The VSH file is a configuration text file, formatted similarly to the Windows .INI file, which outlines the settings affecting “on-access” scans. (VSH is the acronym for VShield). To view or edit the file, use **Windows Explorer** or **My Computer** to locate **default.vsh** in your VirusScan folder, right-click the filename, and select **Edit**. If the file is password protected, it will be unreadable when opened.

Inside the **default.vsh** file, you will find a list of variables, grouped in sections corresponding to the program modules and features. Not all variables function on all platforms.

- Each variable has a name, preceded by a variable-type code. The variable-type codes used are:

  b Boolean. Possible values are 0 and 1. The 0 value instructs VShield to disable the setting, while 1 indicates that the setting is enabled.

  sz String. Possible value is a series of typed words, and/or other alpha-numeric characters.

  u Integer. Possible values fall within a range of numbers that are pre-defined within the program.

- The variable name is followed by an equals (=) sign which, in turn, is followed by a value.
  - —The values in the **default.vsh** file define the current default VShield configuration settings.
  - —The values shown here are the default VShield configuration settings at the time the product was first installed, before the user made any change to the settings.
- The information here provides brief descriptions, not found in the **default.vsh** file, of the function of each variable. The variables are grouped by program module. In the System Scan, E-mail Scan, Download Scan and Internet Filter sections, the variables are sub-grouped by type of property, (i.e., General Options, Detection Options, Action Options, Alert Options, and Report Options.)
- In addition, information is provided here regarding Security options, Exclusion options and the program’s AVCONSOLE (Scheduler) feature.

Click below to view descriptions of the variables.

{button ,JI(`vscan4.HLP',`System_Scan_Options')} System Scan Options

{button ,JI(`vscan4.HLP',`E_mail_Scan_Options')} E-mail Scan Options

{button ,JI(`vscan4.HLP',`Download_Scan_Options')} Download Scan Options

{button ,JI(`vscan4.HLP',`Internet_Filter_Options')} Internet Filter Options

{button ,JI(`vscan4.HLP',`Security_Exclusion_and_AVCONSOLE_Options')} Security Options, Exclusion Options, and AVCONSOLE

Related Topics

The configuration options for VShield's Security, Exclusion and AVCONSOLE features are described below:

{button ,JI(`vscan4.HLP',`vshSecurityOptions')} Security Options

{button ,JI(`vscan4.HLP',`vshAvconfileOpt')} AVCONFILE

{button ,JI(`vscan4.HLP',`vshExclusionOpt')} Exclusion Options

{button ,JI(`vscan4.HLP',`vshExcludedItems')} Excluded Items

Return to general discussion of VSH Options and Variables

SecurityOptions

Variable	Description
bPasswordEnabled	Type: Boolean (1/0) Defines if password protection is enabled Default value: 0
szPasswordCRC	Reserved. Do not modify
bProtectAllOptions	Type: Boolean (1/0) Defines if all property pages are password protected Default value: 1
szPasswordProtect	Reserved. Do not modify

AVCONFILE

Variable	Description
AVCONFILE	Type: String Specifies the path to AVCONSOLE Default: C:\Program Files\Network Associates\McAfee VirusScan\avconsol.ini
SECTION	Type: String Specifies the reporting location within AVCONSOL.INI Default: Item_0

ExclusionOptions

Variable	Description
szExclusionsFileName	Type: String Default value: C:\Program Files\Network Associates\McAfee VirusScan\VSHLog.TXT

ExcludedItems

Variable	Description
NumExcludedItems	Type: Integer (0-n) Defines the number of items excluded from on-access scanning Default value: 1
ExcludedItem_x, where	Type: String

x is a zero-based index

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 filename.

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

0 - Instructs VShield to not exclude subfolders

The configuration options for VShield's System Scan module are described below:

{button ,JI(`vscan4.HLP',`vshSysScanGeneral')} General Option

{button ,JI(`vscan4.HLP',`vshSysScanDetect')} Detection Options

{button ,JI(`vscan4.HLP',`vshSysScanAction')} Action Options

{button ,JI(`vscan4.HLP',`vshSysScanAlert')} Alert Options

{button ,JI(`vscan4.HLP',`vshSysScanReport')} Report Options

Return to general discussion of VSH Options and Variables

General
(System Scan)

Variable	Description
bEnabled	Type: Boolean (1/0) Enables System Scan 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

DetectionOptions
(System Scan)

Variable	Description
bProgFileHeurisitcs	Type: Boolean (1/0) Instructs VShield to scan program files heuristically Default value: 0
bMacroHeuristics	Type: Boolean (1/0) Instructs VShield to scan macros heuristically Default value: 0
bDetectTrojans	Type: Boolean (1/0) Instructs VShield to scan for Trojan viruses Default value: 1
bDetectJoke	Type: Boolean (1/0) Instructs VShield to scan for Joke viruses Default value: 1
bDetectCorrupted	Type: Boolean (1/0) Instructs VShield to scan for corrupted files Default value: 0
bDetectMaybe	Type: Boolean (1/0)

	Instructs VShield to scan for variants of known viruses Default value: 1
bRemoveAllMacros	Type: Boolean (1/0) Instructs VShield to delete all macros from infected files Default value: 0
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 scan when files are created Default value: 1
bScanOnRename	Type: Boolean (1/0) Instructs VShield to scan when files are renamed Default value: 1
bScanOnShutdown	Type: Boolean (1/0) Instructs VShield to scan the boot record of drive A when system is shut down Default value: 1
bScanOnBootAccess	Type: Boolean (1/0) Instructs VShield to scan the boot record of a diskette that was freshly inserted into in the floppy disk drive just before accessing the drive. Default value: 1
bScanAllFiles	Type: Boolean (1/0) Instructs VShield to scan all files, regardless of their extension. Default value: 0
bScanCompressed	Type: Boolean (1/0) Instructs program to scan compressed files Default value: 1
szProgramExtensions	Type: String Defines the extensions of the files to be scanned Default value: EXE COM DO? XL? MD?, SYS BIN RTF OBD (The ? is a wildcard)
szDefaultProgramExtensions	Type: String Defines extensions to be used as default program extensions during scan configuration Default value: EXE COM DO? XL? MD?, SYS

BIN RTF OBD (The ? is a wildcard)

AlertOptions
(System Scan)

Variable	Description
bDMIAlert	Type: Boolean (1/0) Enables Desktop Management Interface Alerting Default value: 0
bSoundAlert	Type: Boolean (1/0) Enables audible beep when virus is detected Default value: 1
bNetworkAlert	Type: Boolean (1/0) Enables Centralized Alerting Default value: 0
szNetworkAlertPath	Type: String Specifies a server's Centralized Alerting folder Default value: none

ActionOptions
(System Scan)

Variable	Description
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
uVshieldAction	Type: Integer (1-5) Instructs VShield to take the action specified when a virus is detected Possible values: 1 - Prompt user for action 2 - Move infected files automatically 3 - Clean infected files automatically (Deny access if files cannot be cleaned) 4 - Delete infected files automatically 5 - Deny access to infected files and continue 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
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
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: 0
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
szMoveToFolder	Type: String Defines folder to which infected files should be moved Default value: \Infected
szCustomMessage	Type: String Defines custom message to be displayed upon virus detection if action is set to Prompt for Action Default value: None

ReportOptions (System Scan)

Variable	Description
bLogToFile	Type: Boolean (1/0) Defines if results should be logged into log file Default value: 1
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) Instructs VShield to log the names of viruses it detects 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) Instructs VShield to write a record of the settings in use during the scanning session that immediately preceded shutting down your system, or unloading VShield Default value: 1
bLogSummary	Type: Boolean (1/0) Instructs VShield to write a summary of its findings and actions during the scanning session that immediately preceded shutting down your system, or unloading VShield 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
szLogFileName	Type: String Defines log file name Default value: C:\Program Files\Network Associates\McAfee VirusScan\VSHLog.TXT

The configuration options for VShield's E-mail Scan module are described below:

{button ,JI(`vscan4.HLP',`vshEmailGeneral')} General Option

{button ,JI(`vscan4.HLP',`vshEmailDetect')} Detection Options

{button ,JI(`vscan4.HLP',`vshEmailAction')} Action Options

{button ,JI(`vscan4.HLP',`vshEmailAlert')} Alert Options

{button ,JI(`vscan4.HLP',`vshEmailReport')} Report Options

Return to general discussion of VSH Options and Variables

EMailGeneralOptions

Variable	Description
bMailType	Type: Boolean (1/0) Defines e-mail server type, MAPI or cc:Mail. Default value: 1 (MAPI)
bCanBeDisabled	Type: Boolean (1/0) Prevents disabling of e-mail scanning Default value: 1
bEnabled	Type: Boolean (1/0) Enables e-mail scanning Default value: 0
bEnabledDummy=0	Type: Boolean (1/0) Automatically selects Internet Mail on the E-mail Scan property page when Download Scan is enabled Default value: 0

EMailDetectionOptions

Variable	Description
bScanAllMails	Type: Boolean (1/0) Instructs VShield to scan all new mail Default value: 0
bScanInternetMail	Type: Boolean (1/0) Instructs VShield to scan Internet Mail Default value: 0
bScanAllFiles	Type: Boolean (1/0) Instructs VShield to scan all files Default value: 0
bScanCompressed	Type: Boolean (1/0) Instructs VShield to include compressed files in scan Default value: 1
szProgramExtensions	Type: String Defines the extensions of the files to be scanned Default value: EXE, COM, DO?, XL?, RTF, BIN, SYS, OBD, VXD, MD?, DLL (The ? is a wildcard)

szDefaultProgramExtensions	Type: String Defines extensions to be used as default program extensions during scan configuration Default value: EXE, COM, DO?, XL?, RTF, BIN, SYS, OBD, VXD, MD?, DLL (The ? is a wildcard)
uPollInterval	Type: Integer (60-999) Defines interval, in seconds, for checking for new mail received via cc:Mail Default value: 60
bDetectTrojans	Type: Boolean (1/0) Instructs VShield to scan for Trojan viruses Default value: 1
bDetectJoke	Type: Boolean (1/0) Instructs VShield to scan for Joke viruses Default value: 1
bDetectCorrupted	Type: Boolean (1/0) Instructs VShield to scan for corrupted files Default value: 0
bDetectMaybe	Type: Boolean (1/0) Instructs VShield to scan for variants of known viruses Default value: 1
bProgFileHeuristics	Type: Boolean (1/0) Instructs VShield to scan program files heuristically Default value: 0
bMacroHeuristics	Type: Boolean (1/0) Instructs VShield to scan macros heuristically Default value: 0

EMailActionOptions

Variable	Description
szMoveFolder	Type: String Defines folder to which infected MAPI e-mail attachments should be moved Default value: \Infected
CC_szMoveFolder	Type: String Defines folder to which infected cc:Mail e-mail attachments should be moved Default value: \Infected
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
uScanAction	Type: Integer (0/3) Instructs VShield to take the action specified when

	a virus is detected Possible values: 0 - Prompt user for action 1 - Move infected files automatically 2 - Delete infected files automatically 3 – Continue Scanning
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: 0
bButtonMove	Type: Boolean (1/0) Instructs VirusScan to give user option of moving 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
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: 0

EMailAlertOptions

Variable	**Description**
bDMIAlert	Type: Boolean (1/0) Enables Desktop Management Interface Alerting Default value: 0
bNetworkAlert	Type: Boolean (1/0) Enables Centralized Alerting Default value: 0
szNetworkAlertPath	Type: String Specifies a server's Centralized Alerting folder Default value: none
bSoundAlert	Type: Boolean (1/0) Enables audible beep when virus is detected Default value: 1
szCustomMessage	Type: String Defines custom message to be displayed upon

	virus detection if action is set to Prompt for Action Default value: McAfee VShield: Virus found in attachment!
bReturnMail	Type: Boolean (1/0) Instructs VShield to notify sender of infected e-mail that was received via a MAPI client Default value: 0
szReturnCc	Type: String Identifies recipient(s) of copy of notification to sender of infected e-mail that was received via a MAPI client Default value: none
szReturnSubject	Type: String Allows insertion of Subject text for notification to sender of infected e-mail that was received via a MAPI client Default value: none
szReturnBody	Type: String Allows inclusion of message text in notification to sender of infected e-mail that was received via a MAPI client Default value: none
bSendMailToUser	Type: Boolean (1/0) Instructs VShield to notify other users of infected e-mail that was received via a MAPI client Default value: 0
szSendTo	Type: String Identifies other users who should receive notification of infected e-mail that was received via a MAPI client Default value: none
szSendCc	Type: String Identifies people who should receive copies of the notification to other users about infected e-mail that was received via a MAPI client Default value: none
szSendSubject	Type: String Allows insertion of Subject text for notification to others of infected e-mail that was received via a MAPI client Default value: none
szSendBody	Type: String Allows inclusion of message text in notification to others of infected e-mail that was received via a MAPI client Default value: none
CC_bReturnMail	Type: Boolean (1/0) Instructs VShield to notify sender of infected e-mail that was received via cc:Mail Default value: 0

CC_bSendMailToUser	Type: Boolean (1/0) Instructs VShield to notify other users of infected e-mail that was received via cc:Mail Default value: 0
CC_szReturnCc	Type: String Identifies recipient(s) of copy of notification to sender of infected e-mail that was received via cc:Mail Default value: none
CC_szReturnSubject	Type: String Allows insertion of Subject text for notification to sender of infected e-mail that was received via cc:Mail Default value: none
CC_szReturnBody	Type: String Allows inclusion of message text in notification to sender of infected e-mail that was received via cc:Mail Default value: none
CC_szSendTo	Type: String Identifies other users who should receive notification of infected e-mail that was received via cc:Mail Default value: none
CC_szSendCc	Type: String Identifies people who should receive copies of the notification to other users about infected e-mail that was received via cc:Mail Default value: none
CC_szSendSubject	Type: String Allows insertion of Subject text for notification to others of infected e-mail that was received via cc:Mail Default value: none
CC_szSendBody	Type: String Allows inclusion of message text in notification to others of infected e-mail that was received via cc:Mail Default value: none

