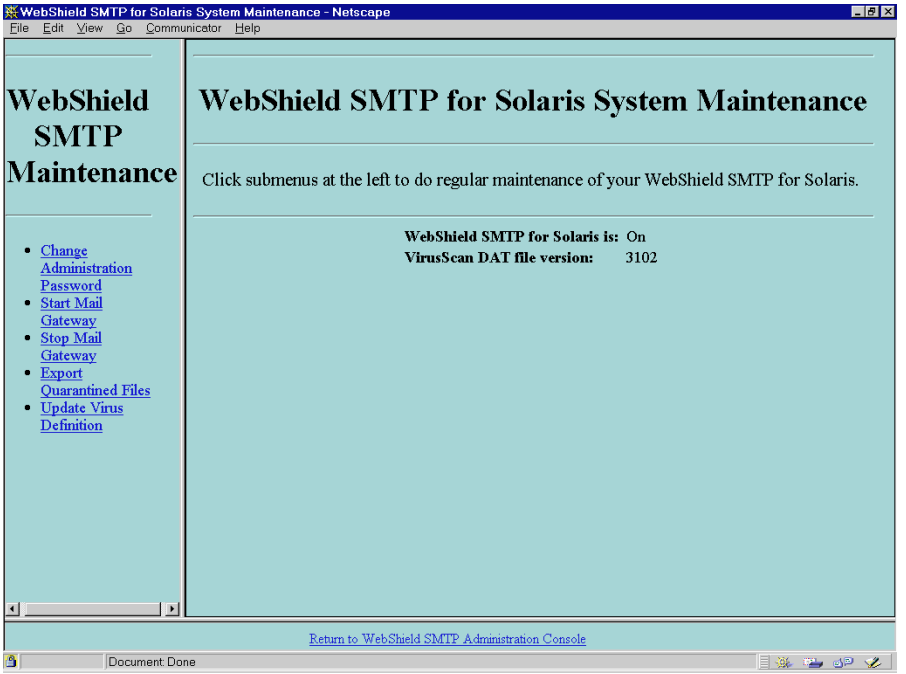


Figure 4-15. System Maintenance page

Change Administration Password

Use the Change Administration Password page (Figure 4-16) to enter or change the password you use to connect to the Administration Console and to administer WebShield SMTP.

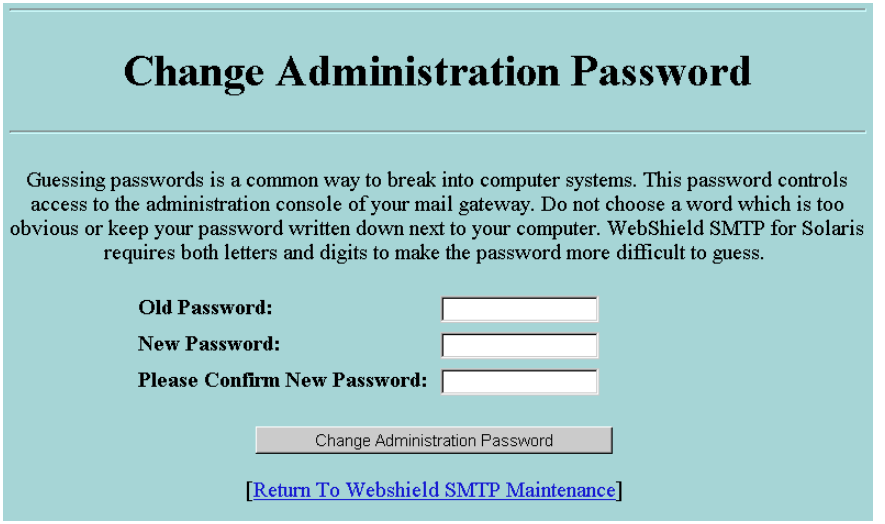


Figure 4-16. Change Administration Password control panel

WebShield SMTP requires a password composed of at least 6 characters, both numerals and lower- and uppercase letters. It will reject a password composed only of letters of a single case, or only of numerals. Choose your password with care. Do not use a password that others who know basic information about you, such as a birthdate, can guess.

✍ *Do not write down your password where unauthorized people might find it.*

Enter your new password again to confirm it, then click Change Administration Password to save it.

To choose other WebShield SMTP maintenance options, click a different link in the pane to the left.

Start Mail Gateway

After you first install it, WebShield SMTP is active by default and the mail gateway is enabled. If for some reason you need to restart WebShield SMTP, click Start Mail Gateway under WebShield SMTP Maintenance, and the Start Mail Gateway form (Figure 4-17) appears.

