McAfee VirusScan for
Windows 95 and Windows 98

Advanced Operations Guide

Version 5.0

LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") BY NETWORK ASSOCIATES, INC. ("McAfee"). BY CLICKING THE ACCEPT BUTTON OR INSTALLING THE SOFTWARE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE. (IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.)

1. **License Grant.** Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, McAfee hereby grants to you a non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation"). You may install one copy of the Software on one computer, workstation, personal digital assistant, pager, "smart phone" or other electronic device for which the Software was designed (each, a "Client Device"). If the Software is licensed as a suite or bundle with more than one specified Software product, this license applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any of such Software products individually.

(i.e., the required number of licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software can exceed the number of licenses you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each Client Device or seat that is licensed, provided that each such copy contains all of the Documentation's proprietary notices.

c. **Volume Licenses.** If the Software is licensed with volume license terms specified in the applicable price list or product packaging for the Software, you may make, use and install as many additional copies of the Software on the number of Client Devices as the volume license authorizes. You must have a reasonable mechanism in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume license, provided that each such copy contains all of the Documentation's proprietary notices.

2. **Term.** This Agreement is effective for an unlimited duration unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must destroy all copies of the Software and the Documentation. You may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

3. **Updates.** For the time period specified in the applicable price list or product packaging for the Software you are entitled to download revisions or updates to the Software when and as McAfee publishes them via its electronic bulletin board system, website or through other online services. For a period of ninety (90) days from the date of the original purchase of the Software, you are entitled to download one (1) revision or upgrade to the Software when and as McAfee publishes it via its electronic bulletin board system, website or through other online services. After the specified time period, you have no further rights to receive any revisions or upgrades without purchase of a new license or annual upgrade plan to the Software.

4. **Ownership Rights.** The Software is protected by United States copyright laws and international treaty provisions. McAfee and its suppliers own and retain all right, title and interest in and to the Software, including all copyrights, patents, trade secret rights, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement. All copies of the Software and Documentation made hereunder must contain the same proprietary notices that appear on and in the Software and Documentation.

5. **Restrictions.** You may not rent, lease, loan or resell the Software. You may not permit third parties to benefit from the use or functionality of the Software via a timesharing, service bureau or other arrangement, except to the extent such use is specified in the applicable list price or product packaging for the Software. You may not transfer any of the rights granted to you under this Agreement. You may not reverse engineer, decompile, or disassemble the Software, except to the extent the foregoing restriction is expressly prohibited by applicable law. You may not modify, or create derivative works based upon, the Software in whole or in part. You may not copy the Software or Documentation except as expressly permitted in Section 1 above. You may not remove any proprietary notices or labels on the Software. All rights not expressly set forth hereunder are reserved by McAfee. McAfee reserves the right to periodically conduct audits upon advance written notice to verify compliance with the terms of this Agreement.

6. **Warranty and Disclaimer**

   a. **Limited Warranty.** McAfee warrants that for sixty (60) days from the date of original purchase the media (e.g., diskettes) on which the Software is contained will be free from defects in materials and workmanship.

   b. **Customer Remedies.** McAfee's and its suppliers' entire liability and your exclusive remedy for any breach of the foregoing warranty shall be, at McAfee's option, either (i) return of the purchase price paid for the license, if any, or (ii) replacement of the defective media in which the Software is contained. You must return the defective media to McAfee at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period. Outside the United States, this remedy is not available to the extent McAfee is subject to restrictions under United States export control laws and regulations.

   c. **Warranty Disclaimer.** Except for the limited warranty set forth herein, THE SOFTWARE IS PROVIDED "AS IS." TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, MCAFEE DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. YOU ASSUME RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, MCAFEE MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

7. **Limitation of Liability.** UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER IN TORT, CONTRACT, OR OTHERWISE, SHALL MCAFEE OR ITS SUPPLIERS BE LIABLE TO YOU OR TO ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR FOR ANY AND ALL OTHER DAMAGES OR LOSSES. IN NO EVENT WILL MCAFEE BE LIABLE FOR ANY DAMAGES IN EXCESS OF THE LIST PRICE MCAFEE CHARGES FOR A LICENSE TO THE SOFTWARE, EVEN IF MCAFEE SHALL HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT THAT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE, SOME STATES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

8. **United States Government.** The Software and accompanying Documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Software and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

9. **Export Controls.** Neither the Software nor the Documentation and underlying information or technology may be downloaded or otherwise exported or re-exported (i) into (or to a national or resident of) Cuba, Iran, Iraq, Libya, North Korea, Sudan, Syria or any other country to which the United States has embargoed goods; or (ii) to anyone on the United States Treasury Department's list of Specially Designated Nations or the United States Commerce Department's Table of Denial Orders. By downloading or using the Software you are agreeing to the foregoing and you are certifying that you are not located in, under the control of, or a national or resident of any such country or on any such list.