EMailReportOptions

Variable	**Description**
bLogToFile	Type: Boolean (1/0) Defines if scan results should be logged into log file Default value: 1
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) Instructs VShield to log the names of viruses it detects 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) Instructs VShield to write a record of the settings in use during the scanning session that immediately preceded shutting down your system, or unloading VShield Default value: 1
bLogSummary	Type: Boolean (1/0) Instructs VShield to write a summary of its findings and actions during the scanning session that immediately preceded shutting down your system, or unloading VShield 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
szLogFileName	Type: String Defines log file name Default value: C:\Program Files\Network Associates\McAfee VirusScan\WebEmail.txt

The configuration options for VShield's Download Scan module are described below:

{button ,JI(`vscan4.HLP',`vshDownloadGeneral')} General Option

{button ,JI(`vscan4.HLP',`vshDownloadDetect')} Detection Options

{button ,JI(`vscan4.HLP',`vshDownloadAction')} Action Options

{button ,JI(`vscan4.HLP',`vshDownloadAlert')} Alert Options

{button ,JI(`vscan4.HLP',`vshDownloadReport')} Report Options

Return to general discussion of VSH Options and Variables

DownloadGeneralOptions

Variable	Description
bEnabled	Type: Boolean (1/0) Enables scanning of downloaded files Default value: 1
bCanBeDisabled	Type: Boolean (1/0) Prevents disabling the scanning of downloaded files Default value: 1

DownloadDetectionOptions

Variable	Description
bScanAllFiles	Type: Boolean (1/0) Instructs VShield to scan all files Default value: 0
bScanCompressed	Type: Boolean (1/0) Instructs VShield to include compressed files in scan Default value: 1
bDetectTrojans	Type: Boolean (1/0) Instructs VShield to scan for Trojan viruses Default value: 1
bDetectJoke	Type: Boolean (1/0) Instructs VShield to scan for Joke viruses Default value: 1
bDetectCorrupted	Type: Boolean (1/0) Instructs VShield to scan for corrupted files Default value: 0
bDetectMaybe	Type: Boolean (1/0) Instructs VShield to scan for variants of known viruses Default value: 1
bProgFileHeuristics	Type: Boolean (1/0) Instructs VShield to scan program files heuristically Default value: 0
bMacroHeuristics	Type: Boolean (1/0)

	Instructs VShield to scan macros heuristically Default value: 0
szProgramExtensions	Type: String Defines the extensions of the files to be scanned Default value: EXE, COM, DO?, XL?, RTF, BIN, SYS, OBD, VXD, MD?, DLL (The ? is a wildcard)

DownloadActionOptions

Variable	**Description**
szMoveToFolder	Type: String Defines folder to which infected files should be moved Default value: \Infected
szCustomMessage	Type: String Defines custom message to be displayed upon virus detection if action is set to Prompt for Action Default value: McAfee VShield: Virus found in download file!
uScanAction	Type: Integer (0/3) Instructs VShield to take the action specified when a virus is detected Default value: 0 Possible values: 0 - Prompt user for action 1 - Move infected files automatically 2 - Delete infected files automatically 3 – Continue Scanning
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
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: 0
bButtonMove	Type: Boolean (1/0) Instructs VirusScan to give user option of moving 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
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: 0

DownloadAlertOptions

Variable	Description
bDMIAlert	Type: Boolean (1/0) Enables Desktop Management Interface Alerting Default value: 0
bNetworkAlert	Type: Boolean (1/0) Enables Centralized Alerting Default value: 0
szNetworkAlertPath	Type: String Specifies a server's Centralized Alerting folder Default value: none
bSoundAlert	Type: Boolean (1/0) Enables audible beep when 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 detection of a hostile ActiveX control or Java applet, or an attempt to connect to a banned URL or IP address. Default value: 0

DownloadReportOptions

Variable	Description
bLogToFile	Type: Boolean (1/0) Defines if scan results should be logged into log file Default value: 1
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) Instructs VShield to log hostile ActiveX control or Java applet it encounters, or attempts to connect to a banned URL or IP address. 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) Instructs VShield to write a record of the settings in use during the scanning session that immediately preceded shutting down your system, or unloading VShield Default value: 1
bLogSummary	Type: Boolean (1/0) Instructs VShield to write a summary of its findings and actions during the scanning session that immediately preceded shutting down your system, or unloading VShield 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
szLogFileName	Type: String Defines log file name Default value: C:\Program Files\Network Associates\McAfee VirusScan\WebInet.txt

The configuration options for VShield's Download Scan module are described below:

{button ,JI(`vscan4.HLP',`vshFilterGeneral')} General Option

{button ,JI(`vscan4.HLP',`vshFilterDetect')} Detection Options

{button ,JI(`vscan4.HLP',`vshFilterAction')} Action Options

{button ,JI(`vscan4.HLP',`vshFilterAlert')} Alert Options

{button ,JI(`vscan4.HLP',`vshFilterReport')} Report Options

Return to general discussion of VSH Options and Variables

INetFltrGeneralOptions

Variable	Description
bEnabled	Type: Boolean (1/0) Enables scanning of downloaded files Default value: 1
bCanBeDisabled	Type: Boolean (1/0) Prevents disabling the scanning of downloaded files Default value: 1

INetFltrDetectionOptions

Variable	Description
bScanIP	Type: Boolean (1/0) Instructs VShield to block designated IP addresses Default value: 1
bScanHost	Type: Boolean (1/0) Instructs VShield to block designated URLs Default value: 1
bScanJava	Type: Boolean (1/0) Instructs VShield to scan for potentially harmful Java applets Default value: 1
bScanActiveX	Type: Boolean (1/0) Instructs VShield to scan for potentially harmful ActiveX objects Default value: 1
bDetectTrojans	Type: Boolean (1/0) Instructs VShield to scan for Trojan viruses Default value: 1
bDetectJoke	Type: Boolean (1/0) Instructs VShield to scan for Joke viruses Default value: 1
bDetectCorrupted	Type: Boolean (1/0) Instructs VShield to scan for corrupted files Default value: 0
bDetectMaybe	Type: Boolean (1/0)

	Instructs VShield to scan for variants of known viruses Default value: 1
bProgFileHeuristics	Type: Boolean (1/0) Instructs VShield to scan program files heuristically Default value: 0
bMacroHeuristics	Type: Boolean (1/0) Instructs VShield to scan macros heuristically Default value: 0

INetFltrActionOptions

Variable	**Description**
uScanAction	Type: Integer (0/1) Instructs VShield to take the action specified when a banned URL, IP address, ActiveX control, or Java applet is detected Default value: 0 Possible values: 0 - Prompt user for action 1 – Deny Access to objects

INetFltrAlertOptions

Variable	**Description**
bDMIAlert	Type: Boolean (1/0) Enables Desktop Management Interface Alerting Default value: 0
bNetworkAlert	Type: Boolean (1/0) Enables Centralized Alerting Default value: 0
szNetworkAlertPath	Type: String Specifies a server's Centralized Alerting folder Default value: none
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
bSoundAlert	Type: Boolean (1/0) Enables audible beep when a banned URL, IP address, ActiveX control, or Java applet is detected Default value: 1
szCustomMessage	Type: String If action is set to Prompt for Action, this variable defines custom message to be displayed when a banned URL, IP address, ActiveX control, or Java applet is detected Default value: McAfee VShield: Hostile internet object or banned site detected!

InetFltrReportOptions

Variable	Description
bButtonDeny	Type: Boolean (1/0) Instructs VShield to give user option of denying access to the site where the potentially dangerous object was 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 banned URL, IP address, ActiveX control, or Java applet is detected Default value: 1
bLogToFile	Type: Boolean (1/0) Defines if scan results should be logged into log file Default value: 1
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) Instructs VShield to log the names of viruses it detects Default value: 1
bLogSettings	Type: Boolean (1/0) Instructs VShield to write a record of the settings in use during the scanning session that immediately preceded shutting down your system, or unloading VShield Default value: 1
bLogSummary	Type: Boolean (1/0) Instructs VShield to write a summary of its findings and actions during the scanning session that immediately preceded shutting down your system, or unloading VShield 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
szLogFileName	Type: String Defines log file name Default value: C:\Program Files\Network

Associates\McAfee VirusScan\WebFiltr.txt

The VSC file is a configuration text file, formatted similarly to the Windows .INI file, which outlines the settings affecting “on-demand” scans. (VSC is the acronym for VirusScan). To view, or edit the file, use **Windows Explorer** or **My Computer** to locate **default.vsc** in your VirusScan folder, right-click the filename, and select **Edit**.

Inside the **default.vsc** file, you will find a list of variables, grouped in sections corresponding to the configuration properties. Not all variables function on all platforms.

- Each variable has a name, preceded by a variable-type code. The variable-type codes used are:

b	Boolean. Possible values are 0 and 1. The 0 value instructs VirusScan to disable the setting, while 1 indicates that the setting is enabled.
sz	String. Possible value is a series of typed words, and/or other alpha-numeric characters.
u or **n**	Integer. Possible values fall within a range of numbers that are pre-defined within the program.

- The variable name is followed by an equals (=) sign, which, in turn, is followed by a value.
  - —The values in the **default.vsc** file define the current default VirusScan configuration settings.
  - —The values shown here are the default VirusScan configuration settings at the time the product was first installed, before the user made any change to the settings.
- The information here also provides brief descriptions, not found in the **default.vsc** file, of the function of each variable. The variables are grouped by configuration property. Click below to view descriptions of the variables.

{button ,JI(`vscan4.HLP',`vscScanItems')} Scan Options
{button ,JI(`vscan4.HLP',`vscDetectionOptions')} Detection Options
{button ,JI(`vscan4.HLP',`vscActionOptions')} Action Options

{button ,JI(`vscan4.HLP',`vscAlertOptions')} Alert Options

{button ,JI(`vscan4.HLP',`vscReportOptions')} Report Options

{button ,JI(`vscan4.HLP',`vscSecurityOptions')} Security Options

{button ,JI(`vscan4.HLP',`vscScanItems')} Scan Items

{button ,JI(`vscan4.HLP',`vscExcludedItems')} Excluded items

ScanOptions

Variable	**Description**
UIType	Type: Boolean (1/0) Specifies which interface is displayed—VirusScan for Windows NT or VirusScan for Windows 95/98. Modifying default results in alternative interface Default value: 0 (Windows 95/98)
bAutoStart	Type: Boolean (1/0) Instructs VirusScan to start scanning immediately as it is launched. If you are using the Windows NT interface, the program starts automatically, regardless of this variable’s setting. Default value: 0
bAutoExit	Type: Boolean (1/0) Instructs VirusScan to exit upon scan completion if no viruses are found Default value: 0
bAlwaysExit	Type: Boolean (1/0) Instructs VirusScan to always exit upon scan completion Default value: 0

bSkipMemoryScan	Type: Boolean (1/0) Instructs VirusScan to skip memory scan Default value: 0
bSkipBootScan	Type: Boolean (1/0) Instructs VirusScan to skip boot sector scanning Default value: 0
bSkipSplash	Type: Boolean (1/0) Instructs VirusScan to not display the initial splash screen when the application is launched Default value: 0
nPriority	Type: Integer (0-5) Specifies the scanning threads priority Possible values: 0 - Normal (default) thread priority 1 - Lowest thread priority 2 - Below normal thread priority 3 - Normal thread priority 4 - Above normal thread priority 5 - Highest thread priority Default value: 0
nChecksum	Reserved. Do not modify
bConfigurableGuiMode	Type: Boolean (1/0) Instructs VirusScan to use the Advanced user interface Default value: 0
szTaskName	Reserved. Do not modify

DetectionOptions

Variable	**Description**
bScanAllFiles	Type: Boolean (1/0) Instructs VirusScan to scan inside all files Default value: 0
bScanCompressed	Type: Boolean (1/0) Instructs VirusScan to scan compressed files Default value: 1
szProgramExtensions	Type: String Defines the extensions of the files to be scanned Default value: Default value: EXE, COM, DO?, XL?, MD?, VXD, SYS, BIN, RTF, OBD, DLL. (The ? is a wildcard)
szDefaultProgramExtensions	Type: String Defines extensions to be used as default program extensions during scan configuration Default value: EXE, COM, DO?, XL?, MD?, VXD, SYS, BIN, RTF, OBD, DLL. (The ? is a wildcard)
bRemoveAllMacros	Type: Boolean (1/0)

	Instructs VirusScan to delete all macros from infected files Default value: 0
bProgFileHeurisitcs	Type: Boolean (1/0) Instructs VirusScan to scan program files heuristically Default value: 0
bMacroHeuristics	Type: Boolean (1/0) Instructs VirusScan to scan macros heuristically Default value: 0
bDetectTrojans	Type: Boolean (1/0) Instructs VirusScan to scan for Trojan viruses Default value: 1
bDetectJoke	Type: Boolean (1/0) Instructs VirusScan to scan for Joke viruses Default value: 1
bDetectCorrupted	Type: Boolean (1/0) Instructs VirusScan to scan for corrupted files Default value: 0
bDetectMaybe	Type: Boolean (1/0) Instructs VirusScan to scan for variants of known viruses Default value: 1

AlertOptions

Variable	**Description**
bNetworkAlert	Type: Boolean (1/0) Enables Centralized Alerting Default value: 0
bSoundAlert	Type: Boolean (1/0) Instructs VirusScan to sound an alert when a virus is detected Default value: 1
szNetworkAlertPath	Type: String Specifies a server's Centralized Alerting folder Default value: none