Click Start to activate your mail gateway and start WebShield SMTP.

Figure 4-17. Start Mail Gateway form

Stop Mail Gateway

Disabling your mail gateway also shuts down WebShield SMTP and means, in most cases, that your mail traffic flow stops. To disable your gateway, go to the WebShield SMTP Maintenance configuration page, then click Stop Mail Gateway. Next, confirm that you want to stop the gateway by clicking the Stop button in the right pane (Figure 4-18).

Figure 4-18. Stop Mail Gateway form

This deactivates your mail gateway and stops all WebShield SMTP functions, but you can still use the administration console. Mail deliveries in progress will continue until complete, but your gateway will not accept any new mail routed from inside or outside your network until you enable your mail gateway again. Messages awaiting delivery will queue on sender' machines in the meantime.

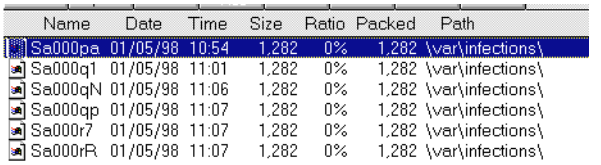
Export Quarantined Files

To save any infected files that you've chosen to preserve on your local system in order to analyze them or to send them to Network Associates for analysis, you first need to export them. Click Export Quarantined Files to see a list of the files WebShield SMTP has saved, if any (Figure 4-19).

If you told WebShield SMTP to preserve copies of files containing viruses (see “Preservation of Detected Viruses” on page 43), you may see a list of files resembling those shown in Figure 4-19.

Figure 4-19. Export Quarantined Files example list

Select the checkboxes for the infected files you want to examine, then click Export Quarantined File(s) at the bottom of the list. If you select more than one file, WebShield SMTP will send the files to your browser in the POSIX tar archive format. Use your browser to save the files you receive to a safe location. Because each file contains a virus, you should save it to a machine that is not a vital component of your network.



Name	Date	Time	Size	Ratio	Packed	Path
Sa000pa	01/05/98	10:54	1,282	0%	1,282	\var\infections\
Sa000q1	01/05/98	11:01	1,282	0%	1,282	\var\infections\
Sa000qN	01/05/98	11:06	1,282	0%	1,282	\var\infections\
Sa000qp	01/05/98	11:07	1,282	0%	1,282	\var\infections\
Sa000r7	01/05/98	11:07	1,282	0%	1,282	\var\infections\
Sa000rR	01/05/98	11:07	1,282	0%	1,282	\var\infections\

Figure 4-20. Exported, Archived, Quarantined Files example

✍ *If you cancel an export, some browsers will report incorrectly that the export completed successfully.*

✍ *Some browsers may save the archived files with the extension .cgi.*

Network Associates recommends that you save these files to a UNIX system, since most viruses cannot infect UNIX systems. Once you save the files, you can unpack them for analysis (Figure 4-20 on page 56).

To choose other WebShield SMTP options, click a different link. To display the initial WebShield configuration page, click Return to WebShield SMTP Administration Console.

Update Virus Definition Files

Every month more than 200 new viruses enter the worldwide viral pool and put your network at risk. To combat these new viruses, Network Associates provides monthly updates to its (DAT) data files so that Network Associates software can detect and remove them from your system. You can update the WebShield SMTP virus definition files in the following ways:

- Download the current zipped data files from the Network Associates FTP site. Select the Import from Network Associates FTP site button to connect directly with the correct site.

- Use data files stored elsewhere on your system or on your network. Specify the path and filename to use in the text box provided Figure 4-21 on page 58). Use standard UNIX notation to locate the correct file.Import from a file on your system containing the current (DAT) data file.

  ✍ *Network Associates DAT files are available from America Online, CompuServe, and other sources. (See "How To Contact Network Associates" on page 8.) New versions are generally published monthly, close to the middle of the month.*

