# Release Notes for
# GroupShield 5.0 Service Pack 2
# for Microsoft Exchange 5.5

===============================================

Service Pack Release:   March 12, 2003

This Service Pack will update the following GroupShield installations:

- GroupShield 5.0 for Microsoft Exchange 5.5.
- GroupShield 5.0 Service Pack 1 for Microsoft Exchange 5.5.
- GroupShield 5.0 for Microsoft Exchange 5.5 updated with Service Pack 1 MSP.
- GroupShield 5.0 Service Pack 1 for Microsoft Exchange 5.5 installations updated to HotFix 1.

This Service Pack will NOT update any version prior to the final release version of GroupShield 5.0 for Microsoft Exchange 5.5.

===============================================

Thank you for using GroupShield software. This file contains important information regarding the release. We strongly recommend that you read the entire document.

## WHAT'S IN THIS FILE

## IMPORTANT NOTE

You can download the Service Pack from the McAfee web site at:

www.mcafeeb2b.com/naicommon/download/upgrade/login.asp

You will need to supply your customer grant number or user name and password to access this site.

## ABOUT THIS SERVICE PACK

### PURPOSE

This Service Pack updates several files to resolve a number of issues from the previous release.

### RESOLVED ISSUES

1. When upgrading from GroupShield 4.5 to GroupShield 5.0, the original paths to the quarantine and log database were not retained for the configuration settings. This issue has been resolved.

   This issue is now resolved by the Configuration Tool, which allows configuration settings from one GroupShield 5.0 server to be transferred to multiple GroupShield 5.0 servers.

2. When quarantining to a directory, if you deleted the quarantine directory including the parent directory structure, the directory structure was not created when the next on-access scan or scheduled scan attempted to quarantine.

   The required directories are now re-created.

3. When heuristic detection is enabled and a virus is found, the alert message may not display the virus name but instead displays “_“ (an underscore symbol).

   The message now displays the word “heuristic”.

4. When the scanning method was changed from VSAPI or MAPI to ESE, some events were not correctly formatted in the Event Viewer. This relates to entries of “ESE97”, where the description was “The description for Event ID (nnn) in Source (ESE97) cannot be found. The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer. The following information is part of the event: MSExchangeIS; ....”

   Events are now correctly formatted in the Event Viewer.

5. When a personal folder was defined as the delivery mailbox on an Outlook client and a message that had more than one infected item as

an attachment was sent using this personal folder, only the first item was detected, renamed or blocked. This occurred only during on-access scanning in ESE mode. This issue has been resolved.

6. E-mail messages forwarded by a PINE client on a Solaris system could not be blocked by subject line. This issue has been resolved.

7. Some aspects of the user interface did not meet the requirements for Windows 2000 certification. This issue has been resolved.

8. Under some circumstances, anti-virus policies distributed by the ePolicy Orchestrator were not being applied. This issue has been resolved.

9. Under some rare conditions, e-mails with unusually long recipient fields and subject fields that were received via SMTP were not handled properly. This issue has been resolved.

10. On cluster servers that have a German or French language version of Microsoft Exchange installed, GroupShield Setup issues a message stating that the local Exchange Server could not be contacted, and the installation is aborted.

    This issue cannot be resolved by the MSP version of the Service Pack. As a workaround, you may change the localized display name of the Information Store cluster resource in the cluster administration to English, namely ‘Microsoft Exchange Information Store’. A full MSI version of the Service Pack is available to address this problem.

(Issues resolved by Hot Fix1, released between Service Pack 1 and Service Pack 2)

11. An on-demand scan terminated immediately after it was started. This issue has been resolved.

12. Long attachment filenames that were either blocked or infected could cause the Exchange Information Store to fail if the option to 'Scan all files' was enabled in the on-access scanner settings. This issue has been resolved.

13. When ESE mode was enabled, the alert message and quarantined item referred to an e-mail that did not correspond to the subject-line blocking rules. This issue has been resolved.

