

User's Guide

GroupScan and GroupShield for Lotus Notes

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

COPYRIGHT

Copyright © 1997 by McAfee, Inc. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc. Notes security technology licensed from Sybari Software, Inc.

TRADEMARK NOTICES

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

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

FEEDBACK

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

Table of Contents

Chapter 1. Introducing GroupScan and GroupShield.....6

What are GroupScan and GroupShield for Lotus Notes?	6
Main features	7
GroupScan and GroupShield key components.....	8
How To Contact Us	9
Customer service	9
Technical support.....	9
McAfee training	11
International contact information.....	11

Chapter 2. Installing GroupScan and GroupShield12

Before You Start.....	12
System requirements	13
Installation for Windows 95.....	14
Installation for Windows NT	18
Automatic installation	18
Command-line installation.....	22
GroupScan Installation for Windows 3.1x.....	25
Installation for OS/2	27
GroupShield Installation for a NetWare Server.....	29
Automating Installation	32
Windows 95 and Windows NT automated installation	32
OS/2, Windows 3.1x, and NetWare automated installation	34
Uninstalling GroupScan and GroupShield	37
Automatically removing GroupScan and GroupShield.....	37

Manually removing GroupScan and GroupShield.....	37
Chapter 3. Using GroupScan and GroupShield.....	39
Overview.....	39
The GroupScan and GroupShield framework.....	39
Common features	40
What is NShield?	42
Using NShield	43
Detecting document infections.....	43
Prank mail detection	45
Server break-in attempts.....	45
Configuring NShield Options.....	46
What is NScan?	50
Using NScan	50
What is NWall?	53
Using NWall	53
NWall components.....	53
Sample NWall Job	56
What is the Quarantine Area?	60
Using the Quarantine Area	60
What is the Menu Add-in?	66
Using the Menu Add-in	66
What is the LiveNotes(tm) Administrator for GroupShield?	67
Enabling the LiveNotes Administrator for GroupShield.....	67
Configuring File Attachment Scanning	69
Scanning .ZIP files.....	71
Scanning .NSF Database Attachments	72
Appendix A. Preventing Virus Infection	74
Keys to a Secure Notes Environment.....	74
Updating Your Data Files	75
What is a data file?	75
Why would I need a new data file?	75

How to apply the data file.....	75
McAfee Virus Information Library.....	77
Appendix B. Understanding Notes Threats	78
Infected file attachments.....	78
Notes Trojan horses.....	78
Notes mail bombs	79
Notes as a carrier	79
Notes virus reproduction.....	80
Notes stealth viruses	80
Notes prank mailing	80
Notes worm attacks	81
Notes server attacks	81
Appendix C. Reference	82
NShield Command-line options	82
NShield NOTES.INI Settings	84
NScan Command-line Options	88
NScan NOTES.INI Settings	91
NWall command-line options for GroupShield	94
NWall NOTES.INI Settings for GroupShield	96
VirusScan Command-line Error Levels.....	100
Index	102

1

Introducing GroupScan and GroupShield

What are GroupScan and GroupShield for Lotus Notes?

GroupScan and GroupShield for Lotus Notes are two powerful software products designed to detect, prevent, and eliminate software viruses and other threats in the Lotus Notes environment. These products combine to provide complete client/server protection. They consistently and accurately identify both known and unknown viruses to help protect the data stored and distributed on Notes servers and clients running Windows NT, Windows 95, Novell Netware, Windows 3.1x and OS/2.

GroupShield provides continuous monitoring and protection of Lotus Notes servers without user intervention. GroupShield's firewall component, NWall, acts as a barrier between your organization and external organizations, analyzing messages as they enter and exit your mail stream. You can use GroupShield's NScan and NShield components to clean, quarantine, or delete virus-infected file attachments, Notes databases, and Notes mail messages.

GroupScan provides continuous monitoring and protection of Lotus Notes clients. You can use GroupScan's NScan and NShield components to clean, quarantine, or delete virus-infected file attachments, Notes databases, and Notes mail messages. GroupScan is also ideal for environments that use Notes document encryption and for providing local protection to mobile or disconnected clients.

GroupScan and GroupShield are important elements of a comprehensive security program that includes a variety of safety measures, such as regular backups, meaningful password protection, training, and awareness. We urge you to set up and comply with such a security program in your organization. For tips on creating a secure system environment, see [Appendix A, "Preventing Virus Infection."](#)

Main features

- Continuous monitoring and virus protection without user intervention
- User-initiated scanning and cleaning of potential viruses
- GroupShield real-time mail stream protection and cleaning, including support for Lotus Notes Mail Agents
- LiveNotes Administrator for GroupShield, a Notes-based interface to configure, monitor, and troubleshoot GroupShield components
- Domino Server protection with real-time document and file scanning to protect servers and client workstations from virus infection. Even protects users who are accessing a Domino-based server from any Web browser
- Virus quarantine area for all detected viruses and false alarm information
- Comprehensive protection against:
 - Infected file attachments—traditional file viruses embedded in a Notes file attachment
 - Notes Viruses—viruses that reproduces using a stored form, button, or hotspot
 - Stealth Viruses—viruses that reproduces using any rich text field in Notes R3
 - Trojan Horses—attacks implemented as buttons, macros, R4 hotspot macros, or Notes-stored forms
 - OLE Trojans or Droppers—viruses payload or attack implemented as an embedded OLE object
 - Notes prank mailing—forged mail sent anonymously
 - Notes server attacks—Notes attacks and viruses targeted specifically at servers

GroupScan and GroupShield key components

NScan

NScan is the on-demand or scheduled scanning and cleaning component. NScan detects and cleans native Notes viruses and infected file attachments.

NShield

NShield provides on-access protection by monitoring reads or writes to Notes databases and their file attachments.

NWall

The GroupShield component NWall performs “on the fly” scanning and cleaning of documents as they enter and exit your mail stream. It is also ideally suited for implementing advanced document routing applications.

LiveNotes Administrator for GroupShield

LiveNotes Administrator is a Notes database that provides a single interface to configure, monitor, and troubleshoot the key components of GroupShield.

Quarantine Area

The Quarantine Area is a Notes database that acts as a repository for all possible and confirmed viruses detected. The Quarantine Area also includes false alarm information. From this database, Notes administrators may analyze and trace new or unknown viruses.

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 by mail 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 (408) 988-3034
and Fax Response
System

Internet support@mcafee.com

McAfee BBS (408) 988-4004
1200 bps to 28,800 bps
8 bits, no parity, 1 stop bit
24 hours, 365 days a year

CompuServe	GO MCAFEE
America Online	keyword MCAFEE
Microsoft Network (MSN)	MCAFEE

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

For corporate-licensed users:

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

For retail-licensed users:

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

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

- Product name and version
- Computer brand, model, and any additional hardware
- Operating system type and version
- Lotus Notes platform and release number
- Network type and version
- Contents of your NOTES.INI, AUTOEXEC.BAT, CONFIG.SYS, and system LOGIN script, if applicable
- Specific steps to reproduce the problem, if applicable
- NOTES.RIP file

McAfee training

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

International contact information

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

McAfee Canada

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

McAfee Europe B.V.

Gatwickstraat 25
1043 GL Amsterdam
The Netherlands
Phone: (0) 31 20 5866100
Fax: (0) 31 20 5866101

McAfee France S.A.

50 rue de Londres
75008 Paris
France
Phone: 33 1 44 908737
Fax: 33 1 45 227554

McAfee Deutschland GmbH

Industriestrasse 1
D-82110 Germering
Germany
Phone: 49 89 89435600
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 GroupScan and GroupShield

Before You Start

This chapter explains how to install the GroupScan and GroupShield products in the Windows 95, Windows NT, Windows 3.1x, OS/2, and Novell Netware environments. Before proceeding, take a moment to review the system requirements and to check the system path for the Lotus Notes directory.

McAfee strongly recommends you use GroupScan and GroupShield in conjunction with VirusScan or NetShield, our comprehensive anti-virus products. Together, the products will provide you maximum protection for the information stored on your computer. GroupShield uses the NetShield Alert Manager, when enabled, to provide true enterprise notification of GroupShield events.

By installing VirusScan or NetShield before installing GroupScan/GroupShield, you will create a virus-free environment. Follow the procedures outlined in your VirusScan or NetShield User's Guide to ensure that your environment is virus-free.

System requirements

- IBM-compatible personal computer running Windows 95, Windows NT 3.5x or later, OS/2 2.x or later, or Novell NetWare 3.12 or later
- For GroupScan, Lotus Notes Release 3.0A or later
- For GroupShield, Lotus Notes Server Release 3.0A to later
- At least 2MB free hard drive space
- The Lotus Notes directory must be listed in the system path. This is required to allow the installation program to properly set up and configure the GroupShield databases.

Installation for Windows 95

Follow the steps outlined below to install GroupScan or GroupShield on a Windows 95 system. The same procedure is followed for installing GroupShield on a Lotus Notes server or GroupScan on a Lotus Notes Client workstation.

Step

Action

1. Start your computer.

 *To expedite GroupShield installation, shut down the Lotus Notes server before installing GroupShield.*

2. Do one of the following:

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

3. Select Run from the Start menu.

- If you are installing from CD-ROM, type:

`x:\OSpath\NotesVer\setup`

where x is the drive that contains the CD-ROM. Type `win95` in place of `OSpath` to specify your operating system. In place of `NotesVer`, enter the subdirectory for Notes3 or Notes4 to match your system. Click OK.

- If you are installing files downloaded from the McAfee Web Site or a network server, type:

`x:\path\setup`


where `x:\path` is the location of the files. Click OK.

Response: The Welcome screen is displayed.

4. Click Next to begin the installation.
5. Enter the Lotus Notes program directory in the space provided. Click Next to continue.
6. Enter the NOTES.INI file directory in the space provided. Click Next to continue.

Response: Setup will now display information about your Lotus Notes configuration.

7. Confirm that all the Lotus Notes information is correct. GroupScan/GroupShield will not install or run properly if this information is not correct. Click Back to make changes or Next to continue.
8. When prompted to enter the database Replica ID, do one of the following:
 - Select No to have Setup automatically create the Replica ID.
 - Select Yes and enter the Replica ID number if you would like to select a specific Quarantine Area Replica ID.

 *Choose this option when installing multiple Notes servers and/or clients and you want to centrally manage the Quarantine Area. For more information on the Quarantine Area, see "What is the Quarantine Area?" on page 60.*

9. Click Next to continue.

Response: GroupScan or GroupShield files are transferred to the Lotus Notes directories.

10. If the installation program locates a McAfee product on your system, you may be asked if you wish to use the previously installed on-demand scanner with your GroupScan or GroupShield product. Type \mathbb{Y} to link GroupScan or GroupShield to this scanner. If you type \mathbb{N} , the on-demand component of VirusScan, which is included as part of the GroupScan/GroupShield product, will be installed on your system in the GroupScan/GroupShield directory.

11. Select the GroupScan/GroupShield components you wish to activate.

- For normal installations select all options.
- Deselect NShield on systems used primarily as Mail Routers.

Click Next to continue.

12. Select NShield settings.


- For client installations, McAfee recommends having NShield on-access protection for all databases.
- For server installations, McAfee recommends having NShield active on Web databases.



Use LiveNotes Administrator for GroupShield to modify this setting after installation. You can use LiveNotes Administrator to configure protection for the Discussion and Document Library databases on the server.

Click Next to continue.

13. Select the default Notification list for GroupScan and GroupShield events.
 - Select Sender to inform the creator of the document that they have sent or saved an infected document.

 *Use LiveNotes Administrator to add additional persons or Notes groups (such as administrators) to the Notification list.*

Click Next to continue.

14. Select an installation directory. Click Next to continue.
15. Select a directory where temporary files may be placed during installation. Click Next to continue.
16. Select a Program Folder for the installation. Click Next to continue.

Response: Setup will now present a list of all the installation settings for your confirmation.

Action: Choose Back to change any of the settings or choose Next to continue the installation.

Response: GroupScan or GroupShield files are copied onto the system.

17. View the GroupScan or GroupShield documentation.
18. Installation is complete. Restart the Lotus Notes server for the changes to take effect.

Response: The system restarts. All changes are enabled. GroupScan/GroupShield is now running in Lotus Notes.

19. To scan your system now, See [“Using NScan” on page 50](#) for instructions on using NScan.


Installation for Windows NT

There are two ways to install GroupScan or GroupShield on a Windows NT system. You can install GroupScan or GroupShield from the Windows interface or you can install from a DOS command line. If you want to install from the command line, see [“Command-line installation” on page 22](#).

Automatic installation

Follow the steps outlined below to install GroupScan or GroupShield on a Windows NT system from the Windows interface. The same procedure is followed for installing GroupShield on a Lotus Notes server or GroupScan on a Lotus Notes Client workstation.

- | Step | Action |
|------|--|
| 1. | Start your computer.

 <i>To expedite GroupShield installation, shut down the Lotus Notes server before installing GroupShield.</i> |
| 2. | Do one of the following: <ul style="list-style-type: none">■ If you are installing from a CD, insert it into the CD-ROM drive.■ If you are installing from files downloaded from a BBS or the McAfee Web Site, decompress the zipped files into a directory on the network or your local drive. |
| 3. | Select Run from the Start menu in Windows NT 4.0 or from the File menu in Windows NT 3.5x. <ul style="list-style-type: none">■ If you are installing from CD-ROM, type: |

`x:\OSpath\NotesVer\setup`

where x is the drive that contains the CD-ROM. Type `winnt` in place of `OSpath` to specify your operating system. In place of *NotesVer*, enter the subdirectory for Notes3 or Notes4 to match your system. Click OK.