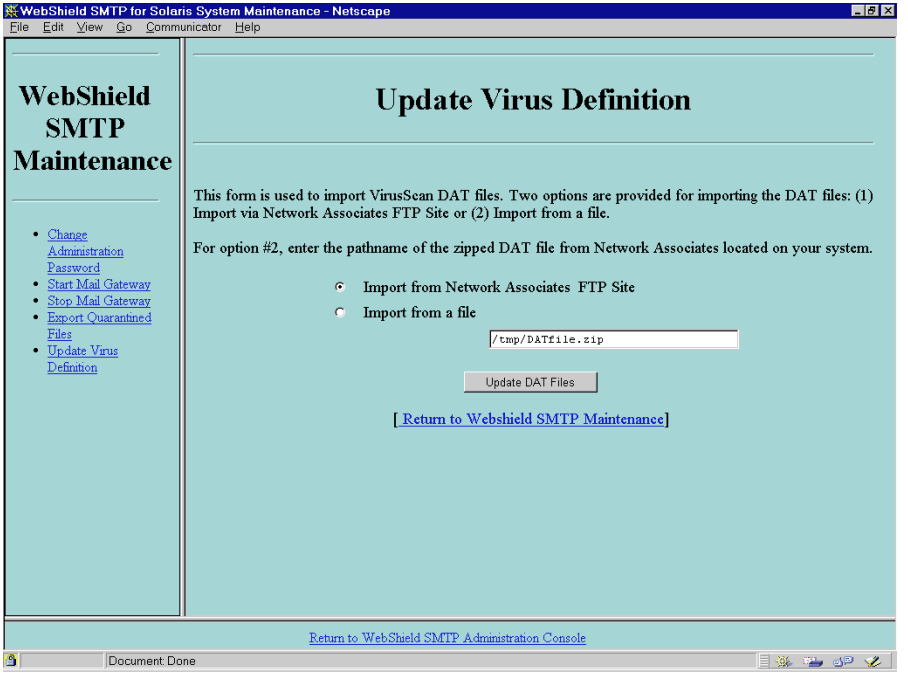


Figure 4-21. Update Virus Definition control panel

To choose additional WebShield SMTP options or to verify the version of DAT files that WebShield SMTP is using, click Return to WebShield SMTP Administration Console at the bottom of the page, then click Reports and Statistics in the left pane. The page that appears lists the current DAT file version.

WebShield SMTP Reports

To monitor WebShield SMTP scanning operations on your network, you can view the log files the program keeps or see a statistical summary of its activity. Click WebShield SMTP Reports in the initial Administration Console configuration page to see the program's current status and the data (DAT) file version it is using (Figure 4-15).

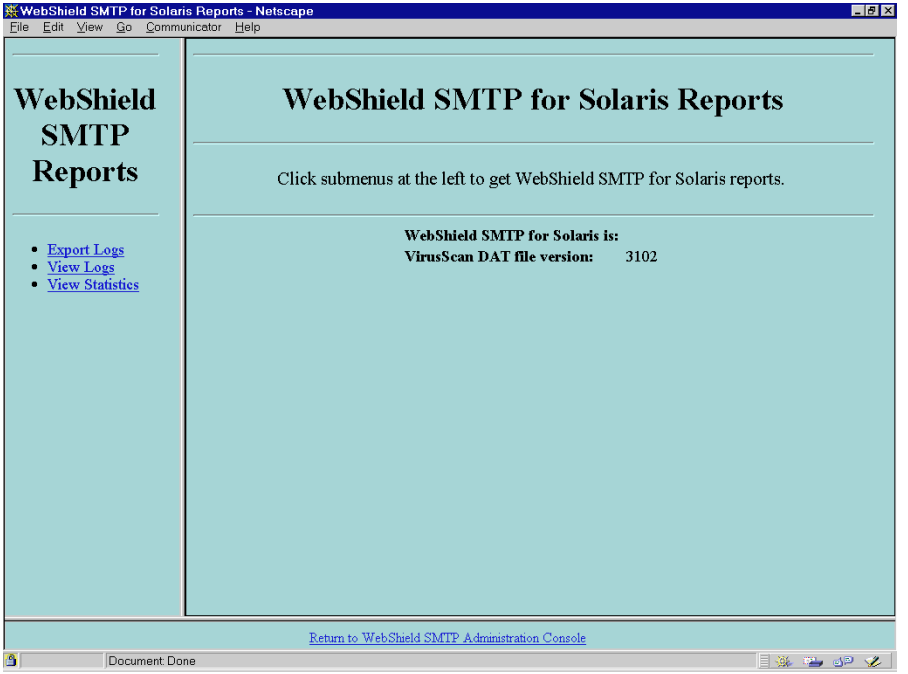


Figure 4-22. WebShield SMTP Reports page

Click the link in the pane to the left that corresponds to the report you want to see or download.

Export Logs

To save WebShield SMTP log files to your local system so you can view them or send them to others, click Export Logs in the left pane, then click the Export Log Now button in the right pane (Figure 4-23).

Figure 4-23. Export Logs form

WebShield SMTP will send its log files to your browser in the POSIX tar format. You can unpack these archived files for viewing later.

If you cancel an export operation, some browsers will report incorrectly that the export completed successfully.