   IN ADDITION, YOU SHOULD BE AWARE OF THE FOLLOWING: EXPORT OF THE SOFTWARE MAY BE SUBJECT TO COMPLIANCE WITH THE RULES AND REGULATIONS PROMULGATED FROM TIME TO TIME BY THE BUREAU OF EXPORT ADMINISTRATION, UNITED STATES DEPARTMENT OF COMMERCE, WHICH RESTRICT THE EXPORT AND RE-EXPORT OF CERTAIN PRODUCTS AND TECHNICAL DATA. IF THE EXPORT OF THE SOFTWARE IS CONTROLLED UNDER SUCH RULES AND REGULATIONS, THEN THE SOFTWARE SHALL NOT BE EXPORTED OR RE-EXPORTED, DIRECTLY OR INDIRECTLY, (A) WITHOUT ALL EXPORT OR RE-EXPORT LICENSES AND UNITED STATES OR OTHER GOVERNMENTAL APPROVALS REQUIRED BY ANY APPLICABLE LAWS, OR (B) IN VIOLATION OF ANY APPLICABLE PROHIBITION AGAINST THE EXPORT OR RE-EXPORT OF ANY PART OF THE SOFTWARE.

SOME COUNTRIES HAVE RESTRICTIONS ON THE USE OF ENCRYPTION WITHIN THEIR BORDERS, OR THE IMPORT OR EXPORT OF ENCRYPTION EVEN IF FOR ONLY TEMPORARY PERSONAL OR BUSINESS USE. YOU ACKNOWLEDGE THAT THE IMPLEMENTATION AND ENFORCEMENT OF THESE LAWS IS NOT ALWAYS CONSISTENT AS TO SPECIFIC COUNTRIES. ALTHOUGH THE FOLLOWING COUNTRIES ARE NOT AN EXHAUSTIVE LIST THERE MAY EXIST RESTRICTIONS ON THE EXPORTATION TO, OR IMPORTATION OF, ENCRYPTION BY: BELGIUM, CHINA (INCLUDING HONG KONG), FRANCE, INDIA, INDONESIA, ISRAEL, RUSSIA, SAUDI ARABIA, SINGAPORE, AND SOUTH KOREA. YOU ACKNOWLEDGE IT IS YOUR ULTIMATE RESPONSIBILITY TO COMPLY WITH ANY AND ALL GOVERNMENT EXPORT AND OTHER APPLICABLE LAWS AND THAT MCAFEE HAS NO FURTHER RESPONSIBILITY AFTER THE INITIAL SALE TO YOU WITHIN THE ORIGINAL COUNTRY OF SALE.

10. **High Risk Activities.** The Software is not fault-tolerant and is not designed or intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines, or any other application in which the failure of the Software could lead directly to death, personal injury, or severe physical or property damage (collectively, "High Risk Activities"). McAfee expressly disclaims any express or implied warranty of fitness for High Risk Activities.

11. **Miscellaneous.** This Agreement is governed by the laws of the United States and the State of California, without reference to conflict of laws principles. The application of the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. This Agreement sets forth all rights for the user of the Software and is the entire agreement between the parties. This Agreement supersedes any other communications with respect to the Software and Documentation. This Agreement may not be modified except by a written addendum issued by a duly authorized representative of McAfee. No provision hereof shall be deemed waived unless such waiver shall be in writing and signed by McAfee or a duly authorized representative of McAfee. If any provision of this Agreement is held invalid, the remainder of this Agreement shall continue in full force and effect. The parties confirm that it is their wish that this Agreement has been written in the English language only.

12. **McAfee Customer Contact.** If you have any questions concerning these terms and conditions, or if you would like to contact McAfee for any other reason, please call (408) 988-3832, fax (408) 970-9727, or write: McAfee Software, 3965 Freedom Circle, Santa Clara, California 95054. http://www.mcafee.com.

    Statements made to you in the course of this sale are subject to the Year 2000 Information and Readiness Disclosure Act (Public Law 105-271). In the case of a dispute, this Act may reduce your legal rights regarding the use of any statements regarding Year 2000 readiness, unless otherwise specified in your contract or tariff.

Table of Contents

Preface

This document contains VirusScan reference information. This information includes the format of VirusScan file formats and how to run VirusScan from the command line.

For information on using VirusScan, see the “McAfee VirusScan for Windows 95 and Windows 98 User’s Guide.”

Understanding the .VSC File Format 1

Saving VirusScan task settings

When you save VirusScan configuration options in a .VSC file, you are saving a text file formatted in a manner similar to the Windows .INI file that outlines VirusScan's settings. The file consists of variables that have a name followed by an equal (=) sign and a value. The values define which settings you selected for VirusScan configuration. The variables are arranged in eight groups: ScanOptions, DetectionOptions, AlertOptions, ActionOptions, ReportOptions, ScanItems, SecurityOptions, and ExcludedItems. The tables on the following pages list each option, along with its default and possible values.

You can distribute .VSC files to other VirusScan users at other computers, overwrite the existing .VSC files on those computers, and thereby copy VShield's System Scan settings for another user to run. To edit the .VSC file, open it with a text editor, such as Notepad.

- **NOTE:** Boolean variables can have only 0 and 1 as possible values. The 0 value tells VShield to disable the setting, while 1 enables the setting.