- If you are installing files downloaded from the McAfee Web Site or a network server, type:

`x:\path\setup`

where `x:\path` is the location of the files. Click OK.


Response: The Welcome screen is displayed.

4. Click Next to begin the installation.
5. Enter the Lotus Notes program directory in the space provided. Click Next to continue.
6. Enter the NOTES.INI file directory in the space provided. Click Next to continue.

Response: Setup will now display information about your Lotus Notes configuration.

7. Confirm that all the Lotus Notes information is correct. GroupScan/GroupShield will not install or run properly if this information is not correct. Click Back to make changes or Next to continue.
8. When prompted to enter the database Replica ID, do one of the following:

- Select No to have Setup automatically create the Replica ID.
- Select Yes and enter the Replica ID number if you would like to select a specific Quarantine Area Replica ID.


 *Choose this option when installing multiple Notes servers and/or clients and you want to centrally manage the Quarantine Area. For more information on the Quarantine Area, see [“What is the Quarantine Area?”](#) on page 60.*

9. Click Next to continue.


Response: GroupScan or GroupShield files are transferred to the Lotus Notes directories.

10. If the installation program locates a McAfee product on your system, you may be asked if you wish to use the previously installed on-demand scanner with your GroupScan or GroupShield product. Type **Y** to link GroupScan or GroupShield to this scanner. If you type **N**, the on-demand component of VirusScan, which is included as part of the GroupScan/GroupShield product, will be installed on your system in the GroupScan/GroupShield directory.
11. Select the GroupScan/GroupShield components you wish to activate.
- For normal installations select all options.
 - Deselect NShield on systems used primarily as Mail Routers.

Click Next to continue.

12. Select NShield settings.
- For client installations, McAfee recommends having NShield on-access protection for all databases.
 - For server installations, McAfee recommends having NShield active on Web databases.
-  *Use LiveNotes Administrator for GroupShield to modify this setting after installation. You can use LiveNotes Administrator to configure protection for the Discussion and Document Library databases on the server.*

Click Next to continue.

13. Select the default Notification list for GroupScan and GroupShield events.
- Select Sender to inform the creator of the document that they have sent or saved an infected document.
-  *Use LiveNotes Administrator to add additional persons or Notes groups (such as administrators) to the Notification list.*

Click Next to continue.

14. Select an installation directory. Click Next to continue.
15. Select a directory where temporary files may be placed during installation. Click Next to continue.
16. Select a Program Folder for the installation. Click Next to continue.

Response: Setup will now present a list of all the installation settings for your confirmation.

Action: Choose Back to change any of the settings or choose Next to continue the installation.

Response: GroupScan or GroupShield files are copied onto the system.

17. View the GroupScan or GroupShield documentation.
 18. Installation is complete. Restart the Lotus Notes server for the changes to take effect.
- Response:** The system restarts. All changes are enabled. GroupScan/GroupShield is now running in Lotus Notes.
19. To scan your system now, See [“Using NScan” on page 50](#) for instructions on using NScan.


Command-line installation

Follow the steps below to install GroupScan on a Lotus Notes client workstation and GroupShield on a Lotus Notes server from the DOS command-line in a Windows NT environment.


Step

Action

1. Open a DOS window.

 *To expedite GroupShield installation, shut down the Lotus Notes server before installing GroupShield.*

2. Do one of the following:
 - If you are installing from CD, insert it into the CD-ROM drive.
 - If you are installing files downloaded from a BBS or the McAfee Web Site, decompress the zipped files into a directory on the network or your local drive.

 *Please ensure that the Lotus Notes directory is listed in the system path before proceeding.*


3. At the prompt, use the `cd` command to change directories to the location of the files. Type `autoinst` and press ENTER.

Response: The GroupScan or GroupShield Welcome screen is displayed.

4. Type `Y` to proceed with installation.

Response: The GroupScan or GroupShield files are copied to the Lotus Notes directories.

5. Verify the Lotus Notes program path. Press ENTER.
6. Verify the Lotus Notes data directory. Press ENTER.
7. Verify the temporary directory that files will be placed in during installation. Press ENTER.
8. Type `Y` to activate NWall mail message scanning for GroupShield.
9. Type `Y` to activate NShield real-time scanning.

 *The files used by NShield are always copied to the Notes program directory, but the `NSF_HOOKS=nshield` setting in `NOTES.INI` is not set if you did not enable real-time scanning with NShield.*

10. Type `Y` to scan Web Navigator activity only.
11. Type `Y` to activate Event notifications by mail.

12. Verify the notification recipient list. Press ENTER.
13. If GroupScan or GroupShield locates a McAfee product on your system, you will be asked if you wish to use the previously installed on-demand scanner. Type **Y** to link GroupScan or GroupShield to this on-demand scanner. If you type **N**, the on-demand component of VirusScan, which is included as part of the GroupScan product, will be installed on your system in the GroupScan directory.
14. If you have not already configured Lotus Notes to associate API programs with your user ID, you will be prompted for your password. Type your password and press ENTER.
15. Installation is complete. Reboot your system for the changes to take effect.

Response: The system restarts. All changes are enabled.

16. To scan your system now, see [“Using NScan” on page 50](#) for instructions on using NScan.


GroupScan Installation for Windows 3.1x

Follow the steps below to install GroupScan on a Windows 3.1x client workstation.

Step

Action

1. Start your computer.
2. Do one of the following:
 - If you are installing from CD, insert it into the CD-ROM drive.
 - If you are installing files downloaded from a BBS or the McAfee Web Site, decompress the zipped files into a directory on the network or your local drive.

 *Please ensure that the Lotus Notes directory is listed in the system path before proceeding.*

3. Select Run from the File menu.

- If you are installing from CD-ROM, type

`x:\win\install`

where *x* is the drive that contains the CD-ROM. Click OK.

- If you are installing from downloaded files, type:

`x:\path\install`


where *x:\path* is the location of the files. Click OK.

Response: GroupScan searches for and displays the Lotus Notes directories.

4. Type **Y** to proceed with the installation.

Response: GroupScan files are transferred to the Lotus Notes directories.

5. If the installation program locates a McAfee product on your system, you may be asked if you wish to use the previously installed on-demand scanner with your GroupScan product. Type **Y** to link GroupScan to this scanner. If you type **N**, the on-demand component of VirusScan, which is included as part of the GroupScan product, will be installed on your system in the GroupScan directory.
6. If you have not already configured Notes to associate API programs with your user ID, you will be prompted for your Notes password. Type it when prompted, and press **ENTER**.
7. To install and activate NShield real-time scanning, type **Y**.

 *The files used by NShield are always copied to the Notes program directory, but the `NSF_HOOKS=nshield` setting in `NOTES.INI` is not set if you did not enable real-time scanning with NShield.*




8. GroupScan is installed. Reboot your system for the changes to take effect.

Response: The system restarts. All changes are enabled. GroupScan is now running in Lotus Notes.

9. To scan your system now, see [“Using NScan” on page 50](#) for instructions on using NScan.

Installation for OS/2

Follow the steps below to install GroupScan on a Lotus Notes client workstation and GroupShield on a Lotus Notes server in an OS/2 environment.

Step	Action
1.	<p>Close all DOS and Win-OS/2 sessions, open the Command Prompt folder, and click the OS/2 Full Screen or OS/2 Window icon.</p> <p> <i>To expedite GroupShield installation, shut down the Lotus Notes server before installing GroupShield.</i></p>
2.	<p>Do one of the following:</p> <ul style="list-style-type: none">▪ If you are installing from CD, insert it into the CD-ROM drive.▪ If you are installing files downloaded from a BBS or the McAfee Web Site, decompress the zipped files into a directory on the network or your local drive. <p> <i>Please ensure that the Lotus Notes directory is listed in the system path before proceeding.</i></p>
3.	<p>At the prompt, use the <code>cd</code> command to change directories to the location of the files. Type <code>install</code> and press ENTER.</p> <p>Response: The Lotus Notes directories are displayed.</p>
4.	<p>Type <code>Y</code> to proceed with installation.</p> <p>Response: The GroupScan or GroupShield files are copied to the Lotus Notes directories.</p>
5.	<p>Type <code>Y</code> to install and activate NShield real-time scanning.</p> <p> <i>The files used by NShield are always copied to the Notes program directory, but the <code>NSF_HOOKS=nshield</code> setting in <code>NOTES.INI</code> is not set if you did not enable real-time scanning with NShield.</i></p>

6. If GroupScan or GroupShield locates a McAfee product on your system, you will be asked if you wish to use the previously installed on-demand scanner. Type **Y** to link GroupScan or GroupShield to this on-demand scanner. If you type **N**, the on-demand component of VirusScan, which is included as part of the GroupScan product, will be installed on your system in the GroupScan directory.
7. If you have not already configured Lotus Notes to associate API programs with your user ID, you will be prompted for your password. Type your password and press **ENTER**.
8. Installation is complete. Reboot your system for the changes to take effect.


Response: The system restarts. All changes are enabled.


9. To scan your system now, see [“Using NScan” on page 50](#) for instructions on using NScan.

GroupShield Installation for a NetWare Server

Follow the steps outlined below to install GroupShield on a NetWare Lotus Notes server.

- | Step | Action |
|------|--|
| 1. | Start your computer.

 <i>To expedite GroupShield installation, shut down the Lotus Notes server before installing GroupShield.</i> |
| 2. | Use ALT+ESC to switch to the System console. |
| 3. | Do one of the following: <ul style="list-style-type: none">■ If you are installing from CD, insert it into the CD-ROM drive.■ If you are installing files downloaded from a BBS or the McAfee Web Site, decompress the zipped files into a directory on the network or your local drive.

 <i>Please ensure that the Lotus Notes directory is listed in the system path before proceeding.</i> |
| 4. | At the prompt, change directories to the location of the files. <ul style="list-style-type: none">■ If you are installing from CD-ROM, type:

<code>LOAD x:\nw\install</code>

where x is the drive that contains the CD-ROM. Click OK. |

- If you are installing from downloaded files or a network server, complete the following:

- At a NetWare client machine, map a NetWare volume and create a directory for GroupShield.

Example:

```
map x:=server name/volume name
```

```
MD x:\Gshield
```

where x is the drive that contains the files.

- Decompress the zipped files into the GroupShield directory.
- Initiate the installation by specifying the full path name including the actual volume name:


```
LOAD volume name/Gshield/Install
```

Response: GroupShield searches for and displays the Lotus Notes directories.

5. Type **Y** to proceed with installation.

Response: GroupShield files are copied to the Notes program and data directories.

6. If GroupShield locates a McAfee product on your system, you will be asked if you wish to use the previously installed on-demand scanner. Type **Y** to link GroupShield to this on-demand scanner.
7. If you have not already configured Lotus Notes to associate API programs with your user ID, you will be prompted for your password. Type your password and press **ENTER**.
8. Type **Y** to install and activate NShield real-time scanning.

 *The files used by NShield are always copied to the Notes program directory, but the `NSF_HOOKS=nshield` setting in `NOTES.INI` is not set if you did not enable real-time scanning with NShield.*

9. GroupShield is installed. Restart the Lotus Notes server for the changes to take effect.


Response: The system restarts. All changes are enabled. GroupShield is now running in Lotus Notes.

10. To scan your system now, See [“Using NScan” on page 50](#) for instructions on using NScan.

Automating Installation

Once GroupScan or GroupShield has been tested and configured on a single system, you may want to duplicate the configuration on additional systems (clients or servers). This is also beneficial for use with commercial software distribution packages. The GroupScan and GroupShield Installation programs provide automatic installations by initiating the following:

- Predefined responses to questions asked during the installation process
- Predefined values for any NOTES.INI setting used by GroupScan and GroupShield.
- Optional external program execution before and/or after the installation process.


 *Windows 95 and Windows NT versions of GroupScan and GroupShield use the InstallShield installer which provides a “silent” install capability. A command prompt installer is used for OS/2, Windows 3.1x, and NetWare systems. Please follow the instructions below based on your system’s installation capability.*

Windows 95 and Windows NT automated installation

The InstallShield-based setup program for Windows 95 and Windows NT platforms provides “record” and “playback” capabilities which can be used for silent installation on other systems.

Recording a response file

By running the GroupScan/GroupShield setup with the `SETUP.EXE -r` command line parameter, you can have InstallShield record your installation choices in a response file, which can be played back for silent installation on another computer. Your installation choices will be recorded in `SETUP.ISS` in the `WINDOWS` directory. The `SETUP.ISS` file is a text file, similar to an `.INI` file.

 *Experienced users may want to modify the `SETUP.ISS` file to create their own automatic install.*

Playing back the Silent Installation

After the response file (SETUP.ISS) is created, you are ready to run the installation in silent mode. No messages are displayed during a silent mode installation. However, the SETUP.LOG file captures installation information and specifies whether or not the installation was successful. Review the log file to determine the result of the installation.

To launch a GroupScan/GroupShield silent install, run `SETUP` with the `-s` option.

Additionally, the `-F1` and `-F2` switches can be used to specify the name and location of the response file and the location of the log file.

OS/2, Windows 3.1x, and NetWare automated installation

For OS/2, Windows 3.1x, and NetWare operating systems, automation of the installation process is controlled by the GroupScan.INI file or GroupShield.INI file. This file is a standard .INI text file that must exist in the same directory as the installation program. A sample file, AUTOINST.INI, is included on the GroupScan and GroupShield distribution disks.