To see or save additional WebShield SMTP reports, click a different link. Click Return to WebShield Administration Console to display the initial WebShield SMTP configuration page.

View Logs

To see the WebShield SMTP log files in your browser window, click View Logs in the left pane of the WebShield SMTP Reports window. The log file you choose will appear in the right pane (Figure 4-24 and Figure 4-25).

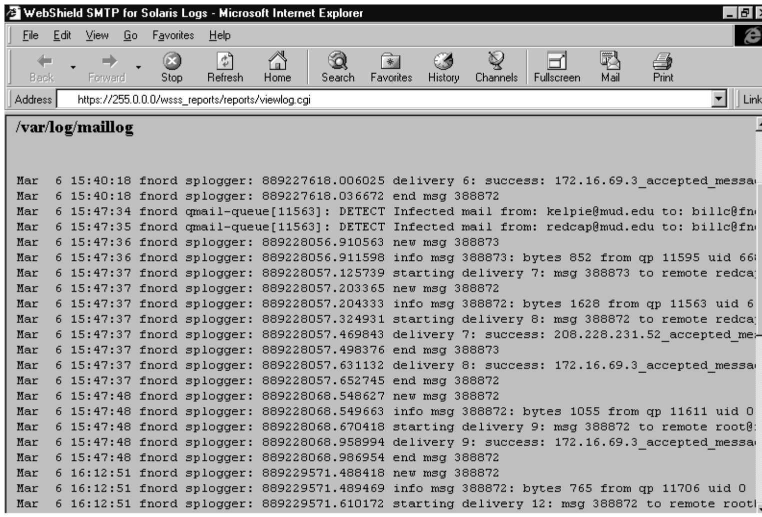


Figure 4-24. View Logs example of mail log report

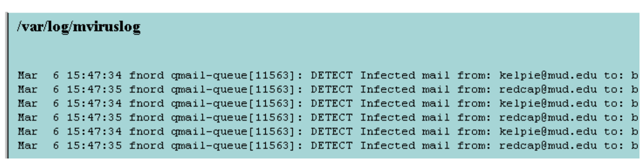


Figure 4-25. View Logs example of mail virus log report

To see or save additional WebShield SMTP reports, click a different link. Click Return to WebShield Administration Console to display the initial WebShield SMTP configuration page.

View Statistics

To see a statistical summary of WebShield SMTP activity in your browser window, click View Statistics in the left pane (Figure 4-26).

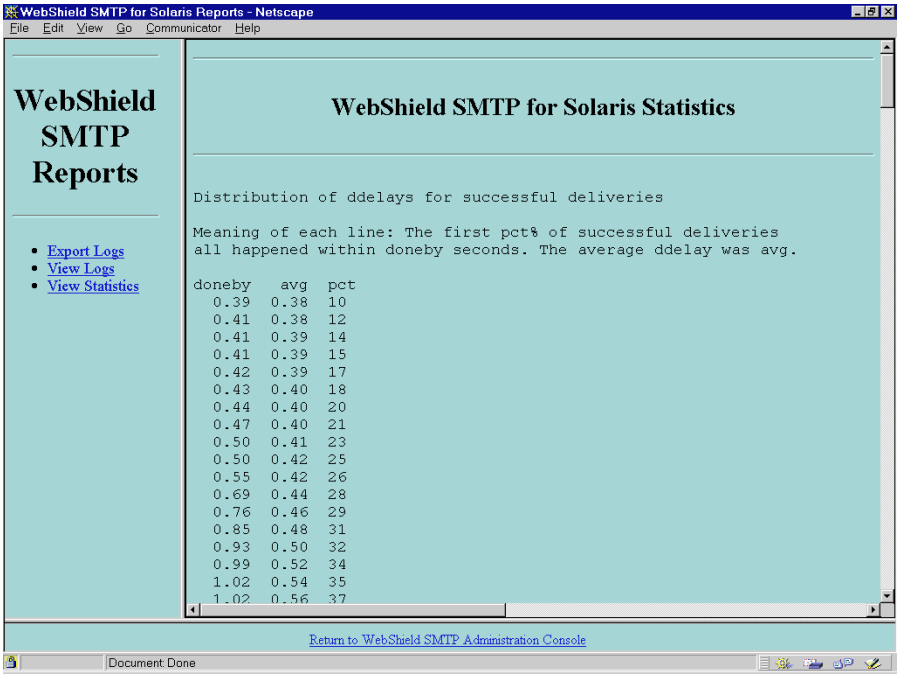


Figure 4-26. View Statistics example report

The summary will include the following sections:

- Distribution of delays for successful deliveries
- Reasons for deferral
- Reasons for failure
- Basic statistics
- Recipients
- Recipient hosts
- Recipients in the best order for mailing lists
- Senders
- Reasons for success

- Sender uids
- Number of messages delivered via sendmail
- Number of viruses detected

To see or save additional WebShield SMTP reports, click a different link. Click Return to WebShield Administration Console to display the initial WebShield SMTP configuration page.