ScanOptions

Variable	Description
bAutoStart	Type: Boolean (0/1) Instructs VirusScan to automatically start scan when launched Default Value: 0
bAutoExit	Type: Boolean (0/1) Instructs VirusScan to exit automatically when finished scanning if no viruses were found Default Value: 0

Variable	Description
bAlwaysExit	Type: Boolean (0/1) Instructs VirusScan to exit automatically when finished scanning even if viruses were found Default Value: 0
bSkipMemoryScan	Type: Boolean (0/1) Instructs VirusScan to skip memory scan Default Value: 0
bSkipBootScan	Type: Boolean (0/1) Instructs VirusScan to skip boot sector scanning Default Value: 0
bSkipSplash	Type: Boolean (0/1) Instructs VirusScan to skip display of the VirusScan splash screen on startup Default Value: 0

DetectionOptions

Variable	Description
bScanAllFiles	Type: Boolean (0/1) Instructs VirusScan to scan all file types Default Value: 0
bScanCompressed	Type: Boolean (0/1) Instructs VirusScan to Scan in compressed files Default Value: 1
szProgramExtensions	Type: String Specifies which file extensions VirusScan will scan Default Value: EXE COM DO? XL?
szDefaultProgramExtensions	Type: String Specifies default value for szProgramExtensions Default Value: EXE COM DO? XL?

AlertOptions

Variable	Description
bNetworkAlert	Type: Boolean (0/1) Instructs VirusScan to send an alert (.ALR) file to a network path being monitored by NetShield for Centralized Alerting when a virus is found Default Value: 0
bSoundAlert	Type: Boolean (0/1) Instructs VirusScan to sound an audible alert when a virus is detected Default Value: 1
szNetworkAlertPath	Type: String Specifies the network alert path being monitored by NetShield for Centralized Alerting. The folder this path points to should contain the Centralized Alerting file, CENTALRT.TXT Default Value: None

ActionOptions

Variable	Description
bDisplayMessage	Type: Boolean (0/1) Instructs VirusScan to display a message upon detection of a virus Default Value: 0
ScanAction	Type: Integer (0-5) Instructs VirusScan to take the action specified when a virus is detected Possible values: 0 - Prompt for action 1 - Move automatically 2 - Clean automatically 3 - Delete automatically 4 - Continue Default Value: 0
bButtonClean	Type: Boolean (0/1) Instructs VirusScan to display the Clean button if ScanAction=0 Default Value: 1
bButtonDelete	Type: Boolean (0/1) Instructs VirusScan to display the Delete button if ScanAction=0 Default Value: 1
bButtonExclude	Type: Boolean (0/1) Instructs VirusScan to display the Exclude button if ScanAction=0 Default Value: 1
bButtonMove	Type: Boolean (0/1) Instructs VirusScan to display the Move button if ScanAction=0 Default Value: 1

Variable	Description
bButtonContinue	Type: Boolean (0/1) Instructs VirusScan to display the Continue button if ScanAction=0 Default Value: 1
bButtonStop	Type: Boolean (0/1) Instructs VirusScan to display the Stop button if ScanAction=0 Default Value: 1
szMoveToFolder	Type: String Indicates where infected files should be moved Default Value: \Infected
szCustomMessage	Type: String Indicates text of message to be displayed on virus detection Default Value: Possible Virus Detected

ReportOptions

Variable	Description
bLogToFile	Type: Boolean (0/1) Instructs VirusScan to log scan activity to a file Default Value: 1
bLimitSize	Type: Boolean (0/1) Instructs VirusScan to limit the size of the log file Default Value: 1
uMaxKilobytes	Type: Integer (10-999) Specifies maximum size of log file in kilobytes Default Value: 10
bLogDetection	Type: Boolean (0/1) Instructs VirusScan to log virus detection Default Value: 1

Variable	Description
bLogClean	Type: Boolean (0/1) Instructs VirusScan to log virus cleaning Default Value: 1
bLogDelete	Type: Boolean (0/1) Instructs VirusScan to log file deletions Default Value: 1
bLogMove	Type: Boolean (0/1) Instructs VirusScan to log file moves Default Value: 1
bLogSettings	Type: Boolean (0/1) Instructs VirusScan to log session settings Default Value: 1
bLogSummary	Type: Boolean (0/1) Instructs VirusScan to log session summaries Default Value: 1
bLogDateTime	Type: Boolean (0/1) Instructs VirusScan to log date and time of scan activity Default Value: 1
bLogUserName	Type: Boolean (0/1) Instructs VirusScan to log user name Default Value: 1
szLogFileName	Type: String Specifies path to log file Default Value: C:\Program Files\Network Associates\McAfee Viruscan\VSCLOG.TXT

ScanItems

Variable	Description
ScanItem_x, where x is a zero-based index	Type: String Instructs VirusScan to scan the item Default value: `C:|1 *` * The string is separated into fields using the pipe (|) character: Field 1 - Path of item to scan. Field 2 - Boolean (1/0) Possible values: 1 - Instructs VirusScan to scan subfolders of the item 2 - Instructs VirusScan not to scan subfolders of the item