ActionOptions

Variable	**Description**
bDisplayMessage	Type: Boolean (1/0) Defines if custom message should be displayed upon virus detection Default value: 0
uScanAction	Type: Integer (1-5) Instructs VirusScan to take the action specified when

	a virus is detected Possible values: 0 - Prompt user for action 1 - Move infected files automatically 2 - Clean infected files automatically 3 - Delete infected files automatically 4 - Continue scanning Default value: 0
bButtonClean	Type: Boolean (1/0) Instructs VirusScan to give user option of cleaning the file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonDelete	Type: Boolean (1/0) Instructs VirusScan to give user option of deleting the file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonExclude	Type: Boolean (1/0) Instructs VirusScan to give user option of excluding the file if Prompt for Action is selected and a virus is detected Default value: 0
bButtonMove	Type: Boolean (1/0) Instructs VirusScan to give user option of moving the infected file if Prompt for Action is selected and a virus is detected Default value: 1
bButtonContinue	Type: Boolean (1/0) Instructs VirusScan to give user option of continuing the scan if Prompt for Action is selected and a virus is detected Default value: 1
bButtonStop	Type: Boolean (1/0) Instructs VirusScan 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
szMoveToFolder	Type: String Defines folder to which infected files should be moved Default value: \Infected
szCustomMessage	Type: String Defines custom message to be displayed upon virus detection Default value: Possible Virus Detected

ReportOptions

Variable	**Description**
bLogToFile	Type: Boolean (1/0)

	Defines if scan results should be logged into log file Default value: 1
bLimitSize	Type: Boolean (1/0) Defines if size of the log file should be limited Default value: 1
uMaxKilobytes	Type: Integer Defines maximum size of the log file in kilobytes Default value: 100
bLogDetection	Type: Boolean (1/0) Instructs VirusScan to log the names of viruses it detects Default value: 1
bLogClean	Type: Boolean (1/0) Defines if clean results should be logged Default value: 1
bLogDelete	Type: Boolean (1/0) Defines if 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) Instructs VirusScan to write a record of the settings in use during the scanning session that just concluded Default value: 1
bLogSummary	Type: Boolean (1/0) Instructs VirusScan to write a summary of its findings and actions during the scanning session that just concluded Default value: 1
bLogDateTime	Type: Boolean (1/0) Defines if date and time of an event should be logged Default value: 1
bLogUserName	Type: Boolean (1/0) Defines if user name should be logged Default value: 1
szLogFileName	Type: String Defines log file name Default value: C:\Program Files\Network Associates\McAfee VirusScan\VSCLog. TXT

ScanItems

Variable	**Description**

NumScanItems	Type: Integer (0-n) Defines the number of items to scan Default value: 1
szScanItem_x	Type: String Default value: C:\ Instructs VirusScan to scan the item The string is separated into fields using the pipe (|) character: Field 1 - Folder portion of item to scan. Leave blank for a single file anywhere on the system Field 2 - File portion of the item to scan. Leave blank if a folder is scanned without a filename Field 3 - Integer (1-3) Possible values: 1 - Scans file 2 - Scans boot-record 3 - Scans from both boot-record and file Field 4 - Boolean (1/0) Possible values: 1 - Instructs VirusScan to scan subfolders of the item 0 - Instructs VirusScan to not scan subfolders of the item

SecurityOptions

Variable	**Description**
szPasswordProtect	Type: Boolean (1/0) Defines if password protection is enabled Default value: 0
szPasswordCRC	Reserved. Do not modify

ExcludedItems

Variable	**Description**
NumExcludeItems	Type: Integer (0-n) Defines the number of items excluded from on-demand scanning Default value: 1
ExcludedItem_x, where x is a zero-based index	Type: String Instructs VirusScan 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 filename

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 VirusScan to exclude subfolders of the excluded item

0 - Instructs VirusScan to not exclude subfolders

Related Topics

The following table lists all options available when running VirusScan from the DOS command-line. These options can be used to configure both on-demand and on-access scans, unless otherwise noted.

When typing commands, remember that if you name a file which resides outside the directory where VirusScan is installed, you must include the full path to that file.

Command-line Option	Limitations	Description
/? or /HELP	None.	Displays a list of VirusScan command-line options, each with a brief description.
/ADL	On-demand scanning only.	Scan all local drives—including compressed drives and PC cards, but not disks—in addition to any other drive specified on the command-line. To scan both local and network drives, use the /ADL and /ADN commands together in the same command-line. OS/2: /ADL includes the CD-ROM drive in the scan, when used with /NODDA
/ADN	On-demand scanning only.	Scan all network drives—including CD-ROM—for viruses, in addition to any other drive(s) specified on the command-line. To scan both local drives and network drives, use the /ADL and /ADN commands together in the same command-line.
/ALERTPATH <*dir*>	On-demand scanning only.	Designates the directory <dir> as a network path monitored by Centralized Alerting.
/ALL	On-demand scanning only.	Overrides the default scan setting by scanning all infectable files—regardless of extension. Using the /ALL option substantially increases the scanning time required. Use it only if you find a virus or suspect that 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.
/ANALYZE	On-demand scanning only. Extended memory required.	Sets VirusScan to scan using its full heuristics, both program and macro. /MANALYZE targets macro viruses only. /PANALYZE targets program viruses only.
/ANYACCESS	On-access scanning only.	Scans: § the boot sector whenever a disk is either read or written to § executables § any newly created files.
/APPEND	On-demand scanning only.	Used with /REPORT to append report message text to the specified report file instead of overwriting it.
/BOOT	On-demand scanning only.	Scan boot sector and master boot record only.
/BOOTACCESS	On-access	Scans a disk's boot sector for viruses whenever the disk is

	scanning only.	accessed (including read/write operations).
/CLEAN	On-demand scanning only.	Clean viruses from all infected files and system areas.
/CLEANDOCALL	On-demand scanning only.	As a precautionary measure against macro viruses, /CLEANDOCALL cleans all macros from Microsoft Word and Office documents. This option deletes all macros, including macros not infected by a virus.
/CONTACT <*message*>	On-access scanning only.	Displays specified message when a virus is detected. This message cannot exceed 255 characters.
/CONTACTFILE <*filename*>	None.	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. 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.
/DEL	On-demand scanning only.	Deletes infected files permanently.
/EXCLUDE <*filename*>	On-demand scanning only.	Do not scan or add validation codes to the files listed in <*filename*>. Use this option to exclude specific files from a scan. List the complete path to each file that you want to exclude on its own line. You may use wildcards * and ?
/FILEACCESS	On-access scanning only.	Scans executable files on accessed as well as execution. This scan will not check the boot sector.
/FREQUENCY <*n* >	On-demand scanning only.	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 /?	None.	Displays a list of VirusScan command-line options, each with a brief description.
/IGNORE <*drive(s)*>	On-access scanning only.	Does not check any files loaded from the specified drive(s).
/LOAD <*filename*>	On-demand scanning only.	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.
/LOCK	Not available in low-memory environments	With this /LOCK option enabled, VirusScan will halt and lock your system if it finds a virus. /LOCK is appropriate in highly vulnerable network

		environments, such as open-use computer labs. Network Associates recommends using /LOCK with the /CONTACTFILE option to tell users what to do or whom to contact if VirusScan locks the system.
/MANALYZE	On-demand scanning only. Extended memory required.	Sets VirusScan's heuristic scanning features to target macro viruses only. /PANALYZE targets program viruses only. /ANALYZE targets both program and macro viruses.
/MANY	On-demand scanning only.	Scans multiple disks consecutively in a single drive. VirusScan will prompt you for each disk. Use this option to check multiple floppy disks quickly. You cannot use the /MANY option if you run VirusScan from a boot disk and you have only one floppy drive.
/MAXFILESIZE <*xxx.x*>	On-demand scanning only.	Scan only files no larger than <xxx.x> megabytes.
/MEMEXCL	On-demand scanning only. Not available for Windows	Excludes the memory address A0000:0000 from scanning.
/MOVE <*dir*> or *.???	On-demand scanning only.	/MOVE <directory>: Moves all infected files found during a scan to the specified directory, preserving drive letter and directory structure. 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	On-demand scanning only.	Disables the tone that sounds whenever VirusScan finds a virus.
/NOBREAK	On-demand scanning only.	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	On-demand scanning only. Extended memory required.	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 checking for virus signatures. VirusScan will still check for modifications to compressed executables if they contain VirusScan validation codes.
/NODDA	On-demand scanning only.	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	On-access scanning only.	Does not scan boot sector while loading VShield.
/NODOC	On-demand scanning only.	Does not scan Microsoft Office files.
/NOEMS	On-access scanning only.	Keeps VShield from using extended memory (XMS).
/NOEXPIRE	On-demand scanning only.	Disables the “expiration date” message if the VirusScan data files are out of date.
/NOMEM	None.	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	On-access scanning only.	Prevents VShield from being removed from memory with the /REMOVE switch
/NOWARMBOOT	On-access scanning only.	Does not check the disk boot sector of the floppy disk in drive A for viruses during warm boot (system reset or CTRL+ALT+DEL).
/NOXMS	On-access scanning only.	Does not use extended memory (XMS).
/ONLY <*drive(s)*>	On-access scanning only.	Checks only files loaded from the specified drive(s).
/PANALYZE	On-demand scanning only. Extended memory required.	Sets VirusScan to scan using program heuristics. /MANALYZE targets macro viruses only; /ANALYZE targets both program and macro viruses.
/PAUSE	On-demand scanning only.	Enables screen pause. The “Press any key to continue” prompt will appear when VirusScan fills a screen with messages. 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. Network Associates recommends omitting /PAUSE when using the report options (/REPORT, /RPTCOR, and /RPTERR)
/PLAD	On-demand scanning only.	Preserves the 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
/RECONNECT	On-access scanning only.	Restores VShield after it has been disabled by certain drivers or memory-resident programs.
/REMOVE	On-access scanning only.	Unloads VShield from memory.
/REPORT <*filename*>	On-demand scanning only.	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, 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. Network Associates recommends omitting /PAUSE when using any report option.
/RPTALL	On-demand scanning only.	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 /RPTERR on the same command-line. Network Associates recommends omitting /PAUSE when using any report option.
/RPTCOR	On-demand scanning only.	Include corrupted files in /REPORT file. When used with /REPORT, this option adds the names of corrupted files to the report file. Corrupted files that VirusScan finds may have been damaged by a virus. You can use /RPTCOR with /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). Network Associates recommends omitting /PAUSE when using any report option.
/RPTERR	On-demand scanning only.	Include errors in /REPORT file. When used with /REPORT, this option adds a list of system errors to the report file. /LOCK is appropriate in highly vulnerable network environments, such as open-use computer labs. You can use /RPTERR with /RPTCOR on the same command-line. System errors can include problems reading or writing to a disk or hard disk, file system or network problems, problems creating reports, and other system-related problems.

		Network Associates recommends omitting /PAUSE when using any report option.
/SAVE	On-access scanning only.	Saves the command-line options to the VSHIELD.INI file.
/SUB	On-demand scanning only.	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.
/UNZIP	On-demand scanning only. Extended memory required.	Scan inside compressed files.
/VIRLIST	On-demand scanning only.	Displays the name and a brief description of each virus that VirusScan detects. You may use the /PAUSE option on the same command-line as /VIRLIST to read the virus list one screen at a time. To redirect the /VIRLIST output to a text file: At the command prompt, type `scan /VIRLIST> filename.txt` Because VirusScan can detect many viruses, this file will be over 250 pages long. This is too large for the MS-DOS “Edit” program to open; Network Associates recommends using Notepad or another text editor to open the virus list.
/XMSDATA	On-access scanning only.	Loads VShield data files into XMS memory.

Related Topics

When you run VirusScan in the DOS environment, a DOS 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 operating system documentation for more information.

VirusScan can return the following error levels:

Error Level	Description
0	No errors occurred; no viruses were found.
2	Driver integrity check failed.
6	A general problem.
8	Could not find a driver.
10	A virus was found in memory.
13	One or more viruses or hostile objects were found.
15	VirusScan self-check failed; it may be infected or damaged.
20	Scanning prevented due to the /FREQUENCY switch.
102	User quit via ESC-X, ^C or Exit button. This can be disabled with the /NOBREAK command-line option.

Related Topics

The ALR file is the Centralized Alerting text that contains virus event variables. Each variable in the file has a name followed by the equal (=) sign and a value. The following is a line-by-line description of the Centralized Alerting (ALR) file format:

[CentralAlert]	Centralized Alerting identifier
uFileVersion	Type: Integer
	Centralized Alerting version number
uStatus	Reserved
szVirusName	Type: String
	The name of the virus.
szItemName	Type: String
	The infected file name and path.
szUserName	Type: String
	The user name.
szSoftware	Type: String
	The name of the Network Associates virus application installed on the reporting machine.
szSoftwareVersion	Type: String
	The version of the virus application.
szComputerName	Type: String
	The name of the machine reporting the event.
uYear	Type: Integer (0000-9999)
	The year of the event.
uMonth	Type: Integer (1-12)
	The month of the event.
uDay	Type: Integer (1-31)
	The day of the event.
uHour	Type: Integer (0-23)
	The hour of the event.
uMinute	Type: Integer (0-59)
	The minute of the event.
uSecond	Type: Integer (0-59)
	The second of the event.