Show Full Configuration

WebShield SMTP records and summarizes the configuration options you chose in each of the other configuration pages in the WebShield SMTP Full Configuration page. To see these settings, click Return to WebShield SMTP Administration Console, then click Show Full Configuration in the left pane. The WebShield SMTP Full Configuration page (Figure 4-27) appears in the right pane of the console.

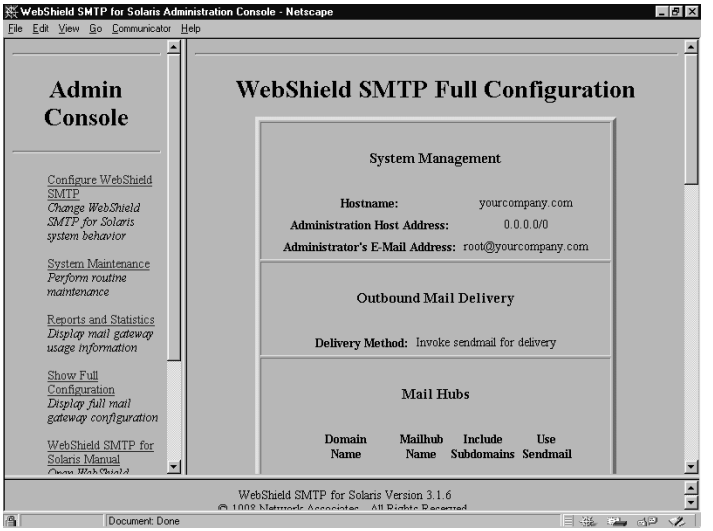


Figure 4-27. Full Configuration page (upper sections)

The sections System Management, Outbound Mail Delivery, and Mail Hubs appear in the upper part of the page. Scroll down to see the center sections, Virus Scanning and Virus Resolution, which also appear on the WebShield SMTP Configuration Summary page (Figure 4-1 on page 34) each time you open or return to the initial WebShield SMTP Adminstration Console view. Continue scrolling down to see the lower sections: Administrator Notification of Viruses, User Notification of Viruses, Mail Log Management, and Virus Log Management.

✍ *You may not edit the settings shown on this page. To change your configuration options, return to the pages that you used to set them originally.*

Online Manual and Virus Information

To use your browser to see this User's Guide online, you must first have an Adobe Acrobat Reader plug-in for your browser. Adobe's free Acrobat Reader package, available from **www.adobe.com/prodindex/acrobat/readstep.html**, automatically installs a plug-in suited to your browser. If you use Internet Explorer 4.0, Adobe has an ActiveX control available for viewing Acrobat .pdf documents with this browser at: **www.adobe.com/supportservice/custsupport/LIBRARY/44ae.htm**.

Once you have Acrobat Reader or an Acrobat plug-in available, click WebShield SMTP for Solaris Manual in the left pane of the initial Administration Console window. If you have the Acrobat Reader available, a second window will open to display the *User's Guide*. If you have the Acrobat Reader plug-in or ActiveX control installed, the *User's Guide* will appear in the right pane. Use your browser's navigation buttons to move between the *User's Guide* and WebShield SMTP configuration pages. You can also print the *User's Guide* from either source.

To view the Network Associates Virus Information Library, click Virus Information in the left pane. If you also installed the `NETAvil` package when you installed WebShield SMTP, your server will send the library information to your browser directly. If you did not installl the `NETAvil` package, your browser willl connect to the Network Associates website to retrieve the virus library.

Safeguards and Help

Read-Only, Locking, and the Override command

WebShield SMTP has a lock-out feature that prevents other administrators from making changes to your configuration options while you are using the Administration Console. WebShield SMTP does not lock you out when you try to view pages or reports that do not allow you to update configuration data. If you try to link to a configuration page that another administrator is using, WebShield SMTP displays the message shown in Figure 4-28.