SecurityOptions

Variable	Description
szPasswordProtect	Type: String This variable is not user-configurable Default Value: 0
szPasswordCRC	Type: String This variable is not user-configurable Default Value: 0
szSerialNumber	Type: String This variable is not user-configurable Default Value: 0

ExcludedItems

Variable	Description
NumExcludeItems	Type: Integer (0-n) Defines the number of items excluded from scanning Default value: 1
ExcludedItem_x, where x is a zero-based index	Type: String Instructs VirusScan to exclude the item from scanning Default value: `\Recycled|*.*|1|1 *` * The string is separated into fields using the pipe (|) character: Field 1 - Folder portion of item to exclude. Leave blank for a single file anywhere on the system. Field 2 - File portion of the item to exclude. Leave blank if a folder is excluded without a file name. Field 3 - Integer (1-3) Possible values: 1 - Exclude from file scanning 2 - Exclude from boot-record scanning 3 - Exclude from both boot-record and file scanning Field 4 - Boolean (1/0) Possible values: 1 - Instructs VirusScan to exclude subfolders of the excluded item 2 - Instructs VirusScan to not exclude subfolders

Understanding the .VSH File Format 2

Saving VShield task settings

When you choose configuration options for VShield's System Scan module, the program saves its settings in a .VSH file in the VirusScan program directory. The .VSH file is a configuration text file, formatted similarly to the Windows .INI file, which outlines VShield's settings. Each variable in the file has a name followed by an equal (=) sign and a value. The values define which settings you selected for VShield configuration. The variables are arranged in seven groups: General, DetectionOptions, AlertOptions, ActionOptions, ReportOptions, SecurityOptions, and ExclusionOptions. The tables on the following pages list each option, along with its default and possible values.

You can distribute .VSH files to other VShield users at other computers, overwrite the existing .VSH files on those computers, and thereby copy VShield's System Scan settings for another user to run. To edit the VSH file, open it with a text editor, such as Notepad.

- **NOTE:** Boolean variables can have only 0 and 1 as possible values. The 0 value tells VShield to disable the setting, while 1 enables the setting.

General

Variable	Description
bLoadAtStartup	Type: Boolean (1/0) Defines if VShield should be loaded at system startup Default value: 1
bCanBeDisabled	Type: Boolean (1/0) Defines if VShield can be disabled Default value: 1

bShowTaskbarIcon	Type: Boolean (1/0) Defines whether VShield taskbar icon is displayed Default value: 1
bNoSplash	Type: Boolean (1/0) Instructs VShield to not show splash screen when program is launched Default value: 0

DetectionOptions

Variable	Description
szProgramExtensions	Type: String Defines extensions to be scanned Default value: EXE COM DO? XL?
szDefaultProgramExtensions	Type: String Defines extensions to be used as default program extensions during scan configuration Default value: EXE COM DO? XL?
bScanOnExecute	Type: Boolean (1/0) Instructs VShield to scan when files are run Default value: 1
bScanOnOpen	Type: Boolean (1/0) Instructs VShield to scan when files are opened Default value: 1
bScanOnCreate	Type: Boolean (1/0) Instructs VShield to when files are created Default value: 1
bScanOnRename	Type: Boolean (1/0) Instructs VShield to when files are renamed Default value: 1
bScanOnBootAccess	Type: Boolean (1/0) Instructs VShield to scan the boot record of a disk drive the first time it is accessed Default value: 1

Variable	Description
bScanAllFiles	Type: Boolean (1/0) Instructs program to scan inside all files Default value: 0
bScanCompressed	Type: Boolean (1/0) Instructs program to scan inside compressed files (PkLite, LZEXE) Default value: 1

AlertOptions

Variable	Description
bNetworkAlert	Type: Boolean (1/0) Instructs VShield to send a network alert to a folder being monitored by NetShield for Centralized Alerting. Default Value: 0
szNetworkAlertPath	Type: String Specifies path being monitored by NetShield for Centralized Alerting. Default Value: None

ActionOptions

Variable	Description
szCustomMessage	Type: String Defines custom message to be displayed upon virus detection if action is set to Prompt for Action Default value: `Possible Virus Detected`
szMoveToFolder	Type: String Defines folder to which infected files should be moved Default value: `\Infected`

uVshieldAction	Type: Integer (1-5) Instructs VShield to take the action specified when a virus is detected Possible values: 1 - Prompt for action 2 - Move infected files to a folder 3 - Clean infected files automatically (Deny access if files can't be cleaned) 4 - Delete infected files automatically 5 - Deny access to infected files Default value: 1
bButtonClean	Type: Boolean (1/0) Instructs VShield to give user option of cleaning file if Prompt for Action is selected and a virus is detected Default value: 1

Variable	Description
bButtonDelete	Type: Boolean (1/0) Instructs VShield to give user option of deleting file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonExclude	Type: Boolean (1/0) Instructs VShield to give user option of excluding file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonStop	Type: Boolean (1/0) Instructs VShield to give user option of denying access to the infected file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonContinue	Type: Boolean (1/0) Instructs VShield to give user option of continuing the intercepted event if Prompt for Action is selected and a virus is detected Default value: 1
bDisplayMessage	Type: Boolean (1/0) Defines if custom message should be displayed in the Prompt for Action dialog box upon virus detection Default value: 0