Related Topics

The following options are for use with VirusScan for Windows 95 and Windows 98, not with VirusScan for DOS. These options can be used as command-line parameters with shortcuts and icons to control the state of VirusScan when it is launched:

- **/NoSplash:** Suppresses the VirusScan splash screen
- **/AutoScan:** Starts scanning automatically

Related Topics

A computer virus is a program that replicates itself, attaches to other programs, and performs unsolicited or unwanted, if not malicious, actions when it executes. The two fundamental virus categories are “boot” and “file” viruses.

Boot viruses dwell in the boot sector of the hard or floppy disk that carries them. These execute as your computer starts. Once they copy themselves into your computer’s memory, they can then spread to other disks or other computers on a network, each time leaving copies of themselves that can repeat the cycle.

File viruses become active only when you execute the program that carries them. Typically, such viruses infect files with the extensions .EXE, .COM, or .DLL, and non-executable files such as Microsoft Word or Excel data and template files. Once executed, the file virus also loads itself into your computer’s memory, then replicates and attaches itself to other executable programs.

The following list describes some of the characteristics of common viruses. Click an item to learn more.

{button ,PI(`vscan4.hlp',`Boot_Virus')} Boot virus
{button ,PI(`vscan4.hlp',`File_virus')} File virus
{button ,PI(`vscan4.hlp',`Stealth_virus')} Stealth virus
{button ,PI(`vscan4.hlp',`Multi_partite_virus')} Multi-partite virus
{button ,PI(`vscan4.hlp',`Mutating_virus')} Mutating virus
{button ,PI(`vscan4.hlp',`Encrypted_virus')} Encrypted virus
{button ,PI(`vscan4.hlp',`Polymorphic_virus')} Polymorphic virus
{button ,PI(`vscan4.hlp',`Macro_Virus')} Macro virus

Related Topics

As the popularity of the Internet has grown in the last few years, website design has become much more sophisticated. Many sites now include interactive elements such as forms, search engines, animations, and a host of other multimedia features that make web browsing more useful and more exciting. Much of the technology that makes these features possible comes from small, easily downloaded programs that interact with your browser software to exchange information, to display multimedia files, to formulate database queries, and to perform other tasks. Java and ActiveX are tools programmers use to write these types of programs.

Programmers use Sun Microsystems' Java programming language to write small, special-purpose applications, or "applets," that run on a Java "virtual machine" incorporated into your browser software, either directly or as a plug-in module. A Java "class" is a prewritten software module that programmers can modify for their own use.

Programmers use Microsoft's ActiveX technology for similar purposes. ActiveX differs from Java primarily in how it runs—where Java runs in a virtual machine built specifically to interpret Java applets, ActiveX serves as a sophisticated software bridge between existing programs, or between other programs and Windows itself. An ActiveX "control" is a software module that links programs and allows them to share data without either having to know anything about how the other operates.

Java classes and ActiveX controls are called, collectively, "objects."

Related Topics

Not so long ago, individual computer users could avoid virus infections without much thought or planning, simply because they rarely came in contact with likely virus sources. Today, however, most computer users send messages to each other, share data and transfer files constantly—whether through a modem, via diskettes, or over networks and the Internet. In this same span of time, viruses have come to number in the thousands and spread more quickly and easily than ever.

In this environment, taking steps to protect yourself from a computer virus infection is no longer a luxury but a necessity. Consider the value of the data on your computer. It would probably require a significant investment of time and money to replace if it became corrupted or unusable because of a viral infection—it may even be irreplaceable. But whether your own data is important to you or not, neglecting to guard against viruses may mean that your computer could play unwitting host to a virus that can spread and attack the data on computers your co-workers and colleagues use.

Scheduling periodic virus scans with VirusScan for Windows 95 and Windows 98 and other Network Associates virus-scanning solutions significantly reduces your vulnerability to infection and prevents unnecessary loss of time, money and data.

Related Topics

Both ActiveX and Java include safeguards designed to prevent harm to your computer system. Nevertheless, determined programmers have developed objects that use Java or ActiveX to read data on your hard disk; pass it back to websites you visit; compose and send offensive e-mail in your name; corrupt or destroy your data; or cause other damage to your system.

Dangerous objects such as these can often lurk on websites until you visit and download them to your system, usually without realizing that they exist. Most browser software includes a feature that allows you to block ActiveX controls or Java applets altogether; or to turn on security features that authenticate objects before downloading them to your system. However, these approaches can deprive you of the interactive benefits of websites you visit by indiscriminately blocking all objects, dangerous or not.

VirusScan for Windows 95 and Windows 98 allows a more judicious approach. It uses an up-to-date database of objects known to cause harm to screen ActiveX controls and Java classes you encounter as you browse. Potentially harmful objects stay where they are, away from your system, while other objects continue to function.

Related Topics

VirusScan for Windows 95 and Windows 98 consists of a Launcher screen that provides access to the program's three major components: VirusScan, VShield, and Scheduler, as well as its three utility tools: Submit to McAfee, Emergency Disk and Virus Info. The functions of each are described below, in general terms, with links to more detailed topics. Typical users will not need to refer to the executable (.exe) files that run or control configuration of each component. The information is provided here for clarification and reference.

Component	Function	Action
VirusScan Central Launcher (VScan40.exe)	Launch program components and utilities.	Provides access to program components: § Opens VirusScan, VShield, Scheduler and Toolbox. § Displays useful information about the status and configuration of the program's elements. {button ,JI(`vscan4.HLP>First',`The_Launcher_Screen')} Click to view **Launcher**
VirusScan (scan32.exe)	On-demand scans of files and disks. For information about on-demand E-mail scanning, see Perform an On-Demand E-mail Scan.	Scans whenever you want: § any set of files on a local or network drive. § boot records, boot sectors, and system files viruses automatically when you turn on or reset your PC. {button ,JI(`vscan4.HLP>First',`The_Virus_Scan_User_Interface')} Click to view **Virus Scan** interface
VShield (vsconfig.exe)	On-access scans	Automatically scans when you: § run, create; copy or rename a file on a local or network drive. § access floppy disks or shut down your system while a diskette is in the floppy disk drive. § receive an e-mail message that includes an attachment. (See Perform an On-Demand E-mail Scan for information about *on-demand* scanning of e-mail.) § download a file from the Internet § visit web pages that have Java or ActiveX objects. {button ,JI(`vscan4.HLP>First',`The_VShield_User_Interface')} Click to view **VShield** interface
VirusScan Scheduler (avconsol.exe)	On-schedule scans	Scans local or network drives automatically, based on a schedule you define. {button ,JI(`vscan4.HLP>First',`The_Scheduler_User_Interface')} Click to view **Scheduler** interface
Submit to McAfee (SendVir.exe)	Submit new or unidentified viruses for analysis	If you have found what you suspect to be a new or unidentified virus, send the infected file to McAfee Labs Anti-Virus Emergency Response Team for analysis
Emergency Disk	Make an	Creates a disk that scans your system,

(edisk.exe)	Emergency Disk	allowing you to identify viruses found in memory.
Virus Info (Virlist32.exe**)**	View current information about viruses	Connects to the Network Associates Virus Information and Technical Documentation Library website, if you have an Internet browser and connectivity.

Other important features include the ability to:

- use SecureCast push technology to facilitate updating your virus definition files as new viruses are identified, and upgrading your virus identification engine as changes are made to the VirusScan software.
- password protect your program settings.
- detect all known virus-types, including boot, file, mutating, polymorphic , macro, stealth, trojan , and encrypted viruses.
- perform Heuristic Scanning to evaluate the probability that a Microsoft Office macro is a virus or that a program file is a virus.
- respond. automatically to virus detection. This may include alerting the user, cleaning the virus, and deleting or isolating the infected file.
- scan compressed files. See Scanning Compressed Files for more information.
- report virus detection and response activities.
- notify others about virus detection, including co-workers, your network administrator, and e-mail correspondent.
- block access to specified websites.
- identify viruses with pinpoint accuracy, using Network Associates Code Trace™, Code Poly™, and Code Matrix™ technologies.

Related Topics

VirusScan for Windows 95 and Windows 98 can scan most of the major compressed file types.

If your file was compressed using. . .	it can be scanned by . . .
ARC	command line scanning feature only
ARJ	command line scanning feature only
CAB	scan.exe, (but not scanpm.exe nor scan86.exe.); not by System Scan
Diet	command line scanning feature only
LHA (LZH)	all components and modules, except System Scan
LZEXE	all components and modules, except Screen Scan
MSCompress (??_)	all components and modules, except System Scan
PKLite	all components and modules, except Screen Scan
TD0 (Teledisk)	all components and modules, except System Scan and Screen Scan
ZIP, PKZip, Winzip	all components and modules, except System Scan

Founded in 1986, Network Associates, Inc. is the leading provider of productive computing tools for DOS, OS/2, UNIX, and Windows environments. Our anti-virus products are used by more than 16,000 corporations worldwide. Our utility products provide data security, automated version updating, and system inspection and editing. Network Associates is also the pioneer and leading provider of electronically distributed software. All Network Associates products may be purchased through dealers or downloaded from bulletin board systems and on-line services around the world.

Network Associates does not stop at developing the world’s best anti-virus and utility products. We back them with the industry's best service and technical support. Product support is provided by a full-time staff of virus researchers, programmers, and support professionals and delivered directly by Network Associates or authorized agents in more than 50 countries worldwide.

Related Topics

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

Network Associates, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
U.S.A.

Related Topics

To learn about scheduling on-site training for any Network Associates product, call (800) 338-8754.

Related Topics

You must have a dial-up or direct-access Internet account with a service provider in order to link to the Network Associates web site. Contact an Internet Service Provider to obtain account information.

If you have Internet access, but do not have one of the supported browsers, you may download software from one of these sites:

Netscape web site: http://www.netscape.com

Microsoft web site: http://www.microsoft.com

Contact each vendor's website directly to learn more about access options using file transfer protocol (FTP) client software or other ways to obtain browser software.

Related Topics

Network Associates is famous for its dedication to customer satisfaction and has continued this tradition by making the Network Associates site on the World Wide Web a valuable resource for answers to technical support issues. Network Associates encourages you to make this your first stop for answers to frequently asked questions, for updates to Network Associates software, and for the latest news and information. Click the website address shown below to link directly to the Network Associates website. To specify the web browser you want to use or to learn how to obtain web browsing software, click here.

World Wide Web	**http://www.nai.com** Click here to link to the Network Associates Web Site.

If you do not find what you need or do not have Web access, try one of Network Associates' automated services:

Automated Voice and Fax Response System	(408) 988-3034
E-mail	support@nai.com
CompuServe	GO NAI
America Online	Keyword MCAFEEI

If the automated services do not have the answer you need, contact Network Associates at one of the following numbers Monday through Friday between 6:00 a.m. and 6:00 p.m. Pacific time.

For corporate-licensed customers:

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

For retail-licensed customers:

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

To provide the answers you need quickly and efficiently, the Network Associates technical support staff needs some information about your computer and software. Please have this information ready before you call:

- Product name and version number
- Computer brand and model
- Any additional hardware or peripherals connected to your computer
- Operating system type and version numbers
- Network type and software version numbers
- Contents of your AUTOEXEC.BAT file, your CONFIG.SYS file, and your system LOGIN script
- Specific steps to reproduce the problem, if applicable

Related Topics

More than 200 new viruses appear each month, as well as harmful ActiveX controls and Java classes. Often, these new viruses and objects cannot be detected by older data files. Network Associates virus researchers are working constantly to update the data files with the most current virus definitions. New data files, or .DAT files, are released every four to six weeks. You will be notified periodically that it is time to update your data files. For maximum protection, you should update VirusScan .DAT files on a regular basis.

Your purchase of VirusScan for Windows 95 and Windows 98 entitles you to free updates to your data files for as long as you use this version of VirusScan. You may not, however, update VirusScan evaluation copies. Please note also that Network Associates cannot guarantee that future data file releases will remain compatible with earlier versions of its products.

See Note

To update your files regularly and conveniently, use any of these methods:

- **SecureCast.** Install and use this Network Associates automatic update service to take advantage of the latest “push” technology to update your data files automatically and invisibly. To learn more, click here.
- **VirusScan One-button Electronic Updating.** Click **Update** in the VirusScan Old Virus Definitions dialog box, when it appears, in order to connect directly with one of the Network Associates FTP sites. To learn more, click here.
- **Network Associates Electronic Services.** Connect to any of the Network Associates electronic services to update your definition files. To learn more, click here.
- **Major electronic services.** Connect to America Online or CompuServe, to update your definition files. To learn more, click here.

Related Topics

Network Associates SecureCast gives you several options for keeping your VirusScan installation up-to-date, with varying levels of user interaction. One option uses BackWeb's technology to automatically update your data files on a regular basis whenever you are connected to the Internet. If you do not connect long enough for a full download, the software will automatically piece out the work and notify you when a complete update package has arrived.

To use SecureCast, either install the client software from the CD-ROM that contains VirusScan, or download it from the Network Associates website **http://www.nai.com**.

The Network Associates Web Site contains its own instructions for downloading and installing SecureCast software. Please refer to the site for details.

VirusScan periodically reminds you as you start your computer to update your virus definition files. You can download new definition files automatically by following these steps:

1 Click **Update** in the Old Virus Definitions dialog box to connect automatically with the directory that contains current data files.

2 In the Update Files dialog that appears, choose the site from which you want to download your new definition files from the list shown. Choose the site closest to your location to shorten your download time.

3 Click **OK**. VirusScan downloads the new files.

To prepare the new files for use with VirusScan, follow these steps:

1 Download the file to a new directory on your computer.

2 The file is compressed. Decompress it with any PKUNZIP-compatible decompression software. If you do not have decompression software, you can download PKUNZIP (shareware) from any of the Network Associates electronic services.

3 Locate the folders on your hard disk that contain VirusScan files. If you followed the recommended installation procedure, VirusScan installs itself here: C:\Program Files\Network Associates\McAfee VirusScan.