14. Support for Microsoft ESE.DLL version 5.5.2655.50 has been added.

15. Support for Microsoft ESE.DLL version 5.5.2657.50 has been added in Service Pack 2.

16. In notification messages, only the first character of the recipient name was shown in the recipient field of some notification messages. This issue has been resolved.

17. In notification messages, the Internet Mail Service was shown as the sender of the message if the Microsoft Exchange option 'ResolveP2' was set. This issue has been resolved.

18. Changes to the 'Maximum Days' setting in the Logging tab of the GroupShield Administration console were not updated correctly if the change was made from a remote computer. This issue has been resolved.

19. There was an issue with Outbreak Manager. When the 'Block All' rule is triggered, Outbreak Manager now correctly quarantines or deletes blocked items based upon the GroupShield configuration settings.

20. Support for AutoUpdate via Linux 7.1 ftp servers has been added.

21. The Blocking options set within GroupShield were not reverted back to their original values after an Outbreak Manager rule triggered and modified these values. This issue has been resolved.

22. The on-demand scan failed when it was unable to access message properties. This issue has been resolved.

23. There was an exception error in ADMIN.EXE, the Microsoft Exchange Administrator console, when remotely applying a GroupShield configuration file. This issue has been resolved.

24. There was an issue where GroupShield was configured to block messages by subject line and a blocked message was subsequently released from the Quarantine database. The message was displayed without the original message text. This issue has been resolved.

25. A Dr. Watson error occurred if ePolicy Orchestrator was updating the GroupShield configuration at the same time as an Outbreak Manager rule triggered, and also changed the GroupShield configuration. This issue has been resolved.

26. This Service Pack includes an updated version of the GroupShield Configuration Tool, GSECONF.EXE, to resolve an issue where the GroupShield Logging parameters were not set correctly if running the

Configuration Tool from a remote computer. For instructions on how to use this utility, please refer to the User Manual, GSECONF.PDF.

27. This Service Pack also includes an updated version of the GroupShield .NAP file (policy management file for ePolicy Orchestrator) to resolve an issue when changing the on-access scanning mode to AVAPI/NONE or MAPI/MAPI. Previously the Administrator was not notified that the Microsoft Exchange Information Store required restarting when changing to these modes. A dialog box is now displayed if the Information Store needs to be restarted.

(Since Hot Fix 1)

28. In ESE mode, the Sender and Recipient information was not always correct when sending notification messages in Microsoft Exchange multi-site environments. This issue has been resolved.

29. GroupShield's ESE scanning mode caused performance issues when scanning very large attachments. This issue has been resolved.

30. During ESE on-access scanning in Microsoft Exchange multi-site environments, the sender was sometimes reported as "(Null)". This issue has been resolved.

31. In ESE mode, a message with both an infected body and attachment was not correctly quarantined. This issue has been resolved.

32. In ESE mode, attachments of quarantined messages contained superfluous garbled characters at the end. This issue has been resolved.

33. In ESE mode, the recipient information within quarantined message files consisted of garbled characters. This issue has been resolved.

34. After a configuration containing a subfolder for scanning by the on-demand scanner was exported, the subfolder was re-imported incorrectly. This issue has been resolved.

35. When folders and mailboxes were imported for scanning by the on-demand scanner, only the folders were imported. This issue has been resolved.

36. The on-demand scan stopped or slowed down when quarantining e-mail messages that had a large number of recipients or attachments. This issue has been resolved.

37. In rare cases, after an on-demand scan, the on-demand report form stated that there were quarantined items, but no details about the quarantined items were included in the report. This issue has been resolved.

38. If attachments were sent embedded within an e-mail and quarantined during an on-demand scan, the quarantine database entries did not have a quarantine number. This issue has been resolved.

39. An updated version of the Outbreak .NAP file (policy management file for ePolicy Orchestrator) has been added to resolve an issue with an expired certificate used for signing the included OCX.