ReportOptions

Variable	Description
szLogFileName	Type: String Defines log file name Default value: C:\Program Files\Network Associates\McAfee Viruscan\Vshlog.txt
bLogToFile	Type: Boolean (1/0) Defines if scan results should be logged into log file Default value: 1

Variable	Description
bLimitSize	Type: Boolean (1/0) Defines if size of the log file should be limited Default value: 1
uMaxKilobytes	Type: Integer (10-999) Defines maximum size of the log file in kilobytes Default value: 100
bLogDetection	Type: Boolean (1/0) Defines if scanning results should be logged Default value: 1
bLogClean	Type: Boolean (1/0) Defines if cleaning results should be logged Default value: 1
bLogDelete	Type: Boolean (1/0) Defines if infected file delete operations should be logged Default value: 1
bLogMove	Type: Boolean (1/0) Defines if infected file move operations should be logged Default value: 1
bLogSettings	Type: Boolean (1/0) Defines if session settings should be logged on shutdown Default value: 1
bLogSummary	Type: Boolean (1/0) Defines if session summary should be logged on shutdown Default value: 1
bLogDateTime	Type: Boolean (1/0) Defines if time and date of an event should be logged Default value: 1
bLogUserName	Type: Boolean (1/0) Defines if user name should be logged Default value: 1

SecurityOptions

Variable	Description
szPasswordProtect	Type: String This option is not user-configurable. Default Value: 0
szPasswordCRC	Type: String This option is not user-configurable. Default Value: 0

ExclusionOptions

Variable	Description
szExclusionsFileName	Type: String This option is not user-configurable.

NumExcludedItems	Type: Integer (0-n) Defines the number of items excluded from on-access scanning Default value: 0
ExcludedItem_x, where x is a zero-based index	Type: String Instructs VShield to exclude the item from on-access scanning Default value: `\Recycled|*.*|1|1 *` * The string is separated into fields using the pipe (|) character: Field 1 - Folder portion of item to exclude. Leave blank for a single file anywhere on the system. Field 2 - File portion of the item to exclude. Leave blank if a folder is excluded without a file name. Field 3 - Integer (1-3) Possible values: 1 - Exclude from file-access scanning 2 - Exclude from boot-record scanning 3 - Exclude from both boot-record and file-access scanning Field 4 - Boolean (1/0) Possible values: 1 - Instructs VShield to exclude subfolders of the excluded item 2 - Instructs VShield to not exclude subfolders

Using VirusScan Command-Line Options 3

Running VirusScan Command line

You can run VirusScan Command Line either from a Windows MS-DOS Prompt window, or by restarting your computer in DOS mode. Network Associates recommends restarting in DOS mode for best results. To learn how to restart your computer in DOS mode, see your Microsoft Windows documentation.

To run VirusScan Command line, follow these steps:

1. Open an MS-DOS Prompt window from within Windows, or restart your computer in DOS mode.
2. Change to the VirusScan program directory. If you installed VirusScan with its default options, type this line at your command prompt to locate the correct directory:

   ```
   C:\Progra~1\McAfee\McAfee~1
   ```

3. Type `scan`, followed by the scan options you want to use, at the command prompt.

   VirusScan Command Line will start immediately and begin scanning your system with the options you choose. When it has finished, it will display the results of its scan operation, then return to the command prompt.

4. To run another scan operation, repeat Step 3. To close the MS-DOS Prompt window, type `exit` at the command prompt. If you restarted your computer in DOS mode, type `win` to start Windows, or restart your computer as you would normally.

The tables on the following pages list all of the VirusScan options available.

- **NOTE:** When you specify a file name as part of a command-line option, you must include the full path to the file if it is not located in the VirusScan program directory.

Command line options

Command-line Option	Description
/? or /HELP	Displays a list of VirusScan command-line options, each with a brief description. To open the “Help” list, use either of these options alone on the command line.
/ADL For OS/2, includes CD-ROM when used with /NODDA	Scan all local drives-including compressed and PCMCIA drives, but not diskettes--in addition to any other drive specified on the command line. Note: To scan both local and network drives, use the /ADL and /ADN commands together in the same command line.
/ADN For OS/2, use /ADL, above, plus /NODDA for CD-ROM	Scan all network drives--including CD-ROM--for viruses, in addition to any other drive(s) specified on the command line. Note: To scan both local drives and network drives, use the /ADL and /ADN commands together in the same command line.