The GroupShield AUTOINST.INI file includes the following:

 See [Appendix C, "Reference" on page 82](#) for a description of the following settings.

[Commands]

- ☐ Start=
- ☐ Finish=

[Settings]

- ☐ GroupShieldQArea=
- ☐ GroupShieldOptions=
- ☐ GroupShieldScanners=
- ☐ GroupShieldTempDir=
- ☐ GroupShieldMaxFile=
- ☐ GroupShieldNotifyList=
- ☐ GroupShieldNotifySubject=
- ☐ GroupShieldNotifyBody=
- ☐ GroupShieldDomain=
- ☐ GroupShieldCRCPool=
- ☐ GroupShieldNamePool=
- ☐ NShieldOptions=
- ☐ NShieldScanners=
- ☐ NShieldTempDir=
- ☐ NShieldMaxFile=
- ☐ GroupShieldTrustedTasks=
- ☐ NWallOptions=
- ☐ NWallScanners=
- ☐ NWallTempDir=
- ☐ NWallMaxFile=
- ☐ NWallDatabase=
- ☐ NWallView=

- ☐ NetwareLogin=
- ☐ NetwareDelay=
- ☐ NSF_HOOKS=
- ☐ AddinMenus=


[Responses]

- ☐ Do you wish to proceed with the installation? [Y/N]=
- ☐ Enter GroupShield source directory:=
- ☐ Notes program directory:=
- ☐ Notes data directory:=
- ☐ Would you like to activate NShield real-time scanning? [Y/N]=
- ☐ Would you like to activate NWall mail message scanning? [Y/N]=
- ☐ Would you like to activate NShield real-time scanning? [Y/N]=
- ☐ Would you like to setup file attachment scanning support? [Y/N]=
- ☐ Would you like to modify the Replica ID # ? [Y/N]=
- ☐ OVERWRITE THE FILE? [Y/N]=

The following examples are for establishing a temporary directory. Note that the second question is dependent on the first response.

- ☐ Temporary Directory:=
- ☐ C:\TEMP does not exist. Would you like to create it? [Y/N]=

The Commands section includes the Start and Finish settings. Any valid command specific to the current platform can be specified in this section.

 *This feature is very useful for performing pre-installation and post-installation tasks, such as installing antivirus file scanners.*

When creating the automated responses, you may specify default values to questions as well as automatic answers. For example, the response setting

Notes program directory:=C:\NOTES\PROG

automatically answers the question “Notes program directory:” With “C:\NOTES\PROG” followed by an ENTER keystroke. However, the response setting

Notes program directory:=?C:\NOTES\PROG

answers the question “Notes program directory:” with “C:\NOTES\PROG” but does not follow it with an ENTER keystroke. The installation program waits for the user to accept the default value or change it as needed. This feature is enabled by preceding the response with a question mark.

Sample GroupShield.INI:

[Commands]

- ❑ Start=DIR C:\TEMP
- ❑ Finish=LOADSCAN A:

[Settings]


- ❑ GroupShieldNotifySubject=Avast yee!
- ❑ GroupShieldMaxFile=1024
- ❑ NWallOptions= +N +M +A +F

[Responses]

- ❑ Do you wish to proceed with the installation? [Y/N]=Y
- ❑ Enter GroupShield source directory:=A:\
- ❑ Notes program directory:=C:\NOTES.400
- ❑ Notes data directory:=C:\DATA\NOTES
- ❑ Would you like to activate NShield real-time scanning? [Y/N]=Y
- ❑ Would you like to activate NWall mail message scanning? [Y/N]=Y
- ❑ Temporary Directory:=C:\TEMP

Testing the automated installation

To test the automated installation, use the `/T` command line option. The `/T` command line option runs through an installation without performing any action (copying files, etc.).

 *The `/T` option must be the only parameter specified.*

Uninstalling GroupScan and GroupShield

Automatically removing GroupScan and GroupShield

Windows NT and Windows 95

Launch the Uninstall program from the GroupScan/GroupShield for Notes program group. This will automatically remove the program.

OS/2, Windows 3.1, and NetWare

Run the installation program, INSTALL.EXE, from the original installation media that came with GroupScan and GroupShield with the `/U` command-line option. This will perform an automated removal of some or all GroupScan and GroupShield components.

Manually removing GroupScan and GroupShield

To manually remove GroupScan/GroupShield complete the following steps:

Step	Action
1.	Edit the NOTES.INI file and remove NShield and NWall from the NSF_HOOKS variable.
2.	Remove the following information from the NOTES.INI file: <ul style="list-style-type: none">■ NShield and NWall (or remove the entire line if no other information appears on that line).■ All lines that begin with GroupShieldxxxxx=, NShieldxxxxx=, or NWallxxxxx=.■ All references to NWALL or NSCAN in the ServerTasks entries in NOTES.INI.
3.	Remove or disable all program documents in the Name & Address Book that execute NSCAN or NWALL on the current system.

4. Shut down the Notes client, Notes server, and any active Notes applications.
5. Remove the following files from the Notes program directory:
 - \$NSHIELD.DLL, NNSHIELD.DLL, _NSHIELD.DLL, VNSHIELD.NLM
 - \$NMENU.DLL, NNMENU.DLL, _NMENU.DLL
 - \$NWALLM.DLL, NNWALLM.DLL, VNWALLM.NLM
 - \$NWALL.EXE, NNWALL.EXE, INWALL.EXE, VNWALL.NLM
 - NSCAN.EXE, NSCAN.NLM
6. Remove the NWall Jobs database, the Quarantine Area database, and the GroupShield Online Guide database from the Notes data directory or subdirectory.

Overview

The GroupScan and GroupShield framework

GroupScan and GroupShield are comprised of three components: NShield, NScan, and the Quarantine Area. GroupShield is comprised of two additional components, NWall, and LiveNotes Administrator. Together, the GroupScan and GroupShield components allow for comprehensive virus protection for Lotus Notes clients and servers. Each component can be configured to meet your specific needs.

- NShield continuously monitors and protects your network from potential viruses and software threats that may be introduced via Notes mail or replication. NShield works in real time to detect and disable viruses as they attempt to enter or move through the system.
- NScan helps you to maintain a virus-free environment on your Lotus Notes client and server by allowing you to perform active scans of your system. NScan detects all of today's known viruses and Notes software attacks, as well as new and unknown variants. NScan can intercept, clean, and log a Notes-based virus, bomb, Trojan horse or infected file attachment before it spreads through any Notes database application including Notes mail.
- The Quarantine Area is a Lotus Notes database that acts as a repository for all detected viruses as well as false alarm information. From this database, Notes administrators can analyze and trace the source of new or unknown viruses and establish a false alarm list to streamline virus detection in the Notes environment.

- NWall is the GroupShield component designed to scan all Notes mail messages and attachments as they are routed through the enterprise. NWall acts as a barrier between the internal Notes mail system and external mail systems.
- LiveNotes Administrator for GroupShield is a Lotus Notes database that acts as an interface for configuring, monitoring, and troubleshooting the GroupShield components. To set up the Administrator for GroupShield, see [“What is the LiveNotes\(tm\) Administrator for GroupShield?” on page 67](#).

Common features

All of the GroupScan and GroupShield components described above share a set of common features that make the suite flexible and easy to use. These features include:


- Detection and cleaning of Notes R3 and R4 macro viruses and bombs resident in stored forms, button macros, hotspot macros, LotusScript, and OLE embedded objects.
- Detection, identification, and automatic cleaning of infected file attachments.
- Centralized Notes-based monitoring and administration that is completely transparent to Notes users.
- A standard Notes Log database where information on activities can be viewed.
- Full infected documents copied to the Quarantine Area. All data fields are preserved to ensure no data loss. Full document restoration is also supported.
- An false alarm facility that allows administrators to identify quarantined documents as false alarms. Once a document is added to the false alarm list, GroupScan and GroupShield skip all documents that share the same design, reducing the number of false alarms that might occur.
- The ability to select databases to exclude from scanning.

Additional GroupShield components:

- An advanced Trust feature that allows servers running GroupShield to trust the scanning by other GroupShield protected servers in your Notes network. This boosts performance while introducing very little risk. The Trust feature also exists between the GroupShield components themselves, a message scanned by NWall will not be rescanned by NShield.
- Alert notification of GroupShield events via Notes Mail and McAfee Alert Manager.

Configuring GroupScan and GroupShield components


NScan, NShield, and NWall are enabled and configured through the settings in the NOTES.INI file.

 *For quick access to all GroupShield settings, open the LiveNotes Administrator database from your Notes client. To enable this utility, see [“What is the LiveNotes\(tm\) Administrator for GroupShield?”](#) on page 67.*

You can access the NOTES.INI file from the GroupScan or GroupShield Menu Add-in in Windows 95 and Windows NT. Select Edit NOTES.INI from the Tools menu (in Notes R3) or the Actions menu (in Notes R4) to configure the GroupScan or GroupShield components.

What is NShield?

NShield provides continuous, unobtrusive protection for Notes clients and servers without user intervention. NShield works by monitoring all reads and writes to the Notes system. NShield monitors processes and tasks, such as user sessions, add-in tasks, and Notes API programs. NShield is implemented as a Notes hook driver and is bound directly to the Lotus Notes database subsystem each time Lotus Notes is initialized.

 *If you routinely use encrypted documents in your Notes environment, you must use the NShield component in GroupScan on the Notes client machines to provide on-access scanning and protection of encrypted documents. When NShield is run on a server, it does not have the proper rights and de-encryption keys to open and the scan encrypted messages.*

When implementing NShield in your Notes environment, the following actions are recommended:

Step	Action
1.	Upon installing GroupScan or GroupShield, run NScan on all your databases to begin with a virus free environment.
2.	Take one of the following steps: <ul style="list-style-type: none"> For Lotus Notes clients running GroupScan, configure NShield to scan on all database document Reads and file attachments. Add the following line to the NOTES.INI file: <pre>NShieldOptions=+H:READ +A -D -M +F +N</pre> For Lotus Notes Servers running GroupShield, configure NShield to scan only interactive databases that users can save documents into, such as; the Web Navigator databases, Discussion databases, and Document Library databases. Configure NShield to scan on document writes by adding the following lines to the NOTES.INI file: <pre>NShieldOptions=+H:WRITE +A -D -M +F +J +N NShieldScanOnly=WEB.NSF, DISCUSSION.NSF, DOCLIB.NSF</pre>

Using NShield

NShield is a real-time anti-virus file scanner that protects the Lotus Notes environment from several types of new software attacks, ranging from simple electronic mail bombs and Trojan horses to viruses that infect workstations. To help ensure that your data remains secure, NShield monitors your Notes client and servers for: infected file attachments, document infections, prank mail activity, and server break-in attempts.

 *For a complete description of software threats in the Lotus Notes environment, see [Appendix B, "Understanding Notes Threats."](#)*

Detecting document infections

Detection for infected documents can occur on database reads and/or database writes, depending on how NShield is configured.

Detection during database writes

When NShield detects an infected document during a write, an alert message appears on the status line of the Notes client. The alert message states that a Notes virus or Trojan has been detected. An alert e-mail is sent to the individuals specified in the GroupScan or GroupShield Notification setting in the NOTES.INI file. NShield responds to an infection according to the infection type:

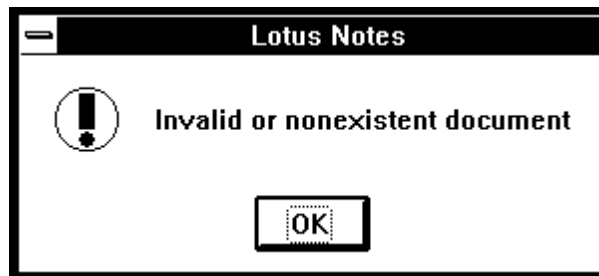
- If a file attachment is infected, an attempt is made to clean the document. If the document cannot be cleaned, the infected attachment is removed from the document.
- If a stored form was found to have auto-launch characteristics, auto-launching is disabled.
- If a stored form was found to have virus characteristics, the stored form is removed.
- If a button macro was found to have virus characteristics, the formula is removed.

- If a hotspot macro was found to have virus characteristics, the formula is removed.
- If a stealth form was found in a rich-text field, the field in which it was found is deleted.
- If an OLE Trojan object was found, the OLE object is removed.

The original document is also written to the Quarantine Area for later analysis or recovery in the event that the detection was a false alarm. See [“Using the Quarantine Area” on page 60](#) for details on using the Quarantine Area.

Detection during database reads

Whenever NShield detects an infected document during a read, NShield returns the following error to the Notes client:




The infected document is written to the Quarantine Area, but is not removed from the source database. If the notification option was activated, your Notes administrator will receive notification of the incident after the infected document is written to the Quarantine Area.

Prank mail detection

NShield's prank mail detection monitors all documents entering the Notes mail stream. NShield searches mail documents for instances when the sender of the message does not match the listed message author. When NShield detects a prank mail attack, NShield responds by taking the following actions:

- Renames the From field to OriginalFrom for reference purposes
- Creates a new From field set to the user name associated with the current server session
- Records the event in the log and sends a message if notification is enabled
- Allows the message to be routed normally with the true message sender listed in the From field

 *If configured, NShield can redirect suspected prank mail messages to the Notes administrator.*

Server break-in attempts

NShield for GroupShield provides server break-in detection by monitoring suspicious activity on all public Name & Address Book databases. The server break-in detection configuration can be modified in the `GroupShieldSecurity=` setting in NOTES.INI file. When NShield detects a server break-in attempt, the following occurs:

- An Invalid or Nonexistent Document error is returned to the perpetrator
- A record of the event is placed in the log
- A mail notification message is sent if the notification option is enabled

Configuring NShield Options

NShield options can be modified in the NOTES.INI file and the Administration database with LiveNotes Administrator. You can quickly modify and review the NShield options in GroupShield by using LiveNotes Administrator.