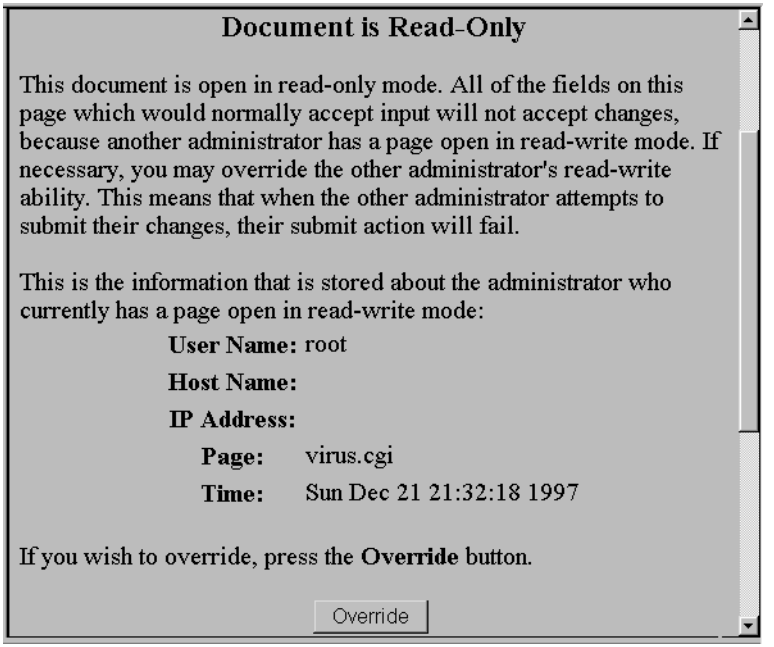


Figure 4-28. WebShield SMTP Console Read-Only message and Override option

The feature includes an override option that allows you to use the page even if another administrator is making changes. If you override the lock, the other administrator cannot save his or her configuration changes.

You must use your judgment about when to use the Override option. The administrator's User Name, the Host Name and IP Address of the system the administrator is using to configure WebShield SMTP, and the name of the configuration page the other administrator is viewing appear on the Read-Only window (Figure 4-28 on page 66). You must decide whether you want to interrupt his or her configuring activity. The time shown on the Read-Only window will also give you a clue about the legitimacy of the other user's lock—if the date is a few weeks ago, for example, you might consider the lock to be less valid than if you saw that the lock was created only a minute ago.

Error handling

The WebShield SMTP Administration Console provides data-checking error handling. While you configure WebShield SMTP, it checks the data you enter for errors. If it detects an error, WebShield SMTP does not update the configuration. Instead, it redisplays the configuration page with an error message at the top of the page. Typically, the error message will appear highlighted in red, as shown in Figure 4-29 on page 68.

At least two kinds of WebShield SMTP data errors are possible:

- Incorrect data format of data entered for a particular type of response
- Conflicting data entered

✍ *You must fix all data errors before the console allows you to go to another page.*

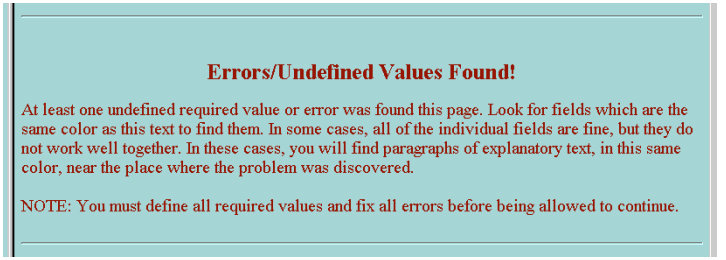


Figure 4-29. Red-Highlighted Error Message example

Online help text

WebShield SMTP provides you with detailed online explanations of its configuration options. The explanatory text does not appear by default so that you can move quickly through the configuration page.

To see the help text for an entire page, select the Show Explanations checkbox under the page heading, then click Redraw. To see explanations for particular sections, select the checkbox under the heading for each section, then click any Redraw button, or scroll to the bottom of the page and click Redraw Page. Your console view will be refreshed with additional text; you can then scroll down to the section you want to see.

To see the help text for a particular option, not for a whole section, select the Explain checkbox for that option only, then click Redraw. To see explanations for several options in different sections without viewing the entire help text for any section, select the Explain checkboxes for the various options you want, then click any Redraw button, or scroll to the bottom of the page and click Redraw Page.

A Reporting New Viruses

Network Associates 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 Network Associates reserves the right to use any information you supply as it deems appropriate, without incurring any obligations whatsoever. Send your suggestions to:

AVResearch@nai.com

To report new virus strains to our European research office, use this e-mail address:

virus_research_europe@cc.nai.com

To report items to our Pacific Rim research office, or our office in Japan, use one of these e-mail addresses:

Japan	avert-jp@ccj.nai.com
Pacific Rim	avert_apac@ccj.nai.com

B Suggested Reading

REFERENCE BOOKS

- *Solaris Performance Tuning*, by Adrian Cockroft. Published by Sun Press.