Command-line Option	Description
/AF <filename>	Inserts validation code which VirusScan uses in virus detection tasks into the file you specify. /AF performs the same function as /AV, but stores its data in a separate file rather than changing the executable files themselves. Notes: * To use /AF, you must specify a [filename], including the full path. If the target path is a network drive, you must have rights to create and delete files on that drive. * The /AF option will not store any information about the Master Boot Record or boot sector of the drive being scanned. * Use of the /AF option will increase your scanning time by about 300%. * This validation code increases the size of each file by 98 bytes.
/ALERTPATH <dir>	Designates a directory as a network path monitored by Centralized Alerting.
/ALL	Overrides the default scan setting by scanning all infectable files—regardless of extension. Note: * Using the /ALL option substantially increases the scanning time required. Use it if you find a virus or suspect you have one. * By default, VirusScan only scans files with the following extensions: .EXE, .COM, .SYS, .BIN, .OVL, .DLL, .DOC, .DOT, .XLA, .XLS, .XLT, .RTF, and .VXD. These are the file types that are most susceptible to viruses.

Command-line Option	Description
/ANYACCESS	Scans only floppy disk files and executables in VirusScan for OS/2. Scans: * the boot sector whenever a diskette is either read or written to * executables * any newly created files. Note: /ANYACCESS cannot be used with /POLY.
/APPEND	* This command, used with /REPORT, will append report message text to the specified report file. * If the /REPORT option is used without /APPEND, the /REPORT option will overwrite the specified report file.
/AV	/AV Adds recovery and validation data to each standard executable file (.EXE, .COM, .SYS, .BIN, .OVL, and .DLL) which VirusScan uses in virus detection tasks. Notes: * To update files on a shared network drive, you must have update access rights. * The /AV option does not store any information about the Master Boot Record or boot sector of the drive being scanned. * This validation code increases the size of each file by 98 bytes. * To exclude self-modifying or self-checking files, or damaged files that might cause false alarms, use the /EXCLUDE option. * Using any of the /AV, /CV, or /RV options together in the same command line returns an error.
/BOOT	Scan boot sector and master boot record only.

Command-line Option	Description
/BOOTACCESS This option not valid for VirusScan Command Line for Windows NT	Scans a diskette's boot sector for viruses whenever the diskette is accessed (including read/write operations).
/CERTIFY This option not valid for VirusScan Command Line for Windows NT	Prevents your system from running files that do not have VirusScan validation codes.
/CF filename	Checks the validation data stored by the /AF option in [filename] as a means of detecting new or unknown viruses. If VirusScan finds that a file or system area has changed, VirusScan will report that a viral infection may have occurred. Notes: * Use of the /CF option increases scanning time by about 250%. * Using any of the /AF, /CF, or /RF options together in a command line returns an error. * Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. If you use /CF on these systems, VirusScan will continuously report boot sector modifications even though no virus may be present. Check your computer's reference manual to determine whether your PC has self-modifying boot code.
/CLEAN	Cleans viruses from infected files and system areas.
/CLEANDOC	Cleans viruses from infected Microsoft Word and Office document files only
/CLEANDOCALL	Cleans all macros from Microsoft Word and Office documents. This option deletes all macros, including macros not infected by a virus.

Command-line Option	Description
/CLEAN	Clean viruses from all infected files and system areas.
/CLEANDOC	Cleans viruses from infected Microsoft Word and Office document files only.
/CLEANDOCALL	As a precautionary measure against macro viruses, /CLEANDOCALL cleans all macros from Microsoft Word and Office documents. Note: This option deletes all macros, including macros not infected by a virus.
/CONTACT <message>	This option not valid for VirusScan Command Line for Windows NT Displays specified message when a virus is detected.
/CONTACTFILE filename	Display the contents of <filename> when a virus is found. It is an opportunity to provide contact information and instructions to the user when a virus is encountered. This option is especially useful in network environments, because you can easily maintain the message text in a central file rather than on each workstation. Note: Any character is valid in a contact message except a backslash (\). Messages beginning with a slash (/)or a hyphen (-) should be placed in quotation marks.

Command-line Option	Description
/CV	Check validation codes added to files by /AV to help detect new or unknown viruses. For more information, see “Configuring Validation Options” on page 37. If a file is modified, VirusScan reports that a viral infection may have occurred. Note: * Using the /CV option will increase scanning time by about 50%. * The /CV option does not check the boot sector for changes. * Using any of the /AV, /CV, or /RV options together in the same command line returns an error.
/DEL	Deletes infected files permanently.
/EXCLUDE <filename or directory> This option not available with VirusScan for OS/2	Use this option to: * Exclude specific files from a scan. List the complete path to each file you want to exclude on its own line. You may use wildcards * and ? * Exclude directories and multiple files; e.g., /EXCLUDE c:\dos excludes all directories and files beginning with c:\dos. * Exclude specific files from both /AF and /AV validation and /CF and /CV checking.
/FAST	* Speeds up the scan by asking VirusScan to examine a smaller portion of each file for viruses. * Because it limits virus detection activities, do not use this option if you have found a virus or suspect one. * Use of this option will reduce scanning time by about 15%.
/FILEACCESS This option not valid for VirusScan Command Line for Windows NT	Scans executable files when they are accessed on a diskette, but does not check the boot sector.