## FILES INCLUDED WITH THIS SERVICE PACK

This Service Pack consists of a package called GS5E55S2.ZIP, which contains the following files:

SERVPK2.TXT =
This text file.

GS5E55S2.MSP =
Microsoft Patch file.

GSE500EN.NAP =
GroupShield policy management file for use with ePolicy Orchestrator.

OUTBREAK46.NAP =
Outbreak Manager policy management file for use with ePolicy Orchestrator.

GSECONF.EXE =
Main executable for Configuration Tool.

CONF0409.DLL =
Language-specific DLL component for English use.

CONF0407.DLL =
Language-specific DLL component for German use.

CONF040C.DLL =
Language-specific DLL component for French use.

CONF040A.DLL =
Language-specific DLL component for Spanish use.

CONF0411.DLL =
Language-specific DLL component for Japanese use.

GSECONF.PDF =
Release Notes for the Configuration Tool.

## INSTALLATION

For more information about the system requirements for McAfee GroupShield 5.0 for Microsoft Exchange 5.5, refer to the README.RTF file, CLUSTER.RTF file, or the Installation Guide that came with the software.

## INSTALLATION REQUIREMENTS

To use this Service Pack, you must have GroupShield 5.0 for Microsoft Exchange 5.5 software installed on the computer you intend to update.

> NOTE:
> This Service Pack does not work with earlier versions of GroupShield software.

## INSTALLING THE SERVICE PACK

To install this Service Pack, follow these steps:

40. Create a temporary directory on your hard disk, then download the .ZIP file from the McAfee web site to this directory.

41. Use a compression utility such as WinZip or PKZip to extract the Service Pack files from the .ZIP file into your temporary directory. Be sure to extract all the files. If using WinZip, select the Use Folder Names and the All Files options.

    You can download the necessary software from most shareware archives, or directly from these web sites:

    WinZip: <http://www.winzip.com/ddchomeb.htm>

    PKZip: <http://www.pkware.com/shareware/>

    The codes in the VALIDATE.TXT file can be used to ensure the files are the correct versions.

    If you plan to use the .ZIP file again, keep it available on your computer. Otherwise, delete the file.

42. Close all GroupShield Administration consoles that are running on the server or the Management Console.

43. Double-click the .MSP file to begin the automatic installation. To do a silent installation instead, see the section, “SILENT INSTALLATION”.

    A wizard page is displayed, similar to that in the original GroupShield.

44. Follow the instructions on the wizard panels.

NOTE:
The installation of the Service Pack requires that the original GroupShield Exchange 5.0 installation file, SETUP.MSI is available in its original location. If this file is not in the same location from which GroupShield 5.0 was originally installed, you might be prompted to specify the directory that contains SETUP.MSI.

Once the installation is completed, you can check that the Service Pack is applied correctly by several methods:

- Examine the registry for the current version of GroupShield. The key is:
  "HKEY_LOCAL_MACHINE\Software\McAfee\GroupShield Exchange",
  The value name is "ProductVersion".

- Examine the version details on the McAfee GroupShield user interface of the Microsoft Exchange Administrator.

- Examine the versions of files in the i386 subdirectory of the GroupShield installation location, such as avexch32.exe, gsevs.dll, naisadm.dll, and updsvc.exe.

## INSTALLING THE SERVICE PACK ON A CLUSTER

1. On the active cluster node, double-click the .MSP file to begin the installation. A wizard page is displayed, similar to that in the original GroupShield.

2. Follow the instructions on the wizard panels.

3. Once the Service Pack is installed on the active cluster node, go to the inactive node and double-click the .MSP file to begin the installation on the inactive node.
   You do not need to make the inactive node active in order to install the Service Pack on the inactive node. The installation will recognize that it is run on the inactive node and will install the files and components as appropriate.

4. Follow the instructions on the wizard panels to finish the installation on the inactive node.

## SILENT INSTALLATION

If required, you can install this Service Pack silently (without any on-screen prompts) from the command line.