4 Copy the new files into the directory or directories that contain your current VirusScan files. When Windows asks you whether you want to replace your old files with the new data files, click **Yes**.

5 Reboot your computer so that changes take place immediately.

To update your VirusScan data files by downloading new files from the Network Associates website, follow these steps:

1 Download the correct data file (for example, DAT-3102.ZIP) from one of the Network Associates electronic services.

On most services, you will find update files in a separate anti-virus section. Instructions for choosing correct data files appear on the Network Associates website. Click here **http://www.nai.com** to connect.

See Note

2 Download the file to a new directory.

The file is compressed. Decompress it with any PKUNZIP-compatible decompression software. If you do not have decompression software, you can also download PKUNZIP (shareware) from any Network Associates electronic service.

3 Locate the folders on your hard disk that contain VirusScan files. If you followed the recommended installation procedure, VirusScan installs itself here: `C:\Program Files\Network Associates\McAfee VirusScan.`

4 Copy the new files into the directory or directories that contain your current VirusScan files. When Windows asks you whether you want to replace your old files with the new data files, click **Yes**.

5 Reboot your computer so that changes take place immediately.

See Note

Related Topics

Network Associates maintains a presence on America Online and CompuServe. Each service includes a software download area where you can find up-to-date .DAT files and other Network Associates software. Keywords to locate Network Associates on each service appear below:

CompuServe	GO NAI
America Online	Keyword MCAFEE

When you have located the Network Associates software download area, follow these steps to update your VirusScan files:

1 Download the correct data file (for example, DAT-3007.ZIP).

On most services, you will find update files in a separate anti-virus section. Instructions for choosing correct data files appear in the same area.

See Note

2 Download the file to a new directory.

The file is compressed. Decompress the file using any PKUNZIP-compatible decompression software. If you do not have decompression software, you can also download PKUNZIP (shareware) from the same electronic site.

3 Locate the folders on your hard disk that contain VirusScan files. If you followed the recommended installation procedure, VirusScan installs itself here: `C:\Program Files\Network Associates\McAfee VirusScan.`

4 Copy the new files into the directory or directories that contain your current VirusScan files. When Windows asks you whether you want to replace your old files with the new data files, click **Yes**.

5 Reboot your computer so that changes take place immediately.

See Note

Related Topics

Network Associates is committed to providing you with effective and up-to-date tools you can use to protect your system. To that end, we invite you to report any new viruses, Java classes, ActiveX controls, or dangerous websites that VirusScan does not now detect. Please note that Network Associates reserves the right to use any information you supply as it deems appropriate without incurring any obligations whatsoever.

If you have found what you suspect to be a new or unidentified virus, send the infected file to McAfee Labs Anti-Virus Emergency Response Team for analysis, using the **Submit to McAfee** Wizard. You are given the option of removing your personal data from the file before submitting it. See Submitting Virus Information to Anti-Virus Emergency Response Team.

To report new virus strains; harmful ActiveX controls and Java classes; or dangerous Internet sites, use these e-mail addresses:

U.S.A	virus_research@nai.com
Europe	virus_research_europe@nai.com
Japan	avert-jp@nai.com
Asia-Pacific	avert-apac@nai.com

Related Topics

Network Associates Technical Document Library is a repository of current information about viruses. It is located on the web at http://www.nai.com/vinfo/ and can be accessed directly from the **VirusScan Central** toolbox. Typical topics include:

Virus Information

- New Virus Entries
- 10 Most Common Viruses
- Virus By Name
- Virus By Type
- Viruses By Payload Activation Date

Virus Hoax Information

- Virus Hoaxes

Virus Research

- McAfee's Virus Research Department

Technical Documentation

- Antivirus Terminology
- Technical Documents

Related Topics

NetShield is one of Network Associates' server anti-virus solutions. It permits a network administrator to set up Centralized Alerting, a client-server arrangement for detecting and responding to virus infections on a consistent, regular, network-wide basis. NetShield collects alert messages from client programs such as VirusScan in a text file, CENTALRT.TXT, and makes them available to the network administrator. To tell VirusScan to route its network alert messages properly, specify the path to the folder that contains CENTALRT.TXT. For more information, see the NetShield User's Guide.

Related Topics

Centralized Alerting is a Network Associates enterprise-wide virus notification solution. Once configured, workstations running VirusScan send virus notifications to servers running NetShield. This helps administrators locate the source of the virus infections and prevent them from spreading.

1 Ask a system administrator for the name of a server running NetShield and its Centralized Alerting Folder.

2 Make sure you have the privileges required to write to this folder.

3 Locate the **Alert** property page(s) for VirusScan or any VShield module that you want to generate network messages.

4 Select **Send Network Alert** on each property page.

5 Click **Browse** to locate the server's Centralized Alerting folder that your system administrator identified.

6 At the server end, designate a file named **CENTALRT.TXT** for the Alert warning message.

Click for additional information on configurable Alert property pages.

Heuristic scanning evaluates the probability that an executable file or a Microsoft Office macro is a virus. When this feature is enabled, VirusScan for Windows 95 and Windows 98 analyzes the characteristics of the executable and/or the macro, and assesses the likelihood that it is a variant of a known virus.

To configure **Heuristics:**

1 Click **Heuristics.** The **Heuristic Scan Settings** dialog box appears.

2 Click the **Enable Heuristic Scanning** checkbox.

3 Select one of the Heuristic scan settings:

Enable macro heuristics scanning to assess macros but not executable programs.

Enable program file heuristics scanning to assess executable programs but not macros.

Enable macro and program file heuristics scanning to asses both macros and executables.

4 Select the **Remove all macros when cleaning infected documents** checkbox to remove macros from the document, whether they are potentially viral or not.

5 Click **OK**.

This feature can be enabled in four circumstances:

{button ,JI(`vscan4.HLP',`Configuring_System_Scan_Detection_Properties')} when configuring the System Scan detection properties for on-access scanning.

{button ,JI(`vscan4.HLP',`Perform_an_Advanced_On_Demand_Scan')} when configuring detection properties for an advanced on-demand scan.

{button ,JI(`vscan4.HLP',`Configuring_On_Demand_E_mail_Scan_Detection_Properties')} when configuring detection properties for on-demand e-mail scanning

{button ,JI(`vscan4.HLP',`Configuring_VirusScan_Detection_Properties')} when configuring the Program property page for a scheduled scanning task.

Lotus cc:Mail users can locate the names of people to include in the e-mail distribution of VShield notifications.

To add an addressee to the list:

1. Type the **addressee's** name in the **Name** box.
2. Click **Add**. The name is added to the list.
3. Click **Close**.

To delete an addressee from the list:

1. Select the addressee's name from the list box.
2. Click **Delete**. The name is removed from the list.
3. Click **Close**.

To select a particular directory or mailing list:

1. Click the in the **Look in** box.
2. Select a directory or mailing list from the drop-down list.

 Related Topics

Provide VShield with the path to cc:Mail Post Office.

1 Enter your name.
2 Enter your cc:Mail password.
3 Enter the path to the cc:Mail Post Office.

Related Topics

Add a file extension or file type to scan.

1 Type the three-character file extension that you want to include in scanning. Do not include the dot that ordinarily precedes file extensions.

2 Click **OK**.

Specify the Internet IP address you want to ban. For a fuller discussion, see Blocking Internet Access to a Particular IP Address

1 Enter the address in the **IP address** box.

2 Enter the subnet in the **Subnet mask** box.

3 Click **OK**.

Specify the URL you want to ban. For a fuller discussion, see Blocking Internet Access to a Particular URL.

1 Enter the URL address in the **URL name** box.

2 Click **OK**.

Choose items to be included in System scanning.

1 If you want to scan a number of drives connected to your computer, click **select item to scan.**

If you want to scan a particular location, click **Select drive or folder to scan**.

2 If you choose **Select item to scan**, click the and select the scope of the scan. You can include all drives connected to your computer, all removable drives, all fixed drives, or all network drives.

OR

3 If you choose **Select drive or folder to scan**, click **Browse** and select the drive or folder to include. Select the **Include subfolders** checkbox if you want to include subfolders in the scan.

4 When finished, click **OK** to save your changes and close the dialog box.

▶ Starts scanning immediately based on the selections defined on the **Where & What**, **Actions** and **Reports** tabs.

- Halts scanning immediately.

- Restores the default for all options on the **Where & What**, **Actions** and **Reports** tabs.

- Select the disk drive, folder files or file types to scan.

- Select VirusScan's response when it detects a virus.

- Select the method of notifying the user that VirusScan has detected a virus, and select a file for reporting scanning outcomes.

On-Access scanning is triggered automatically when a particular event occurs, such as opening or running a file. On-access scans are controlled by the **VShield** component. They can be configured to run automatically when you:

- run, create, copy, or rename a file on a local or network drive.
- access a floppy disk or shut down your system while a floppy disk is in the disk drive.
- receive an e-mail message that includes a file attachment.
- download a file from the Internet
- attempt to connect to banned URL or IP Internet addresses.

{button ,JI(`vscan4.HLP>First',`The_VShield_User_Interface')} Click to view **VShield** interface

On-Demand scanning occurs whenever the user issues the command to scan. You can run **on-demand scans** whenever you want.

- Scans of folders or files on a local or network drive are controlled by the **VirusScan** component, and are based on Classic or Advanced settings. For additional information, see Classic On-Demand Scanning vs. Advanced On-Demand Scanning .
- Scans of e-mail are controlled by the **On-Demand E-mail Scan** component.

{button ,JI(`vscan4.HLP>First',`The_Virus_Scan_User_Interface')} Click to view **VirusScan** interface

{button ,JI(`vscan4.HLP>First',`The_On_Demand_E_mail_Scan_Configuration_Screen')} Click to view **On-Demand E-mail Scan Configuration Screen**.

On-Schedule scanning occurs at times that the user defines in advance, using the **VirusScan Scheduler** component. Scheduled tasks run only if the Scheduler is open at the time specified for the scan.

- Schedules can be set to scan folders or files on any local or network drive automatically.
- User-defined scanning tasks can specify inclusion of particular drives, folders and files.

{button ,JI(`vscan4.HLP>First',`The_Scheduler_User_Interface')} Click to view **Scheduler** interface

Related Topics

If you want to scan local or network drives during times that your screen saver is displayed, it is necessary to perform a Custom installation of VirusScan for Windows 95 and Windows 98 and include **ScreenScan** in the installation.

1 Right-click on your desktop and select Properties. If ScreenScan is installed, select the property page labeled **McAfee ScreenScan**. If this property page is not present, ScreenScan is not installed.

2 Select the checkbox labeled **Enable scanning while in screen saver mode**.

3 By default, ScreenScan is set to scan all fixed drives. You may modify the list of items to be scanned:

- To add items to the list, click **Add** at the bottom of the screen. A dialog box appears in which you can specify other items for scanning.
- To edit items on the list, click **Edit**.
- To remove an item from the list, select the item and click **Remove**.

4 Select the **Include subfolders** checkbox if you want to scan subfolders as well as high-level folders.

5 Click one of the buttons to indicate whether all files should be scanned, or only Program files.

- If you select **Program files only**, click **Extensions** to view a list of file extensions that VirusScan will scan. You can edit the list.

6 Select the **Compressed files** checkbox to include files created with file compression utilities. See Scanning Compressed Files for more information. Because VirusScan decompresses these file types in memory before checking for viruses, this option can increase the time it takes to complete a scan.

7 Click the checkbox labeled **Resume scanning from where ScreenScan left off** if you want ScreenScan to continue scanning that was begun during an earlier screen saver interlude, but subsequently interrupted by mouse movement or keystroke.

8 Click **Advanced** to set scanning priorities.

- Use the slider to set a priority level for virus scanning relative to other programs that may be running while your screen saver is active.
- Select **Enable logging of ScreenScan activities to file** if you want to have a record of scanning activities.
- Click **Browse** to select a folder for the log file.
- Click **OK** when finished with advanced settings. You are returned to the ScreenScan property page.

9 When finished:

- Click **Apply** to save the detection options you chose without leaving the **Program** property page, or
- Click **OK** to save any changes you made in this or any other property page and close the VirusScan Properties dialog box, or
- Click **Cancel** to close the dialog box without saving any changes.

Related Topics

VirusScan provides two scanning modes for on-demand scanning, **Classic** and **Advanced.**

A comparison of the capabilities of each type is displayed below:

Feature	Classic	Advanced
Select location to scan	Single location	Multiple locations
Select the file types to include	Yes	Yes
Prescribe automatic responses to all viruses detected	Yes	Yes
Allow user to customize the assortment of options available when a virus is detected	No	Yes
Select a method of signaling you that a virus has been detected	Yes	Yes
Specify the information recorded in the log of scanning events	VirusScan selects information to include	You select information to include
Circulate information about viruses detected via Centralized Alert Messaging	No	Yes
Circulate information about viruses detected via Desktop Management Interface	No	Yes
Perform heuristic scanning of Microsoft Office macros	No	Yes
Perform heuristic scanning of program files	No	Yes
Exclude selected folders from scanning	No	Yes
Password protect the options you select	No	Yes
Access the Scheduler where you can create a scanning schedule	Yes	Yes

Related Topics

To configure and perform an on-demand scan of a local or network drive:

1 Click **Start** on the bottom-left of your screen.

2 Select **Programs → McAfee VirusScan → McAfee VirusScan Central**. The **McAfee Launcher** appears.

3 Select **Scan.** The **McAfee Virus Scan** screen appears. By default, it opens to the **Classic** scan configuration pages.

To confirm that you are on the Classic Scan page, select the **Tools** menu.

- If the word **Advanced** appears on the menu, you are now in the **Classic** scan page.
- If the word **Classic** appears on the menu, you are now in the **Advanced** scan page. Select **Classic** to configure a classic scan.