Command-line Option	Description
/FORCE	* VirusScan will replace an infected Master Boot Record (MBR) or boot sector with a generic MBR or boot sector if cleaning fails. * VirusScan will use its generic Master Boot Record when cleaning partition table viruses. * Cleans infected boot sectors of diskettes. * Works even if a remover is not yet available for the boot sector virus.
/FREQUENCY hours	Do not scan [n] hours after the previous scan. * In environments where the risk of viral infection is very low, use this option to prevent unnecessary scans. * Remember, the greater the scan frequency, the greater your protection against infection.
/HELP or /?	Displays a list of VirusScan command-line options, each with a brief description. To open the “Help” list, use either of these options alone on the command line.
/IGNORE drive(s) This option not valid for VirusScan Command Line for Windows NT.	Does not check programs loaded from the specified drive(s).
/LOAD filename	* Load scanning options from the named file. * Use this option to perform a scan you’ve already configured by loading custom settings saved in an ASCII-formatted file.

Command-line Option	Description
/LOCK This option not available with VirusScan for OS/2 or VirusScan Command Line for Windows NT.	* With this /LOCK option enabled, VirusScan will halt and lock your system if VirusScan finds a virus. * We recommend using /LOCK with the /CONTACTFILE option to tell users what to do or whom to contact if VirusScan locks the system. * /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs.
/LOG	VirusScan will log the date and time of the current scan by updating or creating a file called SCAN.LOG in the root of the target drive.
/LONGYEAR	* Display years in four-digit format. * By default, VirusScan reports dates in two-digit format.
/MACROHEUR x	Allows you to adjust the level of sensitivity used when performing heuristic scanning for macro viruses in Microsoft Word documents. When using this command, substitute 0, 1, 2, 3, 4, 5, or 100 for the letter x. * Choosing 0 turns off the heuristic scanning feature. * Choosing 1 (minimum) through 5 (maximum) turns on heuristic scanning at varying levels of sensitivity. * Choosing 100 causes VirusScan to detect all macros, including those not found to be viral or probably viral. Such detections are reported as: “This file contains macros.”

Command-line Option	Description
/MANY	* Scans multiple diskettes consecutively in a single drive. VirusScan will prompt you for each diskette. * Use this option to check multiple diskettes quickly. * You cannot use the /MANY option if you run VirusScan from a boot diskette and you have only one floppy drive. For example, if you are running VirusScan from a diskette in the A: drive, and attempt to use the A: drive to scan other diskettes, VirusScan will become unavailable as soon as you remove the VirusScan diskette. The following command will cause an error during execution: a:\scan a: /many
/MAXFILESIZE xxx.x	Scan only files no larger than xxx.x megabytes.
/MEMEXCL hhhh[-hhhh] Not valid for OS/2 or Windows NT This option not available with VirusScan for OS/2 or VirusScan Command Line for Windows NT.	Does not allow VShield to use UMB address specified. Exclude memory area from scanning. (The default is A000-FFFF, 0000=Scan all.) This will prevent VirusScan from checking areas in upper memory which may contain memory-mapped hardware capable of causing false alarms.

Command-line Option	Description
/MOVE <dir> or *.???	/MOVE directory: Moves all infected files found during a scan to the specified directory, preserving drive letter and directory structure. Note: This option has no effect if the Master Boot Record or boot sector is infected, since these are not actually files. /MOVE*.???: VirusScan will change the extension of infected files, but not move them. For example, using the /MOVE*.BAD option will result in any infected files being simply renamed with the extension .BAD but not physically moved.
/NOBEEP	Disables the tone that sounds whenever VirusScan finds a virus.
/NOBREAK	Disables CTRL-C and CTRL-BREAK during scans. * Users will not be able to halt scans in progress with /NOBREAK in use. * Use this option with /LOG to create a meaningful audit trail of regularly scheduled scans
/NOCOMP	Skips checking of compressed executables created with the LZEXE or PkLite file-compression programs. * This reduces scanning time when a full scan is not needed. Otherwise, by default, VirusScan checks inside executable, or self-decompressing, files by decompressing each file in memory and checks for virus signatures. * VirusScan will still check for modifications to compressed executables if they contain VirusScan validation codes.

Command-line Option	Description
/NODDA	No direct disk access. This prevents VirusScan from accessing the boot record. * This feature has been added to allow VirusScan to run under Windows NT. * You might need to use this option on some device-driven drives. * Using /NODDA with the /ADN or /ADL switches may generate errors when accessing empty CD-ROM drives or empty Zip drives. If this occurs, type F (for Fail) in response to the error messages to continue the scan.
/NODISK This option not valid for VirusScan Command Line for Windows NT.	Does not scan boot sector while loading VShield.
/NODOC	Does not scan Microsoft Office files.
/NOEXPIRE	Disables the “expiration date” message if the VirusScan data files are out of date.
/NOMDB This option valid only for VirusScan Command Line for Windows NT.	Does not scan MDB files.
/NOMEM This option not available with VirusScan for OS/2 or VirusScan Command Line for Windows NT.	Does not scan memory for viruses. * This greatly reduces scan time. * Use /NOMEM only when you are absolutely certain that your computer is virus-free.
/NOREMOVE	Prevents VShield from being removed from memory with the /REMOVE switch
/NOUMB	Does not use upper memory blocks (UMB).
/NOWARMBOOT This option not valid for VirusScan Command Line for Windows NT.	Does not check the diskette boot sector for viruses during a warm boot (system reset or CTRL+ALT+DEL).