You can access the NOTES.INI file to configure NShield from the Tools menu in NotesR3 and the Actions menu in NotesR4. See [“Configuring NScan using the Menu Add-in” on page 51](#) for more information on editing the NOTES.INI file.

To configure NShield using the LiveNotes Administrator for GroupShield, follow the instructions outlined below.

Step

Action

1. Click the GroupShield Administrator database icon.

 *To open the LiveNotes database, you must first add the database icon to your Notes workspace. Refer to your Lotus Notes documentation for instructions on adding a database icon to your Notes workspace.*

Response: The LiveNotes Administrator for GroupShield is displayed. See Figurexxxx.

2. From the Configure menu, select NShield Options.

Response: The Configure NShield Options control panel is displayed (Figure 3-1).

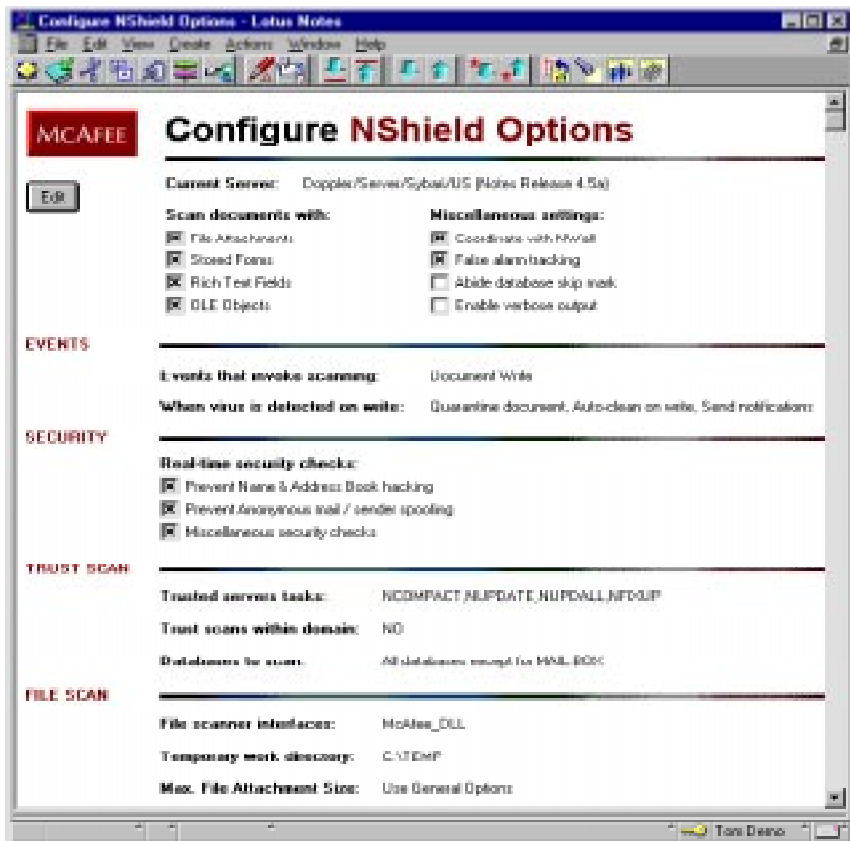



Figure 3-1. Configure NShield Options Dialog Box.

3. Click the Edit button to edit NShield options

 You can enable an NShield options template by clicking the Set button and choosing a pre-configured template.

4. Specify the documents you want to scan by clicking the checkbox next to the document type.
 - If you want to scan documents with file attachments, check File Attachments.
 - If you want to scan documents with stored forms, check Stored Forms.
 - If you want to scan documents with rich text fields, check Rich Text Fields.
 - If you want to scan documents with OLE objects, check OLE Objects.
5. Under Miscellaneous settings, check the options desired.
 - To coordinate settings with NWall, check Coordinate with NWall.
 - To enable false alarm tracking, check False Alarm Tracking.
 - To abide a database skip mark, select Abide Database Skip Mark
 - To allow verbose output, check Enable Verbose Output.
6. In the Events section, specify the following:
 - The events that you want to occur to invoke scanning.
 - The action that you want NShield to take when a virus is detected on a write.
7. Check the desired NShield security options listed under Security.
8. Check the desired trust scan settings listed under Trust Scan.

9. Under File Scan, specify the following:
 - File scanner interfaces
 - Temporary work directory
 - Maximum file attachment size
10. To save settings, click Save.

What is NScan?

NScan provides user-initiated scanning of local databases and helps a Notes administrator ensure that the Notes client and server are virus-free. It differs from NShield in that it allows you to perform an active scan of the system as you work rather than waiting for documents to be read, written, or mailed. It can also be scheduled to run at specified times, typically before or after a scheduled database replication to insure virus free environments.

NScan is a Notes solution that scans for and cleans viruses, bombs, and Trojan horses located in any database application including Notes mail. The program provides the ability to intercept, deactivate, and record all instances of Notes-based viruses. NScan also can be used to scan file attachments and remove any file-based viruses found. This feature can isolate documents with attachments that exceed a desired size, which is useful for removing large attachments from user mail databases

Using NScan

NScan is a stand-alone executable program that can be configured to scan or clean any combination of databases or directories, locally or on a remote server. NScan's general behavior and settings can be modified by altering the GroupScanOptions= or GroupShieldOptions= setting in the NOTES.INI file.

Several methods are available for performing on-demand scans with NScan:

- For Windows 95 and Windows NT, a local scan of all databases can be started by double-clicking the Scan All Databases icon in the GroupScan/GroupShield for Notes program folder or from the Start menu.
- Scans can be performed from the command line.
- Scans can be scheduled using the Notes program document.
- Scans of the current Notes database can be performed from the Menu Add-in.


Configuring NScan using command-line options

To perform an on-demand scan of your Notes environment from the command line, type `NSCAN` at the command prompt followed by the options you wish to invoke and the databases you want to include in the scan. The general syntax is as follows:

```
NSCAN [options] [database names]
```

If you have installed GroupShield, go to the system console on the NetWare server and type `NSCAN *`. Press ENTER. Type `LOAD NSCAN /CLEAN *` to clean your system. Type `NSCAN /?` to display a help screen describing the complete syntax.

A complete description of all command-line options and database parameters is included in [Appendix C, "Reference."](#) If no parameters are specified, the command syntax and a list of valid options are displayed.

 *All directory scanning performed by NScan observes any and all directory links that have been created. A maximum of 64 database names may be specified together on a single command line. However, the entire command line length is limited according to the operating system that NScan is executed on and may prevent the maximum number of database names from being specified.*

Configuring NScan using the Menu Add-in

In addition to performing an on-demand scan from the command prompt, you can also scan the current Notes database by using the GroupScan/GroupShield Menu Add-in. To perform this type of scan, which uses the settings specified in `NOTES.INI`, select Scan Database from the Tools menu (in Notes R3) or the Actions menu (in Notes R4). For more information on the GroupScan Menu Add-in, see ["What is the Menu Add-in?" on page 66.](#)

 *The Menu Add-in is not available for NetWare and OS/2 servers.*

Scheduling scans

Scheduled scanning can be configured by creating Program Jobs in the Name and Address Book. See your Lotus Notes documentation for instructions on using the scheduling feature.

Pausing or terminating NScan

If you wish to pause or terminate NScan during a scan, use the following key-stroke commands:

Command	Description
[SPACE] (or CTRL+S)	Pause NScan during a scan
ESC (or CTRL+C)	Terminate NScan during a scan

What is NWall?

GroupShield's NWall component is designed to scan all Notes mail messages as they are routed through the organization. It is most commonly used as a barrier between the external network and the internal Notes mail system. Implemented as a server add-in task, NWall scans all routed mail for viruses. NWall also provides additional security to mail gateways that connect to mail systems, such as the SMTP Agent for Notes, to scan Internet messages. NWall file attachment scanning can also be used to limit the size of file attachments transmitted via Notes mail.

Using NWall

NWall is a document transfer agent that provides complete and transparent protection to your Notes mail environment. NWall can be used to establish a barrier between your organization and the external network. NWall performs immediate detection and cleaning of infected documents and attachments as they are routed through the enterprise. NWall works with NShield to provide maximum protection without the need to modify the Name & Address Book domain or connection documents.

NWall components

NWall is composed of three parts; the NWall Processor (xNWALL.EXE), the NWall Monitor (xNWALLM.DLL), and the NWall Job Database, NWALL.NSF.

Running the NWall Processor


NWall Processor is the server add-in task. NWall can be run manually from the Notes server console or automatically from a program document in the Name & Address Book. The syntax for running NWall from the Notes server console is:

```
LOAD NWall <options>
```

The options available to NWall are fully described in [Appendix C, "Reference."](#) Once NWall has been started, it runs continuously until the Notes server is shut down or you issue a `TELL` command, disabling NWall. To disable NWall, type one of the following commands:

TELL NWall QUIT (Windows platforms and OS/2)

TELL VNWall QUIT (NetWare)

 You can start NWall automatically when the Notes server is started by including NWall in the list of tasks in the NOTES.INI setting `Server-Tasks=NWall`. See your Notes administrator's guide for more information on running server add-in tasks.

NWall Monitor


The NWall Monitor is a DLL (xNWALLM.DLL) that binds itself to the Notes router. The NWall Monitor redirects mail messages for processing by the NWall Processor. NWall is loaded automatically when the Notes server is started by including NWall in the list of processes in the NOTES.INI setting `NSF_HOOKS=NWALLM`.

NWall Job Database

The Notes database contains the NWall job definition documents. The job definition database is optional since the NWall Processor has a built-in job definition specifically for scanning mail messages. This default job is called Scan Mail and it is enabled by adding `+M` to the `NSF_HOOKS=` line in the NOTES.INI file.

All jobs, with the exception of the default NWall Scan Mail job, are defined in the NWall Jobs database, NWALL.NSF. Each job in the database defines a basic transfer of documents from a source database to a destination database along with scheduling information. The NWall job is defined with the following fields:

Field	Description
NWall name	Descriptive name given to NWall for identification.
NWall server	Determines which server to should run a particular job. This is important in an environment that has multiple servers running NWall that share a replicated NWall Job database.
Source database	Specifies the database from which documents will be read.

Field	Description
Target database	Specifies the database to which documents will be written.
Type of document transfer	Defines the type of document transfer. This can be set to copy documents from the source database to the target database or move/redirect documents from the source database to the target database. It can also be set to “disabled” which prevents the job from running at all.
Frequency of document transfer	Determines how often the source database will be polled for new documents.  <i>This defines the amount of time between the end of the previous run and the start of the next run.</i>
First document transfer time off-set	Determines when the job will be run for the first time. The value listed represents the length of time, in minutes, to wait after NWall has been started and before running the job for the first time. This field is useful for sequencing jobs.
Maximum job execution time	Determines how long the job will continue to process documents. Once this value is reached, the job is stopped and rescheduled. This allows all jobs to be executed uniformly, even if one or more jobs experience heavy volume.
Select macro for source	Identifies which documents in the source database to process. This field can be set to any valid Notes select formula. By default, SELECT @All is used as the select formula.
Filter macro for target	This optional field may be set to any valid Notes filter macro. The macro formulas will be executed on each document transferred. For example: FIELD Subject:= Subject + “(NWall)” will append the string “(NWall)” to the end of the subject field.

Sample NWall Job

This sample illustrates how to create an NWall job that acts as a firewall between external domains and Notes Mail routers and your internal Domains and Notes Mail environment. This job is called the NWall Standard Barrier.

This example configuration for creating a Notes firewall with NWall uses a dedicated server for the NWall function. This is necessary to ensure the proper separation of mail routing, Name & Address Book, and database access between outside domains and the inside Notes network. The NWall server does not share the Name & Address Book with any other server. This limits the risk associated with possible Name & Address Book attacks.

The key to properly setting up the NWall Barrier is ensuring that **ONLY** the NWall task transfers documents between the servers. This configuration requires two NWall Jobs to be created, both defined on the NWall Notes server. The first job routes incoming mail (in InBox) and the second job routes outgoing mail. Two Foreign Domain documents, one on each server, are also required so that the Notes mail router will put messages into InBox.NSF and OutBox.NSF, rather than sending them directly to the other server.

An advantage to using this configuration is the option to create a custom filter macro for both inbound and outbound mail. You could disable return receipt and delivery report flags on incoming mail to eliminate mail notification messages from being sent back. Additionally, you can remove or reset fields that contain information about the internal Notes network, such as "RouteServers" on all outbound mail. Use the Filter Macro for Target field to implement these options on documents processed by an NWall job.

The two NWall job definitions to create the NWall Barrier are shown in Figure 3-2 and 3-3, Configure NWall Job Control Panel 1 and 2.