To run a silent installation, use the following command:

```
      MSIEXEC /q /p <location>GS5E55S2.MSP  REINSTALL=all  REINSTALLMODE=omus
```

The MSIEXEC switches are as follows:

```
   /q = Silent install
   /p = Apply Patch
   <location> = Location of the Patch file
   GS5E55S2.MSP = Patch file
```

The REINSTALLMODE switches are as follows:

```
   o = overwrite missing or older files.
   m = re-write registry (HKLM)
   u = re-write registry (HKCU)
   s = update shortcuts.
```

## INSTALLING THE CONFIGURATION TOOL

NOTE:
You must have applied the patch file, GS5E55S2.MSP from the Service Pack before proceeding.

Copy the files, CONFxxxx.DLL and GSECONF.EXE, from the compressed file into one of the following folders on a GroupShield server:

```
      C:\exchsrvr\ADD-INS\NAISAdm5\i386
```
(C:\exchsrvr is the location where Microsoft Exchange 5.5 is normally installed.)

```
      C:\Program Files\McAfee\GroupShield Exchange\i386
```
(C:\Program Files\McAfee\GroupShield Exchange is the location where GroupShield is normally installed).

The file, CONFxxxx.DLL is language-specific. For example, CONF0409.DLL is for English use. See “Files Included with this Service Pack” for details.

---

## CONTACTING MCAFEE AND NETWORK ASSOCIATES

Technical Support
http://knowledge.nai.com

McAfee Beta Program
Beta Web Site
www.mcafeeb2b.com/beta/

E-mail
avbeta@nai.com

AVERT Anti-Virus Emergency Response Team
www.mcafeeb2b.com/naicommon/avert/default.asp

Download Site
www.mcafeeb2b.com/naicommon/download/

ftp://ftp.nai.com/pub/antivirus/datfiles/4.x

DAT File Updates
www.mcafeeb2b.com/naicommon/download/dats/find.asp

Product Upgrades
www.mcafeeb2b.com/naicommon/download/upgrade/login.asp

Valid grant number required.
Contact Network Associates Customer Service

On-Site Training Information
www.mcafeeb2b.com/services/mcafee-training/default.asp

Network Associates Customer Service
US, Canada, and Latin America toll-free:
Phone: +1-888-VIRUS NO or +1-888-847-8766
Monday - Friday, 8 a.m. - 8 p.m., Central Time

E-mail: services_corporate_division@nai.com
Web: www.nai.com
www.mcafeeb2b.com

For additional information on contacting Network Associates and McAfee – including toll-free numbers for other geographic areas -- see the CONTACT file that accompanied your original product release.

## COPYRIGHT AND TRADEMARK ATTRIBUTIONS

## TRADEMARKS

Active Firewall, Active Security, Active Security (in Katakana), ActiveHelp, ActiveShield, AntiVirus Anyware and design, Bomb Shelter, Certified Network Expert, Clean-Up, CleanUp Wizard, CNX, CNX Certification Certified Network Expert and design, Design (stylized N), Disk Minder, Distributed Sniffer System, Distributed Sniffer System (in Katakana), Dr Solomon’s, Dr Solomon’s label, Enterprise SecureCast, Enterprise SecureCast (in Katakana), Event Orchestrator, EZ SetUp, First Aid, ForceField, GMT, GroupShield, GroupShield (in Katakana), Guard Dog, HelpDesk, HomeGuard, Hunter, LANGuru, LANGuru (in Katakana), M and design, Magic Solutions, Magic Solutions (in Katakana), Magic University, MagicSpy, MagicTree, McAfee, McAfee (in Katakana), McAfee and design, McAfee.com, MultiMedia Cloaking, Net Tools, Net Tools (in

## LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO NETWORK ASSOCIATES, INC. OR THE PLACE OF PURCHASE FOR A FULL REFUND.