If you want to perform an advanced scan, see Perform an Advanced On-Demand Scan

4 Select the **Where & What** tab. By default, VirusScan assumes that you want to scan your **C** drive. If you want to scan a different drive, click **Browse** and select a local or network drive.

5 Next, select the **Include subfolders** checkbox if you want to scan subfolders as well as high-level folders.

6 Click one of the buttons to indicate whether all files should be scanned, or only Program files.

- If you select **Program files only**, click **Extensions** to view a list of file extensions that VirusScan will scan. You can edit the list.

7 Select the **Compressed files** checkbox to include files created with file compression utilities. See Scanning Compressed Files for more information. Because VirusScan decompresses these file types in memory before checking for viruses, this option can increase the time it takes to complete a scan.

8 Activate scanning or continue configuring:

- Click **Scan Now** to proceed with scanning immediately.
- Click **Stop** to halt a scan after it has started.
- Click **New Scan** to over-write your configuration choices with **VirusScan's** defaults.

OR

- Select another tab to continue configuring.

{button ,JI(`vscan4.HLP',`Classic_Scan_Action_Tab')} Action Tab

{button ,JI(`vscan4.HLP',`Classic_Scan_Report_Tab')} Report Tab

Related Topics

1 Select the **Action** tab to specify how VirusScan will respond when it detects a virus. By default**, Prompt for user action** appears as the selected response.

2 Click the down arrow if you want to select a different VirusScan response to virus detection. The display in the **Possible actions** varies in accordance with the response you select:

- If you leave the selected response as **Prompt for user action**, you will be given an opportunity to select any one of the possible actions each time a virus is detected. If you select the other option from the drop-down list, that option will operate automatically each time a virus is detected.
- If you select **Move infected files automatically**, you are asked to provide the location and name of a folder to receive the file.
- If you select **Clean infected files automatically**, **Delete infected files automatically**, or **Continue Scanning**, a message appears explaining your choice.

3 Activate scanning or continue configuring:

- Click **Scan Now** to proceed with scanning immediately.
- Click **Stop** to halt a scan after it has started.
- Click **New Scan** to over-write your configuration choices with **VirusScan's** defaults.

OR

- Select another tab to continue configuring.

{button ,JI(`vscan4.HLP',`Classic_Where_and_What_Tab')} Where and What Tab

{button ,JI(`vscan4.HLP',`Classic_Scan_Report_Tab')} Report Tab

Related Topics

1 Select the **Reports** tab to specify how you want VirusScan to inform you that it has detected a virus, and to set up a log file to record scanning activities.

2 If you selected **Prompt for user action** on the **Action** tab, VirusScan needs to know how to prompt you: with an on-screen message, a beep, or both. By default, the message in the text box will appear dimmed.

- To change the message, select the **Display custom message** checkbox and type a new message.
- To omit the beep, clear the **Sound audible alert** checkbox.

3 You may make changes in the log file set-up. VirusScan creates a file called VSCLog.txt, having a maximum size of 100 KB, and recording all of the available report options shown on the screen. The default location of the log file is C:\Program Files\Network Associates\McAfee Virus Scan\. If you want to change these defaults, you may:

- Clear the Log to file checkbox, thus disabling the logging activity.
- Type a new name or path for the text file generated. VirusScan will only generate a file in plain text format.
- Click **Browse** to select a location for the file.
- Clear the **Limit size of log file** checkbox to remove any size restriction.
- Change the maximum size of the log file.
- Clear the checkboxes for any of the elements of the report that you are not interested in seeing.

4 Activate scanning or continue configuring:

- Click **Scan Now** to proceed with scanning immediately.
- Click **Stop** to halt a scan after it has started.
- Click **New Scan** to over-write your configuration choices with **VirusScan's** defaults.

OR

- Select another tab to continue configuring.

{button ,JI(`vscan4.HLP',`Classic_Where_and_What_Tab')} Where and What Tab

{button ,JI(`vscan4.HLP',`Classic_Scan_Action_Tab')} Action Tab

To configure and perform an on-demand scan of a local or network drive:

1 Click **Start** on the bottom-left of your screen.

2 Select **Programs → McAfee VirusScan → McAfee VirusScan Central**. The **McAfee Launcher** appears.

3 Select **Scan.** The **McAfee Virus Scan** screen appears. By default, it opens to the **Classic** scan configuration pages.

- To confirm that you are on the Classic Scan page, select the **Tools** menu. If the word **Advanced** appears on the menu, you are now on the **Classic** scan page.
- Select **Advanced** to configure an advanced scan.
- If you want to perform a **Classic** scan, see Perform a Classic On-Demand Scan

4 Select the **Detection** tab. By default, VirusScan assumes that you want to scan your **C** drive.

5 If you want to scan additional locations, click **Add**. The **Add Scan Item** screen appears.

See Note

6 Select the button describing the additional location(s).

- If you want to scan a number of drives connected to your computer, click **select item to scan**. Next, click the

and select the scope of the scan. You can include all drives connected to your computer; all removable drives; all fixed drives; or all network drives.

- If you want to scan a particular location, click **Select drive or folder to scan**. Next, click **Browse** and select the drive or folder to include. Finally, select the **Include subfolders** checkbox if you want to include subfolders in the scan.

7 When finished, click **OK** to save your changes and close the dialog box.

8 Click one of the buttons to indicate whether all files should be scanned, or only Program files.

- If you select **Program files only**, click **Extensions** to view a list of file extensions that VirusScan will scan. You can edit the list.

9 Select the **Compressed files** checkbox to include files created with file compression utilities. See Scanning Compressed Files for more information. Because VirusScan decompresses these file types in memory before checking for viruses, this option can lengthen the time it takes to complete a scan.

10 Click **Macro Heuristics** to include scanning of Microsoft Office macros. For more information, see Macro Heuristic Scanning.

11 Activate scanning or continue configuring:

- Click **Scan Now** to proceed with scanning immediately.
- Click **Stop** to halt a scan after it has started.
- Click **New Scan** to over-write your configuration choices with **VirusScan's** defaults.

OR

- Select another tab to continue configuring.

{button ,JI(`vscan4.HLP',`Advanced_Scan_Action_Tab')} Action tab

{button ,JI(`vscan4.HLP',`Advanced_Scan_Alert_Tab')} Alert tab

{button ,JI(`vscan4.HLP',`Advanced_Scan_Report_Tab')} Report tab

{button ,JI(`vscan4.HLP',`Advanced_Scan_Exclusion_Tab')} Exclusion tab

Related Topics

1 Select the **Action** tab to specify how VirusScan will respond when it detects a virus. By default, **Prompt for user action** appears as the selected response.

2 Click the down arrow if you want to select a different VirusScan response to virus detection. The display in the **Possible actions** varies in accordance with the response you select:

- If you leave the selected response as **Prompt for user action**, you will be given an opportunity to select any one of the possible actions selected each time a virus is detected. If you select a different option from the drop-down list, that option will operate automatically each time a virus is detected.
- If you select **Move infected files automatically**, you are asked to provide the location and name of a folder to receive the file.
- If you select **Clean infected files automatically**, **Delete infected files automatically**, or **Continue Scanning**, a message appears explaining your choice.

3 Activate scanning or continue configuring:

- Click **Scan Now** to proceed with scanning immediately.
- Click **Stop** to halt a scan after it has started.
- Click **New Scan** to over-write your configuration choices with **VirusScan's** defaults.

OR

- Select another tab to continue configuring.

{button ,JI(`vscan4.HLP',`Advanced_Detection_Tab')} Detection Tab

{button ,JI(`vscan4.HLP',`Advanced_Scan_Alert_Tab')} Alert tab

{button ,JI(`vscan4.HLP',`Advanced_Scan_Report_Tab')} Report tab

{button ,JI(`vscan4.HLP',`Advanced_Scan_Exclusion_Tab')} Exclusion tab

1 Select the **Alert** tab if you want VirusScan to send a message when it detects a virus.

2 Select the **Send network alert** checkbox if you want an alert to be posted to a network server. The **Browse** button is activated and you can choose for a location for the network alert. When selected, the path to the location appears in the text box.

3 Select the **DMI** checkbox to send notification to network management or desktop management applications that comply with the **Desktop Management Interface** standard.

4 If you selected Prompt for user action on the **Action** tab, VirusScan must know how to prompt you: with an on-screen message, a beep, or both. By default, the message in the text box will appear dimmed.

- To change the message, select the **Display custom message** checkbox and type a new message.
- To omit the beep, clear the **Sound audible alert** checkbox.

5 Activate scanning or continue configuring:

- Click **Scan Now** to proceed with scanning immediately.
- Click **Stop** to halt a scan after it has started.
- Click **New Scan** to over-write your configuration choices with **VirusScan's** defaults.

OR

- Select another tab to continue configuring.

{button ,JI(`vscan4.HLP',`Advanced_Detection_Tab')} Detection Tab

{button ,JI(`vscan4.HLP',`Advanced_Scan_Action_Tab')} Action tab

{button ,JI(`vscan4.HLP',`Advanced_Scan_Report_Tab')} Report tab

{button ,JI(`vscan4.HLP',`Advanced_Scan_Exclusion_Tab')} Exclusion tab

1 Select the **Report** tab if you want VirusScan to maintain a log of its activities. By default, VirusScan creates a file called VSCLog.txt, having a maximum size of 100 KB, and recording all of the available report options shown on the screen. The default location of the log file is C:\Program Files\Network Associates\McAfee Virus Scan\. If you want to change these defaults, you may:

- Clear the **Log to file** checkbox, thus disabling the logging activity.
- Type a new name or path for the text file generated. VirusScan will only generate a file in plain text format.
- Click **Browse** to select a location for the file.
- Clear the **Limit size of log file** checkbox to remove any size restriction.
- Change the maximum size of the log file.
- Clear the checkboxes of any elements of the report that you are not interested in seeing.

2 Activate scanning or continue configuring:

- Click **Scan Now** to proceed with scanning immediately.
- Click **Stop** to halt a scan after it has started.
- Click **New Scan** to over-write your configuration choices with **VirusScan's** defaults.

OR

- Select another tab to continue configuring.

{button ,JI(`vscan4.HLP',`Advanced_Detection_Tab')} Detection Tab

{button ,JI(`vscan4.HLP',`Advanced_Scan_Action_Tab')} Action tab

{button ,JI(`vscan4.HLP',`Advanced_Scan_Alert_Tab')} Alert tab

{button ,JI(`vscan4.HLP',`Advanced_Scan_Exclusion_Tab')} Exclusion tab

1 Select the **Exclusion** tab to specify folders to exclude from virus scanning. By default, VirusScan does not scan files in the Recycled folder.

- Select **Add** to specify a folder to be excluded. Your are given the option of including subfolders and specifying whether the exclusion is from file scanning or boot sector scanning.
- Select **Edit…** to modify the instructions pertaining to a selected folder already listed.
- Select **Remove** to delete a selected folder from the list.

2 Activate scanning or continue configuring:

- Click **Scan Now** to proceed with scanning immediately.
- Click **Stop** to halt a scan after it has started.
- Click **New Scan** to over-write your configuration choices with **VirusScan's** defaults.

OR

- Select another tab to continue configuring.

{button ,JI(`vscan4.HLP',`Advanced_Detection_Tab')} Detection Tab

{button ,JI(`vscan4.HLP',`Advanced_Scan_Action_Tab')} Action tab

{button ,JI(`vscan4.HLP',`Advanced_Scan_Alert_Tab')} Alert tab

{button ,JI(`vscan4.HLP',`Advanced_Scan_Report_Tab')} Report tab

Each time you start your computer, VirusScan performs the scanning tasks that have been enabled and configured on the VShield property pages. See Configure VShield Modules for more information on configuring VShield.

In addition, VirusScan provides three more default scanning configurations. Each one can be configured, scheduled and activated at any time. You can define and schedule as many additional scans as you want. The **VirusScan Scheduler** controls these features. To access the **Scheduler**, click in the system tray at the bottom-right of your screen. The VirusScan Scheduler appears. Alternatively, you can access the **Scheduler** by clicking **Start** on the bottom-left of your screen. Next, select **Programs → McAfee VirusScan → VirusScan Central → Schedule**.

{button ,JI(`VScan4.hlp',`Scheduling_Scanning_Tasks')} Scheduling Scanning Tasks

{button ,JI(`vscan4.HLP',`Creating_New_Tasks')} Creating New Tasks

Related Topics

To schedule scanning tasks:

1 Click in the system tray at the bottom-right of your screen. The Virus Scan Scheduler appears. Alternatively, you can access the Scheduler by clicking **Start** on the bottom-left of your screen. Next, select **Programs → McAfee VirusScan → VirusScan Central → Schedule**.

2 Double-click the task that you want to schedule. The **Task Properties** pages for the selected scan appear.

3 Select the **Program** tab.

4 Provide a descriptive name for the task.

- If you are configuring a task already listed in the Scheduler, the Description box displays the name of the selected task. You can change the description if you want.
- If you are creating a new task, the Description box is empty. Enter a descriptive name for the task.

5 The **Program** text box displays the path to the scanning program file, Scan32.exe. If you have installed VirusShield to a location different from the default installation location, click **Browse** to locate and select the file.

6 The **Start in** text box displays the path to the folder in which Scan32.exe is located. If the file is in a different folder, click **Browse** to locate and select it.

7 The **Parameters** text box allows advanced users to incorporate option switches for this program.

8 **Click** the down arrow in the **Run in** text box if you want the scan to run in a maximized or minimized window rather than a normal window.

9 Click **Configure** to specify properties for the scheduled scan. The **McAfee VirusScan Properties** pages will appear. See Configuring VirusScan Properties for more information.