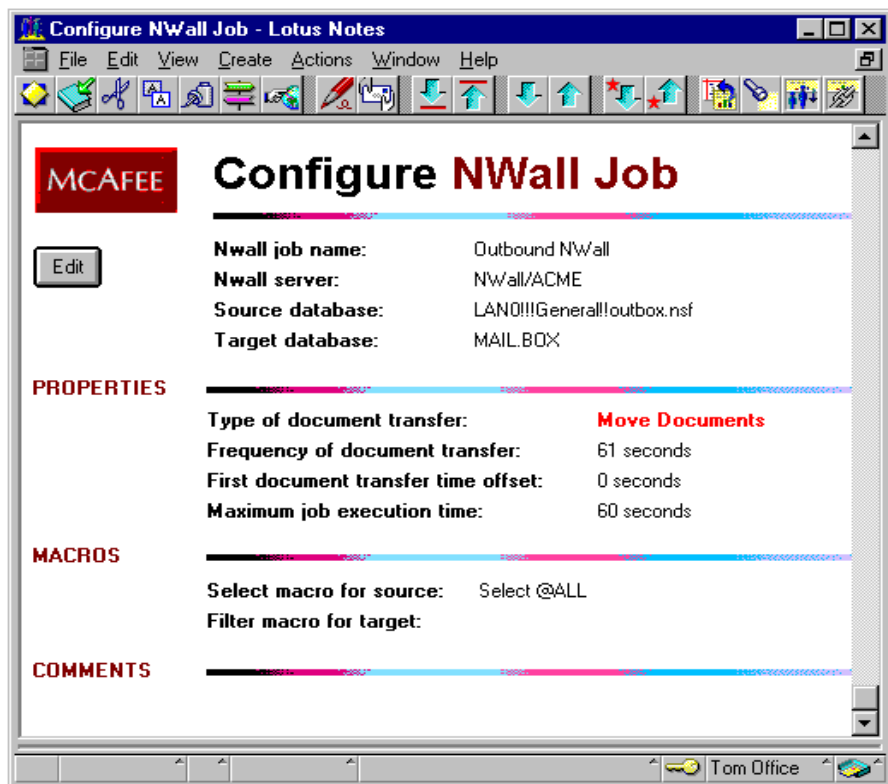


Figure 3-2. Configure NWall Job Control Panel 1

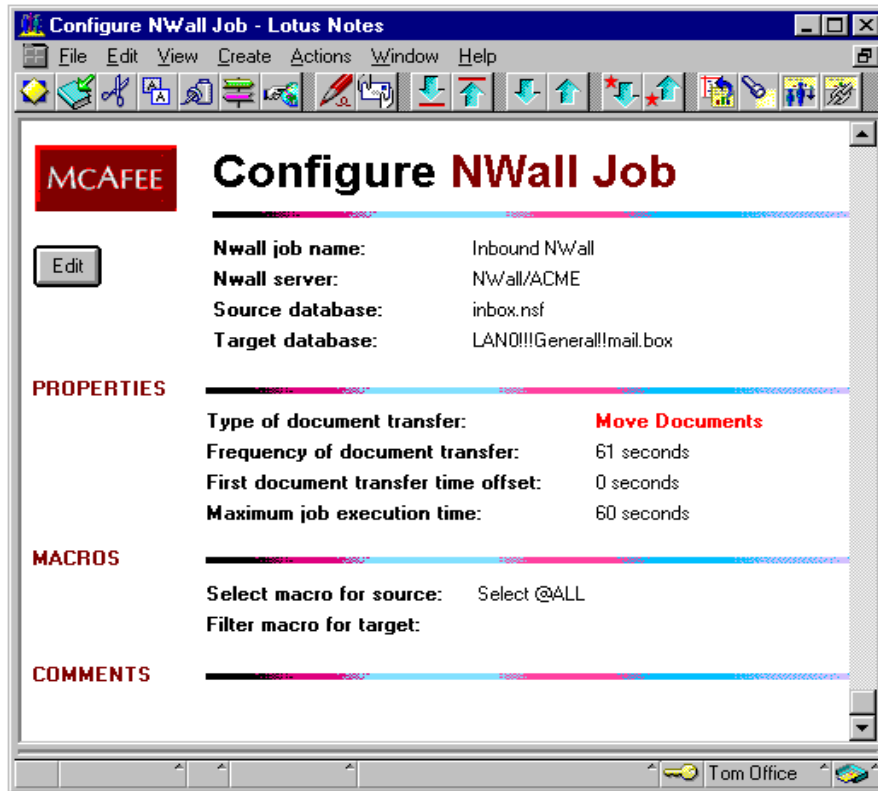


Figure 3-3. Configure NWall Job Control Panel 2

The following diagram, Figure 3-4, depicts the implementation of the NWall Standard Barrier configuration:

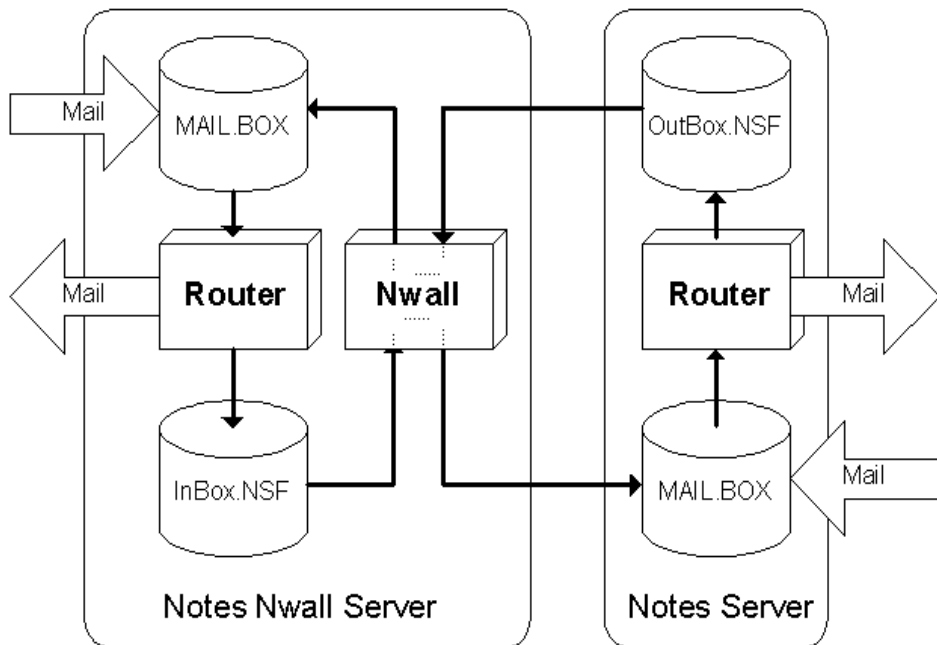




Figure 3-4. NWall Standard Barrier Configuration Diagram

What is the Quarantine Area?

The Quarantine Area is a secured Notes database for isolating possibly infected documents that GroupScan or GroupShield has detected. Once the Quarantine Area has been added to your desktop, you may access it simply by double-clicking on the Quarantine Area icon.


 *See your Notes documentation for details on adding database icons to the desktop.*

Check the Quarantine Area regularly for information on intercepted viruses.

 *GroupScan and GroupShield can be configured to send messages to the Notes administrator upon virus detection. See [Appendix C, "Reference,"](#) for details on setting up notifications.*

The information contained in the Quarantine Area will help you to identify the type and source of virus activity that GroupScan/GroupShield has encountered. All Quarantine Area documents are created automatically when virus activity is detected. The Quarantine Area documents may be edited to change the document's status or add comments for future reference.

GroupShield fully supports the replication of the Quarantine Area between servers. The Quarantine Area becomes a central repository and monitoring tool for virus activity when GroupShield is deployed on multiple servers.

 *It is important to secure the Quarantine Area and limit access to it since replicating the Quarantine Area will replicate infected documents*

Using the Quarantine Area


GroupScan and GroupShield will detain and disable all suspicious documents in the Quarantine Area. For the purpose of analysis, GroupScan/GroupShield preserves the original source document and adds other data to the file, such as virus characteristics, time detected, status, and source of the virus. Each document in the Quarantine Area represents either a captured virus or a false alarm.

Once a document has been quarantined, a Notes administrator can examine the documents to determine whether they are subversive or threatening to the Notes environment.

- If the document contains threatening or harmful data, follow the procedure outlined in [“Responding to a virus” on page 61](#) to mark the document’s virus status.
- If the incident is a false alarm, follow the procedure outlined in [“Responding to a false alarm” on page 62](#) to restore the document or add a suspicious stored form design to the false alarm list.

Responding to a virus

If the suspicious data that GroupScan/GroupShield quarantined is subversive, use this procedure to mark the document as containing a confirmed virus.

 *If you identify a confirmed virus, please send the data to the McAfee Emergency Response Center for analysis. See [“How To Contact Us” on page 9](#) for McAfee contact information.*

Step

Action


1. Open the document from any view except the Restored Documents view.

Response: The document opens and series of buttons appear in the top right corner of the window.

2. Switch the document into Edit mode by pressing CTRL+E or using the equivalent menu command.

3. Click the button marked Confirmed and save the document.

Response: The document remains visible in the current view but is now classified as a confirmed virus.


 *An audit trail is maintained on all changes made to the document status. Click the hotspot labeled Audit Trail located just below the buttons. A list of all changes, including changes to and from confirmed status, will be displayed in a pop-up window.*

Responding to a false alarm

In some instances, sophisticated mail-enabled applications may contain virus-like behavior but are not viruses. If a document does not contain a virus or other harmful data, add information to the false alarm list and restore the document or a copy of the document.

If the false alarm contains a suspicious but non-threatening stored form, GroupScan's and GroupShield's false alarm facility allows you to add the design to a false alarm list so that GroupScan and GroupShield will skip all other documents that contain an identical design.

- If the false alarm contains a stored form, follow the procedures in [“Responding to a false alarm with a stored form”](#) to mark a document as a false alarm and restore a copy to the original source database.

 *The false alarm facility identifies stored form designs, not rich-text elements such as buttons and hotspots.*

- If the false alarm does not contain a stored form, its design cannot be added to the false alarm list. To respond to this type of false alarm, restore the original document to the source database by following the steps in [“Responding to a false alarm without a stored form”](#) on page 64.

Responding to a false alarm with a stored form


Use the following procedure to mark a document as a false alarm and restore a copy to its source database.

Step

Action


1. Open the document from any view except the Restored Documents view.

Response: The document opens and series of buttons appears in the top right corner of the window.

 *If a button marked False Alarm is not present, then this document does not contain a stored form and cannot be added to the false alarm list. See [“Responding to a false alarm without a stored form”](#) for instructions on how to proceed.*

2. Switch the document into Edit mode by pressing CTRL+E or using the Edit menu command.
3. Click the False Alarm button and save the document.

Response: The document remains visible in the current view but is now also visible in the False Alarms view.

 *An audit trail is maintained on all changes made to the document status. Click the hotspot labeled Audit Trail located just below the buttons. A list of all changes, including changes to and from false alarm status, will be displayed in a pop-up window.*

4. Select Restore Copy of Document from the Tools menu.

Response: GroupScan/GroupShield removes all detection data from the document and restores certain source document fields from a copy of the original quarantined document. The selected documents remain visible in the current view and the copy is moved to Restored Documents.

5. Open the Restored Documents view. You will see all of the restored documents organized by date.

6. Open each document that you wish to restore.

Response: Each document is displayed with either a default mail form or a default document form. The presence of certain mail-specific fields (Recipients, SendTo) helps GroupScan/GroupShield to determine which default form is used. If you need to force all documents to be opened with the default document form, run the macro Toggle Restored Display Mode.

7. Do one of the following:

- If the document is displayed with the default mail form, use the standard button macros Send, Reply, and/or Forward to resend the message.
- If the document is displayed with the default document form, use the Restore to Source button to copy the document into the source database. You can then use the Open Source button to open the source database for inspection.

Responding to a false alarm without a stored form


Use the procedure below to restore an original document to its source database.

Step

Action

1. Select the documents you wish to restore from any view except the Restored Documents view.
2. Select Restore Original Document from the Tools menu.

Response: GroupScan/GroupShield removes all detection data from the document and restores certain source document fields from the original quarantined document. The selected document disappears from the current view and is moved to Restored Documents.

 *If you selected a document that is on the list of false alarms, you will receive a warning message. If you choose to proceed, the false alarm will be removed from the list. To restore a document and maintain a false alarm list entry, see “Responding to a false alarm with a stored form.”*

3. Open the Restored Documents view. You will see all of the restored documents organized by date.


4. Open each document that you wish to restore.

Response: Each document is displayed with either a default mail form or a default document form. The presence of certain mail-specific fields (Recipients, SendTo) helps GroupScan/GroupShield to determine which default form is used. If you need to force all documents to be opened with the default document form, run the macro Toggle Restored Display Mode.

5. Do one of the following:
 - If the document is displayed with the default mail form, use the standard button macros Send, Reply, and/or Forward to resend the message.
 - If the document is displayed with the default document form, use the Restore to Source button to copy the document into the source database. You can then use the Open Source button to open the source database for inspection.
6. After the document has been restored, you can delete it from the Quarantine Area.

What is the Menu Add-in?

The GroupScan and GroupShield Menu Add-in is a .DLL file that provides a simple interface for operating NShield and NScan within Lotus Notes. From this menu, you can also access the NOTES.INI file, which you can use to modify NShield's policies. The Menu Add-in is loaded and configured during the standard installation of GroupScan or GroupShield.