The following books are published by O'Reilly & Associates. Visit **http://www.ora.com** for more details.

- *UNIX in a Nutshell*
- *DNS and BIND*, 2nd Edition
- *sendmail*, 2nd Edition

docs.sun.com

Visit **http://www.sun.com/** to learn more about administering Solaris-based servers.

System Administration/Solaris 2.6 System Administrator Collection Vol 1/ Mail Administration Guide

sendmail

http://www.sendmail.org

Visit **http://www.sendmail.org/virtual-hosting.html** to learn more about **virtual domains** in e-mail.

SSL (secure sockets layer)

www.netscape.com/assist/security/ssl

www.mit.edu/pub/usenet/comp.mail.misc

UNIX Email Software Survey FAQ

sendmail FAQ

SMTP–Related RFCs (Requests for Comment) of the IETF (Internet Engineering Task Force)

Visit **http://ds.internic.net** for a complete list of RFC documents. Documents of particular interest include:

RFC 821 (Simple Mail Transport Protocol)

RFC 822 (Internet Mail Format Protocol)

RFC 1123 (Internet Host Requirements)

RFC 1521 (MIME—Multi-purpose Internet Mail Extensions)

RFC 1651 (SMTP Service Extensions)

RFC 1891 (SMTP Delivery Status Notifications)

RFC 1892 (Multipart/Report)

RFC 1893 (Mail System Status Codes)

RFC 1894 (Delivery Status Notifications)

RFC 1985 (SMTP Service Extension for Remote Message Queue Starting)

C Network Associates Support Services

Choosing Network Associates anti-virus and security software helps to ensure that the critical information technology you rely on functions smoothly and effectively. Taking advantage of a Network Associates support plan extends the protection you get from your software by giving you access to the expertise you need to install, monitor, maintain and upgrade your system with the latest Network Associates technology. With a support plan tailored to your needs, you can keep your system or your network working dependably in your computing environment for months or years to come.

Network Associates support plans come under two general headings. If you are a corporate customer, you can choose from three levels of extended support under the Network Associates PrimeSupport program. If you purchased a retail version of a Network Associates product, you can choose a plan geared toward your needs from the Personal Support program.

PrimeSupport Options for Corporate Customers

The Network Associates PrimeSupport program offers a choice of Basic, Extended, or Anytime options. Each option has a range of features that provide you with cost-effective and timely support geared to meet your needs.

PrimeSupport Basic

PrimeSupport Basic gives you telephone access to essential product assistance from experienced Network Associates technical support staff members. If you purchased your Network Associates product with a subscription license, you receive PrimeSupport Basic as part of the package for two years from your date of purchase. If you purchased your Network Associates product with a perpetual license, you can renew your PrimeSupport Basic plan for an annual fee.

PrimeSupport Basic includes these features:

- Telephone access to technical support from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website

PrimeSupport Extended

PrimeSupport Extended gives you personalized, proactive support from an assigned technical support engineer. You'll enjoy a relationship with a support professional who is familiar with your Network Associates product deployment and support history, and who will call you at an interval you designate to verify that you have the knowledge you need to use and maintain Network Associates products. By calling in advance, your PrimeSupport Extended representative can help to prevent problems before they occur. If, however, an emergency arises, PrimeSupport Extended gives you a committed response time that assures you that help is on the way. You may purchase PrimeSupport Extended on an annual basis when you purchase a Network Associates product either with a subscription license or a perpetual license.

PrimeSupport Extended includes these features:

- Access to an assigned technical support engineer
- Proactive support contacts via telephone or e-mail from your assigned support engineer, at an interval you designate
- Committed response times: your support engineer will respond within one hour to pages, within four hours to voicemail, and within 12 hours to e-mail
- Telephone access to technical support from Monday through Friday, 7:00 a.m. to 7:00 p.m. Central Time.
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website.
- Updates to data files and product upgrades via the Network Associates website
- Ability to designate up to five people in your organization as customer contacts

PrimeSupport Anytime

PrimeSupport Anytime offers round-the-clock, personalized, proactive support for Network Associates products deployed in the most business-critical information systems. PrimeSupport Anytime delivers the features of PrimeSupport Extended 24 hours a day, seven days a week, with shorter response time commitments. You may purchase PrimeSupport Anytime on an annual basis when you purchase a Network Associates product either with a subscription license or a perpetual license.