10 Activate scanning or continue configuring:

- Click **Run Now** if you want to perform the scan immediately.

OR

- Select the **Schedule** tab to continue configuring.

OR

- Click the **Status** tab to view information about the scheduled run.

11 When finished:

- Click **Apply** to save the detection options you chose without leaving the **Program** property page, or.
- Click **OK** to save any changes you made in this or any other property page and close the VirusScan Properties dialog box, or
- Click **Cancel** to close the dialog box without saving any changes.

Related Topics

1. Click **Start** on the bottom-left of your screen.
2. Select **Programs → McAfee VirusScan → VirusScan Central → Schedule**. The Scheduler appears.
3. Double-click the task that you want to schedule. The **Task Properties** pages for the selected scan appear.
4. Select the **Schedule** tab.
5. Click the **Enable** checkbox.
6. In the **Run** portion of the screen, select the button representing the frequency with which you want the scan to run.
7. In the **Start at** portion of the screen, select any day(s) of the week on which you want the scan to run, and enter the time of day in the text box.
8. Activate scanning or continue configuring:

   Click **Run Now** on the **Program** tab if you want to perform the scan immediately, or review the configuration options already chosen.

   OR

   Click the **Status** tab to view information about the scheduled run.
9. When finished:

   Click **Apply** to save the detection options you chose without leaving the **Program** property page, or.

   Click **OK** to save any changes you made in this or any other property page and close the VirusScan Properties dialog box, or

   Click **Cancel** to close the dialog box without saving any changes.

There are two methods for adding a new scheduled task. The first involves creating the task *from scratch*. The other involves copying an existing task, then renaming and reconfiguring it.

Method 1-Create a New Task:

1 Select menu choice **Task → New Task**, or click on the toolbar. The **Task Properties** pages appear, and the Description box is empty.

2 Enter a descriptive name for the task.

3 See Scheduling Scanning Tasks (starting with Step 4) for remainder of instructions.

Method 2-Copy an existing task:

1 Select an existing task. Next, **right-click → Copy**. Then, **right-click → Paste.** The **Task Properties** pages appear.

See Note

2 Replace the descriptive name with a new description for the task.

3 See Scheduling Scanning Tasks (starting with Step 4) for remainder of instructions.

Related Topics

To configure VirusScan On-Demand scans of local or network drives:

1 Click **Start** on the bottom-left of your screen.

2 Select **Programs → McAfee VirusScan → VirusScan Central → Schedule**. The Virus Scan Scheduler appears.

3 Select on of the scans listed under **Description**.

4 Click the icon on the Scheduler toolbar. The **McAfee VirusScan Properties** pages appear.

OR

Double-click the description of the scan that you want to configure. The **Task Properties** pages for the selected scan appear. Next, click **Configure**. The **McAfee VirusScan Properties** pages appear.

5 Configure the properties on each of the tabbed pages.

{button ,JI(`vscan4.HLP',`Configuring_VirusScan_Detection_Properties')} Detection Tab

{button ,JI(`vscan4.HLP',`Configuring_VirusScan_Action_Properties')} Action Tab

{button ,JI(`vscan4.HLP',`Configuring_VirusScan_Alert_Properties')} Alert Tab

{button ,JI(`vscan4.HLP',`Configuring_System_Scan_Report_Properties')} Report Tab

{button ,JI(`vscan4.HLP',`Configuring_VirusScan_Exclusion_Properties')} Exclusion Tab

{button ,JI(`vscan4.HLP',`Configuring_VirusScan_Security')} Security Tab

Related Topics

1 Click **Start** on the bottom-left of your screen.

2 Select **Programs → McAfee VirusScan → VirusScan Central → Schedule**. The Virus Scan Scheduler appears.

3 Select a task *other than* **McAfee VShield**. For information on configuring **VShield**, see Configure VShield Modules

4 Click the icon on the Scheduler toolbar. The **McAfee VirusScan Properties** pages appear.

OR

Double-click the description of the scan that you want to configure. The **Task Properties** pages for the selected scan appear. Next, click **Configure**. The **McAfee VirusScan Properties** pages appear.

5 Select the **Detection** tab. By default, VirusScan assumes that you want to scan your **C** drive.

6 If you want to scan additional locations, click **Add**. The **Add Scan Item** screen appears.

See Note

7 Select the button describing the additional location(s).

- If you want to scan a number of drives connected to your computer, click **Select item to scan**.
- If you want to scan a particular location, click **Select drive or folder to scan**.

8 If you choose **Select item to scan**, click the and select the scope of the scan. You can include all drives connected to your computer; all removable drives; all fixed drives; or all network drives.

OR

If you choose **Select drive or folder to scan**, click **Browse** and select the drive or folder to include. Next, select the **Include subfolders** checkbox if you want to include subfolders in the scan.

9 When finished, click **OK** to save your changes and close the dialog box.

10 In the **What to scan** portion of the screen, select any or all of the checkboxes.

- Select the **Scan Memory** checkbox to include memory-resident viruses in the scan. These viruses are retained in memory after they run, continuing to affect other files.
- Select the **Scan boot sectors** checkbox to include boot sector viruses in the scan. The boot sector is the first logical division of a hard or floppy disk. Your computer's BIOS looks here soon after you turn it on to find the files and programs it needs to start operations.
- Select the **Compressed files** checkbox to include files created with file compression utilities. See Scanning Compressed Files for more information.. Because VirusScan decompresses these file types in memory before checking for viruses, this option can lengthen the time it takes to complete a scan.
- Select the **Start automatically** checkbox if you want the scan to begin without any prompts, but based only on options selected on the **Scheduler** See Scheduling On-Demand Scans to Run Automatically for more information.

11 Next, in the **What to scan** portion of the screen, click one of the buttons to indicate whether all files should be scanned, or only Program files.

- If you select **Program files only**, click **Extensions** to view a list of file extensions that VirusScan will scan. You can edit the list.

12 Click **Heuristics** to configure Heuristic scanning.

13 Click **Apply** to save your changes without closing the dialog box. This completes the **Detection** property page.

14 Click another tab to continue.

See Note

Related Topics

1 Click **Start** on the bottom-left of your screen.

1 Select **Programs → McAfee VirusScan → VirusScan Central → Schedule**. The Virus Scan Scheduler appears.

3 Select a task *other than* **McAfee VShield**. For information on configuring **VShield**, see Configure VShield Modules

4 Click the icon on the Scheduler toolbar. The **McAfee VirusScan Properties** pages appear.

OR

Double-click the description of the scan that you want to configure. The **Task Properties** pages for the selected scan appear. Next, click **Configure**. The **McAfee VirusScan Properties** pages appear.

5 Select the **Action** tab to specify how VirusScan will respond when it detects a virus. By default**, Prompt for user action** appears as the selected response.

6 Click the down arrow if you want to select a different VirusScan response to virus detection. The display in the **Possible actions** varies in accordance with the response you select. : If you leave the selected response as **Prompt for user action**, you will be given an opportunity to select any one of the possible actions each time a virus is detected. If you select one of the other options from the drop-down list, that option will operate automatically each time a virus is detected.

- If you leave the selected response as **Prompt for user action**, clear the possible actions that you do not want to apply. Leave the checkmark for actions that you want to apply.
- If you select **Move infected files automatically**, you are asked to provide the location and name of a folder to receive the file.
- If you select **Clean infected files automatically**, **Delete infected files automatically**, or **Continue Scanning**, a message appears explaining your choice.

7 Click **Apply** to save your changes without closing the dialog box. This completes the **Action** property page.

8 Click another tab to continue.

- **See Note**
- Related Topics

1 Click **Start** on the bottom-left of your screen.

2 Select **Programs → McAfee VirusScan → VirusScan Central → Schedule.** The Virus Scan Scheduler appears.

3 Select a task *other than* **McAfee VShield**. For information on configuring **VShield**, see Configure VShield Modules

4 Click the icon on the Scheduler toolbar. The **McAfee VirusScan Properties** pages appear.

OR

Double-click the description of the scan that you want to configure. The **Task Properties** pages for the selected scan appear. Next, click **Configure**. The **McAfee VirusScan Properties** pages appear.

5 Select the **Alert** tab if you want VirusScan to send a message when it detects a virus.

6 Select the **Send network alert** checkbox if you want an alert to be posted to a network server. The **Browse** button is activated and you can browse for a location for the network alert. When selected, the path to the location appears in the text box.

7 Select the **DMI** checkbox to send notification to network management or desktop management applications that comply with the **D**esktop **M**anagement **I**nterface standard.

8 If you selected **Prompt for user action** on the **Action** tab, VirusScan needs to know how to prompt you: with an on-screen message, a beep, or both. By default, the message in the text box will appear dimmed.

- To change the message, select the **Display custom message** checkbox and type a new message.
- To omit the beep, clear the **Sound audible alert** checkbox.

9 Click **Apply** to save your changes without closing the dialog box. This completes the **Alert** property page.

10 Click another tab to continue.

See Note
Related Topics

1 Click **Start** on the bottom-left of your screen.

2 Select **Programs → McAfee VirusScan → VirusScan Central → Schedule.** The Virus Scan Scheduler appears.

3 Select a task *other than* **McAfee VShield**. For information on configuring **VShield**, see Configure VShield Modules

4 Click the icon on the Scheduler toolbar. The **McAfee VirusScan Properties** pages appear.

OR

Double-click the description of the scan that you want to configure. The **Task Properties** pages for the selected scan appear. Next, click **Configure**. The **McAfee VirusScan Properties** pages appear.

5 Select the **Report** tab if you want VirusScan to maintain a log of its activities. By default, VirusScan creates a file called VSHLog.txt, having a maximum size of 100 KB, and recording all of the available report options shown on the screen. The default location of the log file is C:\Program Files\Network Associates\McAfee Virus Scan\. If you want to change these defaults, you may:

- Clear the **Log to file** checkbox, thus disabling the logging activity.
- Type a new name or path for the text file generated. VirusScan will only generate a file in plain text format.
- Click **Browse** to select a location for the file.
- Clear the **Limit size of log file** checkbox to remove any size restriction.
- Change the maximum size of the log file.
- Clear the checkboxes for any of the elements of the report that you are not interested in seeing.

6 Click **Apply** to save your changes without closing the dialog box. This completes the **Report** property page.

7 Click another tab to continue.

See Note

Related Topics

1 Click **Start** on the bottom-left of your screen.

1 Select **Programs → McAfee VirusScan → VirusScan Central → Schedule.** The Virus Scan Scheduler appears.

3 Select a task *other than* **McAfee VShield**. For information on configuring **VShield**, see Configure VShield Modules

4 Click the icon on the Scheduler toolbar. The **McAfee VirusScan Properties** pages appear.

OR

Double-click the description of the scan that you want to configure. The **Task Properties** pages for the selected scan appear. Next, click **Configure**. The **McAfee VirusScan Properties** pages appear.

5 Select the **Exclusion** tab to specify folders to exclude from virus scanning. By default, VirusScan does not scan files in the **Recycled** folder.

- Select **Add…** to specify a folder to be excluded. Your are given the option of including subfolders and specifying whether the exclusion is from file scanning or boot sector scanning.
- Select **Edit…** to modify the instructions pertaining to a selected folder already listed.
- Select **Remove** to delete a selected folder from the list. :

6 Click **Apply** to save your changes without closing the dialog box. This completes the **Exclusion** property page.

7 Click another tab to continue.

- **See Note**
- Related Topics

1 Click **Start** on the bottom-left of your screen.

2 Select **Programs → McAfee VirusScan → VirusScan Central → Schedule.** The Virus Scan Scheduler appears.

3 Click the icon on the Scheduler toolbar. The **McAfee VirusScan Properties** pages appear.

OR

Double-click the description of the scan that you want to configure. The **Task Properties** pages for the selected scan appear. Next, click **Configure**. The **McAfee VirusScan Properties** pages appear.

4 Select the scanning task for which you want to configure security options. If you select McAfee VShield, see Configuring VShield Security Properties for instructions. If you select one of the other scanning tasks listed, proceed to step 5.

5 Select the **Security** tab.

6 Select the page(s) to be password protected.

- The graphic representation of an open lock changes to a closed lock, indicating that the option is “locked down.”
- The Password button is enabled.
- The Inherit security options checkbox is enabled.

7 Click **Password**. The **Specify Password** dialog box opens.

8 Enter a password. Next, re-enter the password exactly as you first typed it.

9 Click **OK**.

10 If you are configuring a task that was created by copying a previously existing task, select the **Inherit Security Options** checkbox to apply the security options of the original task to the new task. The checkbox is enabled after you select one of the property pages for password-protection.

11 Click **Apply** to save your changes without closing the dialog box. This completes the **Detection** property page.

12 Click another tab to continue.

See Note

Information on Security for On Access and Internet Scanning

Designate property pages, (tabs) requiring password-protection.

1 Select the property page(s) to be password–protected.

2 Click **Password** to specify a password.

3 Click **OK** when finished.

Prohibit access to a URL that you believe to contain harmful ActiveX or Java objects.

1 Click **Start** on the bottom-left of your screen.

1 Select **Programs → McAfee VirusScan → VirusScan Central → VShield.** The VShield property pages appear**.**

{button ,JI(`vscan4.HLP>Third',`Navigate_to_the_VShield_Configuration_Pages')} Click for information on alternative approaches to accessing VShield property pages.

3 Select **Internet Filter** in the components box on the left side of the configuration pages. The Internet filter property pages appear.