 *To use the Menu Add-in, the NOTES.INI setting AddinMenus must include the full filename of the menu .DLL file. For example, under Windows 3.1x, the setting should be AddinMenus=_NMENU.DLL. If another menu add-in is already listed, separate the .DLL filenames with a comma.*

Once the Menu Add-in is loaded, you can access three new menu options from the Tools menu (in Notes R3) or from the Actions menu (in Notes R4):

- **GroupScan/GroupShield NShield**, which is used to enable or disable the NShield scanner for the Notes client. A checkmark next to this menu option indicates that NShield is enabled.
- **Scan Database**, which is used to scan the current Notes database with the NScan on-demand scanner. See [“Configuring NScan using the Menu Add-in”](#) below for details on using this menu option.
- **Edit NOTES.INI**, which provides easy access to the NOTES.INI file. From this file, you can modify the settings that control the behavior of the GroupScan and GroupShield components. See [Appendix C, “Reference” on page 82](#) for settings in this file.

Using the Menu Add-in

In addition to performing an on-demand scan at any time from the command prompt, you can also scan the current Notes database by using the Menu Add-in. To perform this type of scan, which uses the settings specified in NOTES.INI, select Scan Database from the Tools menu (in Notes R3) or the Actions menu (in Notes R4).

What is the LiveNotes[™] Administrator for GroupShield?

The Administrator for GroupShield provides an easy-to-use interface for configuring, monitoring, and troubleshooting all of the components of GroupShield. You can use the Administrator to:

- Modify GroupShield NOTES.INI settings and its general operation
- Modify NShield and NWall settings
- Configure notification options
- Create and administer NWall jobs
- Set and view external scanner settings

Enabling the LiveNotes Administrator for GroupShield

The Administrator for GroupShield is made up of two components, a server task add-in and a Lotus Notes Database. The server task must be running to enable dynamic modification of the GroupShield settings. The Administrator for GroupShield is loaded and configured during the standard installation of GroupShield.

You can open the Administrator database (GSAV.NSF) from within the Notes client.

To verify that LiveNotes Administrator or any other GroupShield component is loaded on the server, use the command `SHOW STAT GROUPSHIELD` at the server console. A normal output would be as follows:

```
show stat groupshield
```

```
GroupShield.NShield.Attacks = 0
```

```
GroupShield.NShield.Quarantined = 0
```


```
GroupShield.NShield.Scanner = Writes Only (+A -D -E +F +N +R -T +Z)
```

```
GroupShield.NShield.Spoofing = 0
```

GroupShield.NShield.Version = 3.13 (Build 180)
GroupShield.NWall.Job1 = Scan mail (02/20/97 11:26:10 AM)
GroupShield.NWall.Job1.Error = 0
GroupShield.NWall.Job1.Total = 0
GroupShield.NWall.Monitor = 3.13 (Build 180)
GroupShield.NWall.Processed = 0
GroupShield.NWall.Quarantined = 0
GroupShield.NWall.Redirected = 0
GroupShield.NWall.Status = ONLINE
GroupShield.NWall.Version = 3.13 (Build 180)
GroupShield.Task.NLNOTES = Enabled
GroupShield.Task.NNWALL = Synchronized
GroupShield.Task.NROUTER = Enabled
GroupShield.Task.NSERVER = Enabled

Configuring File Attachment Scanning

GroupScan and GroupShield scan and clean infected file attachments from Lotus Notes documents and mail messages. You can scan, clean, and isolate infected file attachments on-demand with NScan or on-access with NShield and by implementing NWall's real time mail stream protection.

 *If you currently have an on-access file virus scanner installed on your GroupScan or GroupShield machine, you must exclude the Temporary directory used by GroupScan or GroupShield from scans done by the on-access scanner. This must be done to prevent the on-access scanner from sending false results to the GroupScan/GroupShield scanner.*

GroupScan and GroupShield integrate with VirusScan and NetShield engines to scan and clean the traditional file-based viruses found in the file attachments. GroupScan/GroupShield can use a currently installed McAfee scan engine or install its own McAfee scan engine. There are several ways GroupScan/GroupShield can interact with the external McAfee scanners. The scanning method used depends on the operating system and the current availability of the different scanner types. GroupScan/GroupShield may use more than one type of scanner, depending on the type of file that is attached to the Notes document. This is useful as you may need a certain scanner to perform both scanning and cleaning of a particular file type.

Configure GroupScan to use scanner types with the NOTES.INI setting GroupScanScanners=, or configure GroupShield to use scanner types with the GroupShieldScanners= setting in the NOTES.INI file.

Available options are: McAfeeDLL, McAfee, NetShield (for GroupShield) and VShield. With each option there are a set of NOTES.INI settings for each external scanner type. These settings are prefixed by the scanner type name. For example:

`McAfee_Extensions=.ZIP`

`McAfeeDLL_Extensions=.DOC.DOT.XLS.XLT.EXE.COM`

The above settings indicate which external scanner to use when a particular file type is attached in the Notes document.

.DLL Integration (McAfeeDLL)

Currently available for Windows NT and Windows 95, this provides the tightest integration between GroupScan/GroupShield and an external scanning engine. This offers the best performance, as in many cases it can scan the attached file while in memory instead of detaching the document to disk. This also option also allows NShield to provide on access scanning of file attachments. The only limitation to this method is that there are several file types that cannot be scanned or cleaned.

Launch command line scanner (McAfee)

Available for all operating systems, this provides the most comprehensive scanning and cleaning capabilities. The only limitation to this option is that it cannot be used by NShield for on access scanning of file attachments. This is due to the fact that it is technically not possible for NShield to launch the external scanner executable file.

On access scanner integration (NetShield or VShield)

This option is only listed for backwards compatibility. It has been replaced by the McAfeeDLL option in GroupScan/GroupShield v3.1.3 and later. Use this option for NShield on operating systems that have a McAfee on access scan engine but do not have the .DLLs available.

Scanning .ZIP files

This is setup by default for Windows NT and Windows 95 installations. GroupScan/GroupShield uses the McAfee .DLLs (on supported operating systems) directly to scan files attached to Notes documents. To properly scan and clean .ZIP files GroupScan/GroupShield must use the McAfee command line scan engine. The specific settings in NOTES.INI that enable this configuration are as follows:

GroupScanScanners=..., McAfee (for GroupScan)

GroupShieldScanners=..., McAfee (for GroupShield)

McAfee_Method=EXTERNAL

McAfee_Description=Scan32

McAfee_Vendor=VirusScan

McAfee_Version=2.5.4

McAfee_Extensions=.ZIP.

McAfee_Action=CURE

McAfee_ScanCall=SCAN32 /ALL /UINONE /NOMEM /NOBOOT /
LOG %R /NOLOGUSER /NOLOGDATETIME /COMP %F

McAfee_ScanVirus=4

McAfee_ScanOK=0

McAfee_WorkDir=C:\Program Files\McAfee\VirusScan NT

McAfee_IDString=%F % (

McAfee_CureCall=SCAN32 /ALL /UINONE /NOMEM /NOBOOT /
NOLOG /CLEAN /COMP %F


McAfee_CureOK=5

Scanning .NSF Database Attachments

GroupScan and GroupShield provide a very flexible interface for integrating McAfee anti-virus products for scanning file attachments. However a common type of file attachment in the Notes environment is the Notes database (.NSF extension) or Notes template database (.NTF extension). To enable scanning of these attachments, NScan is configured as an external file scanner that can be invoked by NWall or NScan (NShield only supports automatic and real-time file scanners, not external scanners). GroupScan/GroupShield will automatically configure NScan to scan Notes database file. To manually configure NScan as an external scanner, follow the steps outlined below.

Step	Action
1.	<p>In the NOTES.IN file, add NScan to the current list of GroupScan/GroupShield scanners.</p> <p>For systems running GroupScan, add the command line</p> <pre>GroupScanScanners=..., NScan</pre> <ul style="list-style-type: none"> For systems running GroupShield, add the command line <pre>GroupShieldScanners=..., NScan</pre>
2.	<p>Define the NScan configuration settings by adding the following commands:</p> <pre> NScan_Method=EXTERNAL NScan_Description=GroupScan NScan NScan_Vendor=McAfee NScan_Version=312 NScan_Extensions=.NSF.NTF NScan_Action=DELETE NScan_ScanCall=NScan %F +A -T +S NScan_ScanVirus=255,4095 NScan_ScanOK=0 </pre>

Response: The Trust Other Servers feature is disabled. The entire database will be trusted (since it is an attachment) if the scan does not detect any viruses.

 *The most important option for this configuration is the +S which silences output but also forces NScan to exit with a non-zero return code (ERRORLEVEL) when a virus is found.*

A

Preventing Virus Infection

Keys to a Secure Notes Environment

GroupScan and GroupShield can be used as an effective tool for preventing, detecting, and recovering from virus infection in the Lotus Notes environment. They are most effective, however, when used in conjunction with VirusScan and NetShield and a comprehensive computing security program that includes a variety of safety measures, such as regular backups, meaningful password protection, user training, and awareness.

To create a secure Notes environment and minimize your chance of infection, McAfee recommends that you take the following steps:

- | Step | Action |
|------|---|
| 1. | Follow the installation procedures as outlined in Chapter 2, "Installing GroupScan and GroupShield." |
| 2. | Enable NShield to continuously monitor Notes for virus activity. |
| 3. | Make frequent backups of important Notes databases. Even with GroupScan/GroupShield, some viruses (as well as fire, theft, or vandalism) can render data unrecoverable without a recent backup. |

Outlining a full security program is beyond the scope of this manual. However, by following the steps provided in this appendix and reading the information provided in [Appendix B, "Understanding Notes Threats,"](#) you can gain a clearer understanding of potential threats to the Notes environment and how they can affect your data.

Updating Your Data Files

To offer the best virus protection possible, McAfee continuously updates the files that GroupScan and GroupShield use to detect viruses in attached files. McAfee recommends that you update these files on a regular basis for maximum protection.

What is a data file?

The data files; CLEAN.DAT, NAMES.DAT, and SCAN.DAT all provide virus information to the GroupScan and GroupShield software.

Why would I need a new data file?

New viruses are discovered at a rate of more than 200 a month. Often, these new viruses are not detected using older data files. The data files that came with your copy of GroupShield might not be able to help GroupShield detect a virus that was discovered months after you bought the product.

McAfee's virus researchers are working constantly to update the data files with the latest virus definitions. The new data files are released approximately every four to six weeks.


How to apply the data file

To update your data files, take the following steps.


Step

Action

1. Download the data file (for example, DAT-9703.ZIP) from one of McAfee's electronic services. On most services, it is located in the anti-virus area.

 *Please note that your ability to access these updates is legally restricted by the maintenance terms outlined in the README.1ST file accompanying the software and detailed in the software license agreement.*

2. Copy the file to a new directory.
3. The file is in a compressed format. Decompress the file using any PKUNZIP-compatible decompressing software. If you do not have the decompressing software, you can download PKUNZIP (shareware) from McAfee electronic sites.
4. Locate the directories on your hard drive where your GroupScan or GroupShield software is currently loaded. Copy the new files into the directory or directories, overwriting the old data files.

 *Depending on the Installation type selected, the directory could either be your GroupScan or GroupShield directory under Program Files/McAfee or it could be in your Notes Program directory.*
5. Reboot your computer to make the changes take place immediately.

McAfee Virus Information Library

The McAfee Virus Information Library is a comprehensive database containing more than 250 technical documents and information about more than 1,000 viruses.

This library offers detailed information concerning computer viruses, their methods of infection, their effect on computers, instructions on removing them, and methods of preventing them.

The McAfee Information Library is available on the CD-ROM version of this package in the Windows 95 help file format. This information is also available through the McAfee Web Site.

The Virus Information Library is continuously being updated through our web site to offer the most comprehensive, up-to-date information available.

For information on reaching the McAfee Web Site, see [“How To Contact Us” on page 9](#).

B

Understanding Notes Threats

The Lotus Notes environment is vulnerable to several types of new software attacks. These can range from simple electronic mail bombs and Trojan horses to viruses that infect workstations, servers, and networks. This appendix provides definitions for the most common software threats in the Lotus Notes environment.

Infected file attachments

This is by far the most common threat in the Lotus Notes environment. This occurs when infected files are attached to a Notes document. The most typical occurrence is the Word Concept virus. Standard anti-virus products are unable to directly remove this virus from Notes databases. This type of infection spreads rapidly via replication within the Notes environment.

Notes Trojan horses

This class of attack (sometimes referred to as Button Bombs) relies on tricking the user into pressing a button that initiates a malicious action. One way of doing this is to copy the look and feel of a well known form, such as the standard mail memo, by using the Store Form in Document feature of Notes. A second way is to present something alluring to the user, such as a big button that says Try Me!

A rectangular button with a light gray background and a thin black border. The text "Try Me!" is centered on the button in a bold, black, sans-serif font.

Once the button has been pressed, the following actions can be carried out:

- Execution of programs already resident on the system
- Detaching of infected files embedded in the mail document, which then can be run
- Halting or crashing the Notes client

The distinguishing feature of a Trojan horse is that it requires the user to take some action. The infected document or mail message must be loaded and displayed, and the user must activate the attack. Detection and prevention of this form of attack relies on identifying mail with stored forms and/or viewing button macros before they are executed.

Notes mail bombs

Like the Notes Trojan horse, the mail bomb relies on stored forms. When a mail document is infected with a mail bomb, Lotus Notes crashes as soon as the user tries to read the infected document. Mail bombs can be embedded in button macros and are activated when a user reads or edits a document.