Command-line Option	Description
/NOXMS This option not valid for VirusScan Command Line for Windows NT.	Does not use extended memory (XMS).
/ONLY drive(s)	Checks only programs loaded from the specified drive(s).
/PAUSE	Enables screen pause. The “Press any key to continue” prompt will appear when VirusScan fills a screen with messages (for example, when you’re using the /SHOWLOG or /VIRLIST options).Otherwise, by default, VirusScan fills and scrolls a screen continuously without stopping, which allows VirusScan to run on PCs with multiple drives or that have severe infections without needing your input. We recommend omitting /PAUSE using the report options (/REPORT, /RPTCOR, /RPTMOD, and /RPTERR)
/PLAD Not valid for ScanPM or VirusScan Command Line for Windows NT.	Preserve Last Access Dates on Novell NetWare drives. Normally, proprietary network drives update the last access date when VirusScan opens and examines a file. However, some tape backup systems use this last access date to decide whether to back up the file. Use /PLAD to ensure that the last access date does not change as the result of scanning.
/POLY	Checks for polymorphic viruses. Note: /ANYACCESS cannot be used with /POLY.
/RECONNECT	Restores on-access scanning after certain drivers or TSRs have disabled it.
/REMOVE	Unloads VShield from memory.

Command-line Option	Description
/REPORT <filename>	Creates a report of infected files and system errors, and saves the data to [filename] in ASCII text file format. * If [filename] already exists, /REPORT will overwrite it. To avoid overwriting, use the /APPEND option with /REPORT: VirusScan will instead add report information to the end of the file, instead of overwriting it. * You can also use /RPTALL, /RPTCOR, /RPTMOD, and /RPTERR to add scanned files, corrupted files, modified files, and system errors to the report. * You can include the destination drive and directory (such as D:\VSREPRT\ALL.TXT), but if the destination is a network drive, you must have rights to create and delete files on that drive.
/RF <filename>	Removes recovery and validation data created by the /AF option. from [filename] * If filename resides on a shared network drive, you must be able to delete files on that drive. * Using any of the /AF, /CF, or /RF options together in the same command line returns an error.
/RPTALL	Include all scanned files in the /REPORT file. * When used with /REPORT, this option adds the names of corrupted files to the report file. * You can use /RPTCOR with /RPTMOD and /RPTERR on the same command line.

Command-line Option	Description
/RPTCOR	Include corrupted files in /REPORT file. * When used with /REPORT, this option adds the names of corrupted files to the report file. Corrupted files which VirusScan finds may have been damaged by a virus. * You can use /RPTCOR with /RPTMOD and /RPTERR on the same command line. * There may be false readings in some files that require an overlay or another executable to run properly (that is, a file that is not executable on its own).
/RPTERR	Include errors in /REPORT file. * When used with /REPORT, this option adds a list of system errors to the report file. * System errors can include problems reading or writing to a diskette or hard disk, file system or network problems, problems creating reports, and other system-related problems. * You can use /RPTERR with /RPTCOR and /RPTMOD on the same command line.
/RPTMOD	Include modified files in /REPORT file. * When used with /REPORT, this option adds a list of modified files to the report file. * VirusScan defines a modified file as one including unmatching validation codes (using the /CF or /CV options). * You can use /RPTMOD with /RPTCOR and /RPTERR on the same command line.

Command-line Option	Description
/RV	Removes validation and recovery data from files validated with the /AV option. * To update files on a shared network drive, you must have access rights to update them. * Using any of the /AV, /CV, or /RV options together in the same command line returns an error.
/SAVE	Saves the command-line options to the VSHIELD.INI file.
/SHOWLOG	Displays the contents of SCAN.LOG. * SCAN.LOG stores the time and date of previous VirusScan activity. You can create a VirusScan log file by using the /LOG option. * The SCAN.LOG file contains text and some special formatting. You may use the /PAUSE option to read the log data one screen at a time.
/SUB	Scans subdirectories inside a directory. * By default, when you specify a directory to scan rather than a drive, VirusScan will examine only the files it contains, not its subdirectories. * Use /SUB to scan all subdirectories within any directories you have specified. * It is not necessary to use /SUB if you are scanning an entire drive.
/SWAP This option not valid for VirusScan Command Line for Windows NT.	Loads VShield kernel (9.2KB) only; swaps the rest to [pathname]

Command-line Option	Description
/VIRLIST	Displays the name and a brief description of each virus that VirusScan detects. * You may use the /PAUSE option to read the virus list one screen at a time. You can use /VIRLIST with /PAUSE on the command line. * You can save the list of virus names and descriptions to a file by redirecting the output of the command. For example, enter: * scan /virlist > filename.txt * Because VirusScan can detect many viruses, this file is more than 250 pages long.
/XMSDATA This option not valid for VirusScan Command Line for Windows NT.	Loads VShield data files into XMS memory.

Index

I

K

L

M

N

P

R