PrimeSupport Anytime includes these features:

- Access to an assigned technical support engineer
- Proactive support contacts via telephone or e-mail from your assigned support engineer, at an interval you designate
- Committed response times: your support engineer will respond within half an hour to pages, within one hour to voicemail, and within four hours to e-mail
- Telephone access to technical support 24 hours a day, seven days a week
- Unrestricted access 24 hours per day to Network Associates technical support information via the Network Associates website
- Updates to data files and product upgrades via the Network Associates website
- Ability to designate up to 10 people in your organization as customer contacts

PrimeSupport At a Glance

Feature	Basic	Extended	Anytime
Technical support via telephone	Monday–Friday 8:00 a.m.–8:00 p.m.	Monday–Friday 7:00 a.m.–7:00 p.m.	24 hours a day, 7 days a week
Technical support via website	Yes	Yes	Yes
Software updates	Yes	Yes	Yes
Assigned support engineer	—	Yes	Yes
Proactive support contact	—	Yes	Yes
Designated customer contacts	—	5	10
Committed response time	—	Pager: 1 hour Voicemail: 4 hours E-mail: 12 hours	Pager: 30 mins. Voicemail: 1 hour E-mail: 4 hours

Ordering PrimeSupport

To order PrimeSupport Basic, PrimeSupport Extended or PrimeSupport Anytime for your Network Associates products:

- Contact your sales representative; or
- Call Network Associates Support Services at 1-800-988-5737 or 1-650-473-2000 from 6:00 a.m. to 5:00 p.m. Pacific Time, Monday through Friday.

The PrimeSupport program described in this guide is available in North America only. To learn about PrimeSupport options available outside North America, contact your regional sales office. Contact information appears near the front of this guide.

Support Services for Retail Customers

If you purchase your Network Associates product through a retail vendor or from the Network Associates website, you also receive some support services as part of your purchase. The specific level of included support depends on the product that you purchased. Examples of the services you receive include:

- Free data (.DAT) file updates for the life of your product via the Network Associates website, your product's AutoUpdate feature, or the SecureCast service. You can also update your data files by using your web browser to visit http://www.nai.com/download/updates/updates.asp.
- Free program (executable file) upgrades for one year via the Network Associates website, your product's AutoUpdate feature, or the SecureCast service. If you purchased a deluxe version of a Network Associates product, you receive free program upgrades for two years. You can also upgrade your software by using your web browser to visit:

  http://www.nai.com/download/upgrades/upgrades.asp.
- Free access 24 hours a day, seven days a week to online or electronic support through the Network Associates voice and fax system, the Network Associates electronic bulletin board system or website, and though such other electronic services as America Online and CompuServe.

  To contact Network Associates electronic services, choose one of these options:

  - Automated voice and fax system: (408) 988-3034
  - Network Associates electronic bulletin board system): (408) 988-4004
  - Network Associates website: http://www.nai.com
  - CompuServe: GO NAI
  - America Online: keyword NAI
- Ninety days of complimentary technical support from a Network Associates support technician during regular business hours, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time.

After your complimentary support period expires, you can take advantage of a variety of personal support options geared toward your needs. Contact Network Associates Customer Care at (972) 278-6100 to learn more about the options available, or visit the Network Associates website at:

http://www.nai.com/services/support/support.asp.

Network Associates Consulting and Training

Network Associates provides expert consulting and comprehensive education that can help you maximize the security and performance of your network investments through the Network Associates Total Service Solutions program.

Professional Consulting Services

Network Associates Professional Consulting Services is ready to assist during all stages of your network growth, from planning and design, through implementation, and with ongoing management. Network Associates consultants provide an expert supplemental resource and independent perspective to resolve your problems. You'll get help integrating Network Associates products into your environment, along with troubleshooting assistance or help in establishing baselines for network performance. Network Associates consultants also develop and deliver custom solutions to help accomplish your project goals—from lengthy, large-scale implementations to brief problem-solving assignments.

Total Education Services

Network Associates Total Education Services builds and enhances the skills of all network professionals through practical, hands-on instruction that you can take right back to your job. The Total Education Services technology curriculum focuses on network fault and performance management and covers problem solving at all levels. Network Associates also offers modular product training so that you understand the features and functionality of your new software.

You can enroll in Total Education Services courses year-round at Network Associates educational centers, or you can learn from customized courses conducted at your location. All courses follow educational steps along a learning path that takes you to the highest levels of expertise. Network Associates is a founding member of the Certified Network Expert (CNX) consortium.

To learn more about these programs, contact your sales representative or call Total Service Solutions at 1-800-395-3151.

Index

U

W