Notes as a carrier

Infected mail documents can carry platform-specific file-infecting viruses that can infect the Notes environment. This type of attack (also known as a dropper) is most common in file attachments. The virus activates when the infected mail document is detached and run. Fortunately, unless a Trojan horse detaches and executes the attachment for you, you can check the executable for a virus with NScan before running it.

Notes virus reproduction

Virus reproduction is when an infected document replicates and spreads through Internet mail to the list of people with whom a user has corresponded. This is probably the most destructive attack, because it allows any of the Notes attacks described in this appendix to become fully reproducible. When Notes viruses are spread, the From field takes on the identity of the user so the recipients see a message from someone they recognize. Because many organizations are connected to the Lotus Notes Network, CompuServe Enterprise Information Link, WorldCom, and other organizations, a virus reproducing in this way can be devastating.

Notes stealth viruses

Many of the techniques described thus far rely on the stored form feature of Notes. However, it is relatively easy to identify documents that have stored forms embedded in them, because the presence of a \$BODY, \$INFO, and \$TITLE items signifies that a stored form is present. To avoid detection, a technique called *stealthed form* is sometimes used to convert a stored form into a normal rich-text item such as the Body item used in all mail messages. The stealthed form executes whenever the rich-text item is displayed. This technique allows formulas to be executed directly from any rich-text field, making detection extremely difficult. This technique also undermines mail filters and background macros designed to detect stored forms.

Notes prank mailing

One of the perceived strengths of Notes is its ability to identify document authors and editors. This serves as a deterrent to would-be attackers, because they can be identified and held accountable for their actions. Unfortunately, despite the Notes security features, mail can be forged or sent anonymously. Although the server mail router does log a warning if the sender name cannot be found, the mail is routed to all of the specified recipients.

Notes worm attacks


A worm attack uses Notes replication for transmission by embedding itself into a widely used and replicated Notes database. Each time a user opens the infected document, the worm activates, using any of the techniques described in this appendix. Although viruses can be embedded just like worms, a worm does not actively try to reproduce itself.


Notes server attacks

In addition to the Notes user attacks described above, attacks and viruses can be directed toward Notes servers. These server attacks either destroy data or breach security for later infiltration by an outside intruder. Usually, these security violations are accomplished through attacks on the Name & Address Book.

NShield Command-line options


This section describes the options that are available when configuring the NShield settings, NShieldOptions=, in the NOTES.INI file


Option	Default	Description
+A	Off	Checks files attachments. Scans all file attachments to Notes documents and alerts you of any viruses found.  <i>This option is only active when NetShield or VirusScan is installed and linked to GroupScan/GroupShield for on-access file attachment scanning</i>
+D	Off	Checks database design notes for suspicious designs. This option is useful when implementing a new database.
+F	On	Enables false alarm tracking. Looks in the Quarantine Area for documents marked as False Alarms before flagging and disabling documents.
+H	+H:option	Sets the event(s) NShield will hook. Option would be set to: READ, WRITE or ALL.
+J	On	Provides coordinated joint scanning between NWall and NShield. Prevents scanning collisions on MAIL.BOX. If NWall was enabled during installation, the default is on.
+K	Off	Skips the scanning of a selected database.


Option	Default	Description
+L	Off	For testing purposes, stores all output from NShield in GSCAN.LOG and GSHIELD.LOG.
+M	Off	Enables mail redirection to NWall. This option allows NShield to bypass the Notes Router, redirecting all MAIL.BOX messages to NWall for processing.  <i>If NWall is not running, this setting will cause mail to accumulate in MAIL.BOX.</i>
+N	Off	Enables mail notifications. When this option is selected, mail is sent to addresses specified by the GroupScan/GroupShieldNotifyList setting in NOTES.INI.
+O	On	Scans all OLE embedded objects.
+R	On	Scans all rich text fields (RTFs) to identify potentially harmful buttons, hotspots, and stealth forms.
+T	Off	Allows replicated notes to be scanned just once (unless they are updated) rather than once on each server. This trust feature is useful in a GroupShield environment where multiple servers are scanning and cleaning documents.
+U	On	Disables viruses by updating the source database document. Automatically disables viruses by removing the suspected problem from the document.
+V	Off	Displays verbose screen output, or detailed information, on the screen for each document processed.
+Z	On	Scans the stored forms embedded in documents.

NShield NOTES.INI Settings

This section details the NOTES.INI settings that determine the behavior of NShield. To modify or delete these settings, use the Administrator for Notes, select Edit NOTES.INI from the GroupScan/GroupShield Menu Add-In or use a text editor, such as NOTEPAD.EXE.

 Refer to your operating system guide for more information on how to edit text files.

Setting	Description
NShieldOptions=	Allows you to specify the options that NShield will use when executed. Because NShield is not invoked from a command line (it is a .DLL file), all options must be specified with this setting. For a list of NShield options, see “NShield Command-line options” on page 82 . Example: NShieldOptions= +h:All +n +m
GroupScanQArea= GroupShieldQArea=	Specifies the location of the Quarantine Area database. The value is set during the installation process and should not need to be changed. Example: GroupScanQArea=C:\DATA\QAREA.NSF
NShieldScanners=	Overrides the shared setting GroupScan/GroupShieldScanners for NShield.
GroupScanScanners= GroupShieldScanners=	Specifies McAfee's file scanner definitions used when scanning file attachments. Example: GroupScanScanners=McAfee  If NetShield is installed, this setting should be changed to GroupShieldScanners= NetShield to activate real-time file attachment scanning. If VirusScan is installed, this setting should be changed to GroupShieldScanners=VShield.
NShieldTempDir=	Overrides the shared setting GroupScan/GroupShieldTempDir for NShield.



Setting	Description
GroupScanTemp-Dir= GroupShieldTemp-Dir=	Specifies the path to a temporary directory where GroupScan/GroupShield can scan file attachments. When GroupScan/GroupShield encounters one or more attachments within a document, each attachment is detached to a temporary file. The location of this file is a process-safe subdirectory of the specified directory. Example: GroupScanTempDir=C:\TEMP
NShieldScanOnly=	Specifies a specific list of Databases that NShield should protect. Without this option, NShield will protect all databases.
NShieldMaxFile=	Overrides the shared setting GroupScan/GroupShieldMaxFile for NShield.
GroupShieldMax-File= GroupShieldMax-File=	Specifies the maximum size of a file attachment in kilobytes that GroupScan/GroupShield will allow. Note that the size is based on the true size of the attachment and not its compressed size. When this setting is enabled, any attachment greater than the size specified is considered an attack. Example: GroupScanMaxFile=2048 (Isolate notes over 2MB)
GroupShieldTrusted-Tasks=	Specifies the list of Notes task names that NShield will trust. NShield will not scan any activity initiated by the tasks listed.  <i>Tasks specified must have the platform prefix included if the task is a server add-in task.</i> Example: GroupShieldTrustedTasks=nupdate
GroupShieldTrusted-Signers=	This feature is similar to ECLs in that it allows for “signers” of messages not to have the message scanned.


Setting	Description
GroupShieldNotifyList= GroupShieldNotifyList=	Specifies the list of mail addresses to receive notification messages. Any combination of users, groups, and mail-in databases may be specified in the comma-delimited list. Notifications also can be sent to a source document field reference. The syntax for a field reference is %FIELDNAME. Example: GroupScanNotifyList=Administrators,%From
GroupScanNotifySubject= GroupShieldNotifySubject=	Overrides the default subject line of a detection notification message. Any text string is allowed and will appear in the subject line of the notification message. Example: GroupScanNotifySubject=Virus Detected!!!
GroupShieldNotifyBody= GroupShieldNotifyBody=	Overrides the default body text of a detection notification message. Any text string is allowed and will appear in the body field of the received notification message. Example: GroupScanNotifyBody=Please call x1234 now.
GroupShieldMailBox=	The mail redirection facility of NShield is used to bypass the Notes Router and redirect all mail messages delivered to MAIL.BOX to GroupShield NWall for processing. This setting allows redirection to occur on a database other than MAIL.BOX. This setting would only be used in advanced routing applications. Example: GroupShieldMailBox=SHARED.BOX
GroupScanDomain= GroupShieldDomain=	Specifies the trusted server domain name associated with this Notes system. By default, the trusted server domain name is equal to the Notes domain, but this setting provides an override. Note that two Notes systems must have the same trusted server domain name and both have the /T option enabled for documents to be trusted between the systems. Example: GroupScanDomain=AcmeTrust

Setting	Description
GroupScanRCPool= GroupShield-CRCPool=	Allows you to increase the maximum number of false alarms that can be stored in memory. Use this setting to change from the default value of 1000 to a larger number. Increasing this value is only necessary if you have more than 1000 false alarms in the Quarantine Area. Example: GroupScanCRCPool=4001
GroupScanName-Pool= GroupShieldName-Pool=	Allows you to increase the size of the memory buffer used to store all composite item names of a single note. The default value is 4096 bytes.
GroupShieldSecurity=	Specifies the additional security checks to be activated. By default, all security checking will be enabled after installation. Under certain circumstances, however, you may need to disable some options. Possible values: 0 - Turns off all security checks. 1 - Enables only NAB attack security checks. 2 - Enables only prank mail detection. 255 - Enables all security checks. Example: GroupShieldSecurity=255
NSF_HOOKS=	This setting is actually provided by Notes but is required for the operation of NShield. One or more hook drivers are listed by name (without file extension or platform prefix character) and separated by commas. Notes loads each hook driver listed for each Notes process started. The hook driver must be a .DLL file located in the Notes program directory. Example: NSF_HOOKS=NShield

NScan Command-line Options

Option	Default	Description
/A	Off	Checks files attachments. Scans all file attachments to Notes documents and alerts you of any viruses found. <i>✍ Type scan (os2scan or scan32) /? to display a list of VirusScan command-line options and descriptions of how they can be used.</i>
/B	On	Scans all subdirectories and Notes directory link files of the selected directory.
/D	Off	GroupShield option that checks database design notes for suspicious designs. This option is useful when implementing a new database.
/E	Off	Enables scanning of encrypted documents. <i>✍ Do not enable this option for scheduled scans. The first encrypted document will cause NScan to pause for a password.</i>
/F	On	Enables false alarm tracking. Looks in the Quarantine Area for documents marked as False Alarms before flagging and disabling documents for virus infection.
/K	Off	Skips the scanning of a selected database.
/I	N/A	Displays NOTES.INI settings that are relevant to GroupShield.
/N	Off	Enables mail notifications. When this option is selected, mail is sent to addresses specified by the GroupScanNotifyList setting in NOTES.INI.
/O	On	Scans all OLE embedded objects.

Option	Default	Description
/P	Off	<p>Pauses NScan after it has completed its scan and before it exits.</p> <p> <i>If NScan is run in its own window, which closes automatically when NScan exits, this option should be enabled to allow the user to read the scan results before the window closes.</i></p>
/R	On	Scans all rich text fields (RTFs) to identify potentially harmful buttons, hotspots, and stealth forms.
/S	Off	Silences screen output. When this option is enabled, a non-zero exit code is returned when a virus is detected in one of the scanned databases. All NScan activity is logged in LOG.NSF.
/T	Off	<p>Allows replicated notes to be scanned just once (unless they are updated) rather than once on each server. This trust feature is useful in a GroupShield environment where multiple servers are scanning and cleaning documents. By default, servers in the same Notes Domain will trust each other when this feature is enabled.</p> <p> <i>Running NScan with the trust feature enabled will update all documents scanned with a special encoded trust mark. As a result, unread document marks will appear on documents that have been previously read.</i></p>
/U	On	Disables viruses by updating the source database document. Automatically disables viruses by removing the suspected problem from the document.
/V	Off	Displays verbose screen output, or detailed information, for each document processed.
/W:	N/A	Establishes a time window within which documents should be processed by checking documents from x days ago to now. /W:1 tells NScan to check documents created in the last day.


Option	Default	Description
/X	Off	Deletes the source database document that is infected rather than disabling the virus in the document.  <i>The +U option must be set for the +X option to be enabled.</i>
/Z	On	Scans the stored forms embedded in documents.


The following options are actually commands for a specific set of options listed above. Note that the options are processed from left to right, so if you wish to modify one option in a command, be sure to place it to the right of the command.

Option	Description	Function
/SCAN	+R -U +F	Scans and reports on potential problems without actually disabling them. This option takes the least time and system resources and is useful when first introducing GroupScan/GroupShield into an environment, since it allows false alarms to be dealt with prior to updating source database.
/CLEAN	+R +U +F	Scans and cleans potential problems. Although NScan will by default perform a clean operation, this option ensures that none of the options have been set differently in the NOTES.INI.

NScan NOTES.INI Settings

This section details the NOTES.INI settings that determine the behavior of the NScan hook driver. To modify or delete these settings, select Edit NOTES.INI from the GroupScan/GroupShield Menu Add-In or use a text editor, such as NOTEPAD.EXE.



 Refer to your operating system guide for more information on how to edit text files.


Setting	Description
GroupShieldOptions= GroupShieldOptions=	<p>Allows you to specify the options that NScan will use when executed.</p> <p> Entering these settings is optional. However, McAfee recommends that you specify any settings you regularly use. Options specified on the command line will override these settings.</p> <p>Example: GroupScanOptions= +k</p>
GroupScanQArea= GroupShieldQArea=	<p>Specifies the location of the Quarantine Area database. The value is set during the installation process and should not need to be changed.</p> <p>Example: GroupScanQArea=C:\DATA\QAREA.NSF</p>
GroupScanScanners= GroupShieldScanners=	<p>Specifies McAfee's file scanner definitions used when scanning file attachments. Multiple definition names may be listed, each separated with a comma.</p> <p>Example: GroupScanScanners=McAfee</p>
GroupScanTempDir= GroupShieldTempDir=	<p>Specifies the path to a temporary directory where GroupScan/GroupShield can scan file attachments. When GroupShield encounters one or more attachments within a document, each attachment is detached to a temporary file. The location of this file is a process-safe subdirectory of the specified directory.</p> <p>Example: GroupScanTempDir=C:\TEMP</p>

Setting	Description
GroupScanMaxFile= GroupShieldMax- File=	Specifies the maximum size of a file attachment in kilobytes that GroupScan/GroupShield will allow. Note that the size is based on the true size of the attachment and not its compressed size. When this setting is enabled, any attachment greater than the size specified is considered an “attack.” Example: GroupScanMaxFile=2048 (Isolate notes over 2MB)
GroupScanNotifyL- ist= GroupShieldNotifyL- ist=	Specifies the list of mail addresses to receive notification messages. Any combination of users, groups, and mail-in databases may be specified in the comma-delimited list. Notifications also can be sent to a source document field reference. The syntax for a field reference is %FIELDNAME. Example: GroupScanNotifyList=Administrators,%From
GroupScanNoti- fySubject= GroupShieldNoti- fySubject=	Overrides the default subject line of a detection notification message. Any text string is allowed and will appear in the subject line of the notification message. Example: GroupScanNotifySubject=Virus Detected!!!
GroupScanNotify- Body= GroupShieldNotify- Body=	Overrides the default body text of a detection notification message. Any text string is allowed and will appear in the body field of the received notification message. Example: GroupScanNotifyBody=Please call x1234 now.
GroupScanDomain= GroupShieldDomain=	Specifies the trusted server domain name associated with this Notes system. By default, the trusted server domain name is equal to the Notes domain, but this setting provides an override. Note that two Notes systems must have the same trusted server domain name and both have the /T option enabled for documents to be trusted between the systems. Example: GroupScanDomain=AcmeTrust

Setting	Description
GroupScan-CRCPool= GroupShield-CRCPool=	Allows you to increase the maximum number of false alarms that can be stored in memory. Use this setting to change from the default value of 1000 to a larger number. Increasing this value is only necessary if you have more than 1000 false alarms in the Quarantine Area. Example: GroupScanCRCPool=4001
GroupScanName-Pool= GroupShieldName-Pool=	Allows you to increase the size of the memory buffer used to store all composite item names of a single note. The default value is 4096 bytes.


NWall command-line options for GroupShield

Option	Default	Description
/F	On	Enables false alarm tracking. Looks in the Quarantine Area for documents marked as False Alarms before flagging and disabling documents for virus infection.
/M	Off	Processes redirected mail from NShield.
/N	Off	Enables mail notifications. When this option is selected, mail is sent to addresses specified by the GroupScanNotifyList and GroupShieldNotifyList setting in NOTES.INI.  <i>The subject and content of the notifications can be customized using the GroupScanNotifySubject and GroupScanNotifyBody settings in the NOTES.INI.</i>
/O	On	Scans all OLE embedded objects.
/P	Off	Pauses NScan after it has completed its scan and before it exits.  <i>If NScan is run in its own window, which closes automatically when NScan exits, this option should be enabled to allow the user to read the scan results before the window closes.</i>
/R	On	Scans all rich text fields (RTFs) to identify potentially harmful buttons, hotspots, and stealth forms.
/S	Off	Silences screen output. When this option is enabled, a non-zero exit code is returned when a virus is detected in one of the scanned databases. All NScan activity is logged in LOG.NSF.
/T	Off	Allows replicated notes to be scanned just once (unless they are updated) rather than once on each server. This trust feature is useful in a GroupShield environment where multiple servers are scanning and cleaning documents. By default, servers in the same Notes Domain will trust each other when this feature is enabled.

Option	Default	Description
/V	Off	Displays verbose screen output, or detailed information, for each document processed.
/X	Off	Deletes the source database document that is infected rather than disabling the virus in the document. <i> The +U option must be set for the +X option to be enabled.</i>
/Z	On	Scans the stored forms embedded in documents.

NWall NOTES.INI Settings for GroupShield


This section details the NOTES.INI settings that determine the behavior of NWall. To modify or delete these settings, select Edit NOTES.INI from the GroupShield Menu Add-In or use a text editor, such as NOTEPAD.EXE.

 Refer to your operating system guide for more information on how to edit text files.

Setting	Description
NWallOptions=	Allows you to specify the options that NWall will use when executed. Because NWall is not invoked from a command line (it is a .DLL), all options must be specified with this setting. Example: NWallOptions= +t +n +m
GroupShieldQArea=	Specifies the location of the Quarantine Area database. The value is set during the installation process and should not need to be changed. Example: GroupShield-QArea=C:\DATA\QAREA.NSF
NWallScanners=	Overrides the shared setting GroupShieldScanners for NWall.
GroupShieldScanners=	Specifies McAfee's file scanner definitions used when scanning file attachments. Multiple definition names may be listed, each separated with a comma. Example: GroupShieldScanners=McAfee
NWallTempDir=	Overrides the shared setting GroupShieldTempDir for NWall.
GroupShieldTempDir=	Specifies the path to a temporary directory where GroupShield can scan file attachments. When GroupShield encounters one or more attachments within a document, each attachment is detached to a temporary file. The location of this file is a process-safe subdirectory of the specified directory. Example: GroupShieldTempDir=C:\TEMP


Setting	Description
NWallMaxFile=	Overrides the shared setting GroupShieldMaxFile for NWall.
GroupShieldMaxFile=	<p>Specifies the maximum size of a file attachment in kilobytes that GroupShield will allow. Note that the size is based on the true size of the attachment and not its compressed size. When this setting is enabled, any attachment greater than the size specified is considered an “attack.”</p> <p>Example: GroupShieldMaxFile=2048 (Isolate notes over 2MB)</p>
GroupShieldNotifyList=	<p>Specifies the list of mail addresses to receive notification messages. Any combination of users, groups, and mail-in databases may be specified in the comma-delimited list. Notifications also can be sent to a source document field reference. The syntax for a field reference is %FIELDNAME. For instance, if a mail message with an infected file attachment was detected by GroupShield, the sender would be notified if %From was specified in the list.</p> <p>Example: GroupShieldNotifyList=Administrators, %From</p>
GroupShieldNotifySubject=	<p>Overrides the default subject line of a detection notification message. Any text string is allowed and will appear in the subject line of the notification message.</p> <p>Example: GroupShieldNotifySubject=Virus Detected!!!</p>
GroupShieldNotifyBody=	<p>Overrides the default body text of a detection notification message. Any text string is allowed and will appear in the body field of the received notification message.</p> <p>Example: GroupShieldNotifyBody=Please call x1234 now.</p>

Setting	Description
GroupShieldMailBox=	<p>The mail redirection facility is used to bypass the Notes Router and redirect all mail messages delivered to MAIL.BOX to GroupShield NWall for processing. This setting allows redirection to occur on a database other than MAIL.BOX. This setting would only be used in advanced routing applications.</p> <p>Example: GroupShieldMailBox=SHARED.BOX</p>
GroupShieldDomain=	<p>Specifies the trusted server domain name associated with this Notes system. By default, the trusted server domain name is equal to the Notes domain, but this setting provides an override. Note that two Notes systems must have the same trusted server domain name and both have the /T option enabled for documents to be trusted between the systems.</p> <p>Example: GroupShieldDomain=AcmeTrust</p>
GroupShield-CRCPool=	<p>Allows you to increase the maximum number of false alarms that can be stored in memory. Use this setting to change from the default value of 1000 to a larger number. Increasing this value is only necessary if you have more than 1000 false alarms in the Quarantine Area.</p> <p>Example: GroupShieldCRCPool=4001</p>
GroupShieldName-Pool=	<p>Allows you to increase the size of the memory buffer used to store all composite item names of a single note. The default value is 4096 bytes.</p>
NWallDatabase=	<p>Identifies the full path and filename of the NWall Jobs Database that you have created. If this setting has not been added to the NOTES.INI file, NWall will look for a database named NWall.NSF.</p> <p>Example: NWallDatabase=NWall.NSF</p>

Setting	Description
NWallView=	<p>Defines the view within the NWall Jobs Database that NWall uses to obtain the list of jobs. This setting is useful in large or complex NWall implementations. The default view name is FireView.</p> <p>Example: NWallView=FireView</p>
NWallTrustClient=	<p>Determines if mail originated by the Notes client on the server itself will be redirected for scanning by NWall. If the Notes client uses a different mail server than local server, enable this option by setting it equal to 1.</p> <p>Example: NWallTrustClient=1</p>
NWallActiveAfterQuit=	<p>Determines if the NWall monitor will still be active after the NWall server add-in task has been exited. By default, this option is enabled and set to 1. Setting this option to 0 will cause redirection (and thus scanning) to be disabled whenever the NWall server add-in task ends.</p> <p>Example: NWallActiveAfterQuit=0</p>
NWallPhantom=	<p>Defines the name of the phantom routing target displayed when the NWall monitor redirects mail to SCAN.BOX.</p> <p> <i>Do not use a Notes group name, because the phantom name will override the group name.</i></p> <p>Example: NWallPhantom=Mail Vaccination</p>

VirusScan Command-line Error Levels

When you run VirusScan from a DOS or OS/2 command line, an error level is set. You can use the ERRORLEVEL in batch files to take different actions based on the results of the scan.

 See your DOS or OS/2 operating system documentation for more information.

VirusScan can return the following error levels:

ERRORLEVEL	Description
0	No errors occurred; no viruses were found.
1	Error occurred while accessing a file (reading or writing).
2	A VirusScan data file is corrupted.
3	An error occurred while accessing a disk (reading or writing).
4	An error occurred while accessing the file created with the /AF option; the file has been damaged.
5	Insufficient memory to load program or complete operation.
6	An internal program error has occurred (out of memory error).
7	An error occurred in accessing an international message file (MCAFEE.MSG).
8	A file required to run VirusScan, such as SCAN.DAT, is missing.
9	Incompatible or unrecognized option(s) or option argument(s) specified in the command line.
10	A virus was found in memory.
11	An internal program error occurred.

ERRORLEVEL	Description
12	An error occurred while attempting to remove a virus, such as no CLEAN.DAT file found, or VirusScan was unable to remove the virus.
13	One or more viruses were found in the Master Boot Record, boot sector, or files.
14	The SCAN.DAT file is out of date; upgrade VirusScan data files.
15	VirusScan self-check failed; it may be infected or damaged.
16	An error occurred while accessing a specified drive or file.
17	No drive, directory, or file was specified; nothing to scan.
18	A validated file has been modified (/CF or /CV options).
19-99	Reserved.
100+	Operating system error; VirusScan adds 100 to the original number.
102	CTRL+C or CTRL+BREAK was used to interrupt the Scan. (You can disable CTRL+C or CTRL+BREAK with the /NOBREAK command-line option.)

A

America Online 10

B

BBS 9

Bulletin Board System 9

C

CompuServe 10

Configuring

GroupScan components 41

GroupShield components 41

NShield 82

Customer service 9

D

Detecting infections 43

DOS error levels
VirusScan 100

F

File attachment scanning 69

G

GroupScan &
GroupShield

automatically removing 37

components 39

Features 7

Installation 12

introducing 6

manually removing 37

Menu Add-in 66

uninstalling 37

GroupShield

LiveNotes Administrator 67

NWall 53, 94

I

Installation 12, 32
automating 32

Installing Group-
Scan & Group-
Shield

on OS/2 27

on Windows NT and 95
14

Installing Group-
Shield

on a NetWare server
29

Installing GrouS-
can

on Windows 3.1x 22

Internet support 9

L

LiveNotes 6

LiveNotes Admin-
istrator 40, 67
enabling 67

LiveNotes Admin-
istrator 8

M

McAfee

BBS 9

support 9

virus information library
77

website 9

Menu Add-in 6

configuring NScan 51
using 66

Microsoft Network
(MSN) 10

N

Notes threats

- mail bombs 79

- Notes as a carrier 79

- prank mailing 80

- stealth viruses 80

- Trojan horses 78

- virus reproduction 80

- work attacks 81

NScan 6, 8, 39

- command-line options 88

- pausing 52

- settings 91

- terminating 52

- using 50

- using command-line options 51

- what is NScan 50

NShield 6, 8, 39, 42

- command-line options 82

- configuring options 46

- disabling 46

- using 43

- what is NShield 42

NWall 6, 8, 40

- command-line options 94

- components 53

- using 53

- what is NWall 53

P

Prank mail detection 45

Preventing infection 74

Q

Quarantine Area

- 8, 39

- responding to a false alarm 61

- responding to a virus 61

- using the Quarantine Area 60

R

Reference 82

S

Scanning

- .NSF database attachments 72

- .ZIP files 71

- file attachments 69

Scheduled scanning 51

Server break-in attempts 45

Support

- international 11

System requirements 13

T

Technical support

- 9

- contacting 9

- international 11

Training

- scheduling 11

U

Uninstalling

- GroupScan and

- GroupShield 37

- Using GroupScan and GroupShield

- 39

V

Virus

- detecting document infections 43

- false alarm 61

- preventing infection 74

- responding to 61

- understanding 78

Virus Information

- Library 77

VirusScan

- DOS error levels 100

W

What are GroupScan and GroupShield? 6

World Wide Web 9