4 Select the **Detection** tab.

5 Assure that the **Enable Java & ActiveX** filter checkbox is selected.

6 Select the **Internet URLs to block** checkbox near the bottom of the screen.

7 Click the adjacent **Configure** button. The **Banned URLs** dialog box opens.

8 Click **Add**. The Add URL dialog box opens.

9 Enter the URL in the text box.

10 Click **OK**. The name of the banned URL appears in Banned URLs dialog box.

11 Click **OK**

12 Click **Apply** if you want to save your changes and continue configuring, or, if finished making configurations changes, click **OK** to save your changes and close the property pages.

13

Related Topics

Prohibit access to an Internet IP Address that you believe to contain harmful ActiveX or Java objects.

1 Click **Start** on the bottom-left of your screen.

2 Select **Programs → McAfee VirusScan → VirusScan Central → VShield.** The VShield property pages appear.

{button ,JI(`vscan4.HLP>third',`Navigate_to_the_VShield_Configuration_Pages')} Click for information on alternative approaches to accessing VShield property pages.

3 Select **Internet Filter** in the components box on the left side of the configuration pages. The Internet Filter property pages appear.

4 Select the **Detection** tab.

5 Assure that the **Enable Java & ActiveX filter** checkbox is selected.

6 Select the **IP Addresses to block** checkbox near the bottom of the screen.

7 Click the adjacent **Configure** button. The **Banned IP addresses** dialog box opens.

8 Click **Add**. The **Add IP address** dialog box opens.

9 Enter the address in the IP address text box.

10 Enter the Subnet in the Subnet mask text box.

11 Click **OK**. The address appears in **Banned IP addresses** dialog box.

12 Click **OK**

13 Click **Apply** if you want to save your changes and continue configuring, or, if finished making configurations changes, click **OK** to save your changes and close the property pages.

Related Topics

Once activated and configured, the appears in the system tray at the bottom-right of your screen, in the same location as the current time. This indicates that VShield is operating in the background, watching for and then scanning files that you access, e-mail you receive, files you download or Java and ActiveX objects that you encounter. To enable or disable scanning activity, or to see a summary of actions:

1 Double-click the VirusScan icon to open the Status dialog box pages.

2 Click the tab that corresponds to the program component you want to enable or disable, or whose progress you want to check.

VShield reports the number of files it has scanned, moved or deleted and the number of infected files it has found for the System Scan, E-mail Scan and Download Scan program components. For Java and ActiveX applets or Internet sites, VShield reports the number of items it has scanned and the number it has “banned,” or kept you from encountering. If you have activated its logging feature, VShield also records the same information in the log file for each program component.

3 Click **Enable** to start the program component. To disable it, click **Disable**.

See Note

4 Click **Properties** to open the VShield Properties dialog box, where you can set options that tell VShield how to perform each type of scan.

5 Click **Close** to close the VShield Status dialog box.

Related Topics

When one or more of VShield's modules are running, the icon appears in the system tray at the lower-right corner of your screen. You can enable or disable each of VShield's four modules independently of the others. You can also enable or disable VShield entirely. In that case, VShield continues running in memory but performs none of its "on-access" scanning functions. Its system tray icon changes to

.

Important: The terms "enabling" and "disabling" are not the same as "stopping" and "starting," which refer to closing a program component completely, so that it is neither functioning nor running in memory. For information about stopping and starting, see Unload and Reload VirusScan Components.

There are three ways to enable or disable VShield Modules:

Using the system tray shortcut menu:

1 Right-click in the system tray. A drop-down menu appears.
2 Select **Enable**. A sub-menu appears, listing the VShield modules. Modules that are enabled have a checkmark alongside them. Modules that are disabled have no checkmark.
   - To enable a module that has no checkmark, select it.
   - To disable a module that has a checkmark, select it.
   - If you disable all the modules, the system tray icon changes to

.

Using the System Scan Status screens:

1 Right-click in the system tray. A drop-down menu appears.
2 Select **Status**. The **Scan Status** screens appears, displaying a tab for each of the modules.
   Note: An alternative approach to displaying the **Scan Status** screen is to *double-click* the .
3 Select the tab representing the module you want to enable or disable. Each tab contains a button that reads **Enable**, if the module is currently disabled, or **Disable**, if the module is currently enabled.
   - To enable the module, click **Enable**.
   - To disable the module, click **Disable**.

Using the VShield Configuration Manager property pages:

1 Open the VShield Configuration Manager. See Navigate to the VShield Configuration Pages
2 Select the module that you want to enable or disable from the list on the left side of the screen. Near the top of the **Detection** tab for each module there is a checkbox that says **Enable** followed by the name of the module.
   - To enable the module, select the Enable checkbox.
   - To disable the module, clear the Enable checkbox.

When all of VirusScan's components are loaded into memory, two VirusScan icons appear in the system tray at the lower-right of your screen.

- The representing the McAfee VirusScan Scheduler
- The icon, if one or more VShield modules are enabled, or the icon, if none of the VShield modules is enabled.

Unloading the Scheduler or VShield removes them from memory. As a result, you cannot perform on-access or on-schedule scans. See Scanning: On-Access, On-Demand, or On-Schedule. However, this does not impair your ability to perform on-demand scans using VirusScan. See Perform a Classic On-Demand Scan.

Important: The terms "unloading " and "reloading" are synonymous, respectively, with "stopping" and "starting." These terms refer to closing a program component completely so that it is neither functioning nor running in memory. *But these terms are not the same as "disabling" and "enabling."* The latter terms refer to blocking performance of VShield modules but allowing them to continue running in memory. For more information, see Enable and Disable VShield or its Modules.

To unload Scheduler

- if it is not open, right-click in the system tray. A drop-down menu appears. Next, select **Exit. McAfee VirusScan Scheduler** is unloaded from memory and the icon disappears from the system tray.
- if it is already open, select **Exit** from the **Task** menu. **McAfee VirusScan Scheduler** is unloaded from memory and the icon disappears from the system tray**.**

To reload Scheduler

- Click **Start** on the bottom-left of your screen.
- Next, Select **Programs → McAfee VirusScan → McAfee VirusScan Scheduler.** The Scheduler is reloaded into memory and its icon reappears in the system tray.

To unload VShield

- From the system tray, right-click or . Next, select **Exit. McAfee VShield** is unloaded from memory and the icon disappears from the system tray.
- From the **Scheduler**, select **McAfee VShield** from the list of tasks. Next click . **McAfee VShield** is unloaded from memory and the icon disappears from the system tray.

To reload VShield

- Click **Start** on the bottom-left of your screen.
- Next, Select **Programs → McAfee VirusScan → McAfee VirusScan Scheduler.** The Scheduler opens.
- Then, select **McAfee VShield** from the list of tasks.
- Finally, click . **McAfee VShield** is reloaded into memory and its icon reappears in the system tray.

The VShield component includes four modules that you can configure in advance to perform scans each time a particular event occurs, such as opening a file or an e-mail attachment. Those modules are:

- System Scan (for On-Access scanning)
- E-mail Scan (for On-Access scanning)
- Download Scan
- Internet Filter.

You may configure each of these components yourself, or you may use the configuration **Wizard** to define their properties.

See Note

Using The Wizard:

1 Right-click the in the system tray at the bottom-right of your screen, in the same location as the current time.

2 From the menu, select **Properties**. Then, select **System Scan** or any of the other modules listed. The on-access property pages appear.

3 Click **Wizard** beneath the list of modules. The configuration **Wizard** appears.

4 Follow the on-screen instructions.

Configuring The Modules Yourself:

1 Right-click the in the system tray at the bottom-right of your screen, in the same location as the current time.

2 From the menu, select **Properties**. Then, select the module you want to configure. The on-access property pages appear, displaying the module you selected. See Navigating to the VShield Configuration Pages for information on alternative ways to access the **VShield** property pages.

3 Select options on each of the tabbed pages for the selected module, or select a different module from the list on the left side of the screen. Click a button for instructions on configuring each of the modules:

{button ,JI(`vscan4.HLP',`Configuring_System_Scan_Properties')} System Scan
{button ,JI(`vscan4.HLP',`Configuring_On_Access_E-Mail_Scan_Properties')} E-mail Scan
{button ,JI(`vscan4.HLP',`Configuring_Download_Scan_Properties')} Download Scan
{button ,JI(`vscan4.HLP',`Configuring_Internet_Filter_Properties')} Internet Filter
{button ,JI(`vscan4.HLP',`Configuring_VShield_Security_Properties')} Security

4 If you want to configure another module, select it from the box on the left side of the screen and repeat Step 3 until you are finished configuring.

5 When finished.

Click **Apply** to save the detection options you chose without leaving the **E-mail Scan** property page now visible, or

Click **OK** to save any changes you made in this or any other property page and close the VShield Properties dialog box, or

Click **Cancel** to close the dialog box without saving any changes.

Related Topics

1 Click **Start** on the bottom-left of your screen.

1 Select **Programs → McAfee VirusScan → VirusScan Central → VShield**. The VShield property pages appear.

{button ,JI(`vscan4.HLP>Third',`Navigate_to_the_VShield_Configuration_Pages')} Click for information on alternative approaches to accessing VShield property pages.

3 Select **E-mail Scan** from the program components shown on the left side of the VShield configuration screen.

The E-mail Scan configuration pages appear.

By default, the **Detection** tab is displayed.

4 Click the **Enable Scanning of e-mail attachments** checkbox. The rest of the property page is enabled.

5 Configure the properties on each of the tabbed pages.

See Note

{button ,JI(`vscan4.HLP',`Configuring_On_Access_E_mail_Scan_Detection_Properties')} Detection Tab

{button ,JI(`vscan4.HLP',`Configuring_On_Access_E_mail_Scan_Action_Properties')} Action Tab

{button ,JI(`vscan4.HLP',`Configuring_On_Access_E_mail_Scan_Alert_Properties')} Alert Tab

{button ,JI(`vscan4.HLP',`Configuring_On_Access_E_mail_Scan_Report_Properties')} Report Tab

Related Topics

Click a button for information specific to your e-mail software:

{button ,JI(`vscan4.HLP',`Configuring_a_Microsoft_Exchange_(MAPI)_E-mail_Client')} Microsoft Exchange (MAPI)

{button ,JI(`vscan4.HLP',`Configuring_Lotus_cc:Mail')} Lotus cc:Mail

{button ,JI(`vscan4.HLP',`Configuring_a_POP-3_Internet_Mail_Client')} POP-3 Internet Mail Client

The instructions here relate only to ***on-access scanning*** of e-mail received via a ***Microsoft Exchange or other MAPI compliant program***, including Microsoft Exchange v4.0, v5.0 and v5.5; Microsoft Outlook 97 and Outlook 98; and cc:Mail v8.0 and v8.01 (MAPI-compliant version only.)

- Other MAPI-compliant client software will most likely work correctly with VShield, but Network Associates does not certify VShield compatibility with client software not listed above.
- For information relating to ***on-demand scanning*** of e-mail, see Configuring On-Demand E-mail Scan Properties
- For information about ***on-access scanning*** of e-mail received via a ***POP-3 or proxy mail client*** such as America Online, Eudora Light, Netscape, and Outlook Express, see Configuring a POP-3 Internet Mail Client

Note: If your e-mail program is in a different network domain from the one you regularly log into for general purposes, you will have to provide your e-mail user identification and password each time you start or reboot your system.

1 Click the **Enable Scanning of e-mail attachments** checkbox.

2 Select the **Microsoft Exchange (MAPI)** checkbox.

3 Click **All new mail** or **Select Folder** to designate which e-mail should be scanned.

4 If you choose **Select Folder**, click **Browse** to select the folder containing the e-mail to be scanned.

5 Click one of the buttons in the **Attachments** section of the screen to indicate whether all e-mail attachments should be scanned, or only Program files.

6 If you select **Program files only**, click **Extensions** to view a list of file extensions that VirusScan will scan. You can edit the list.

7 Select the **Compressed files** checkbox to include files created with file compression utilities. See Scanning Compressed Files for more information. Because VirusScan decompresses these file types in memory before checking for viruses, this option can lengthen the time it takes to scan your e-mail.

8 Click **Apply** to save your changes without closing the dialog box. This completes the **Detection** property page.

9 Click another tab to continue.

See Note

Related Topics

On-demand e-mail scanning can be accessed using the toolbar or Tools menu of your MAPI-compliant e-mail program, such as Microsoft Outlook.

Select **Tools → E-mail Scan properties** or click . The **E-mail Scan Properties** pages appear.

Configure the properties on each of the tabbed pages.

{button ,JI(`vscan4.HLP',`Configuring_On_Demand_E_mail_Scan_Detection_Properties')} Detection Tab

{button ,JI(`vscan4.HLP',`Configuring_On_Demand_E_mail_Scan_Action_Properties')} Action Tab

{button ,JI(`vscan4.HLP',`Configuring_On_Demand_E_mail_Scan_Alert_Properties')} Alert Tab

{button ,JI(`vscan4.HLP',`Configuring_On_Demand_E_mail_Scan_Report_Properties')} Report Tab

Microsoft Exchange Users, see Note

1. Select the **Detection** tab. By default, this tab is active when you access the on-demand **E-mail Scan Properties** pages.
2. Select either **Scan all messages** or **Scan unread messages only**.
3. Click one of the buttons in the **Attachments** section of the screen to indicate whether all e-mail attachments should be scanned, or only Program files.
4. If you select **Program files only**, click **Extensions** to view a list of file extensions that on-demand e-mail scan will include in scanning. You can edit the list.
5. Select the **Compressed files** checkbox to include files created with file compression utilities. See Scanning Compressed Files for more information. Because VirusScan decompresses these file types in memory before checking for viruses, this option can lengthen the time it takes to scan your e-mail.
6. Click **Heuristics** to configure Heuristic Scanning.
7. Click **Apply** to save your changes without closing the dialog box. This completes the **Detection** property page.
8. Click another tab to continue.

Related Topics

1. Select the **Action** tab to specify how on-demand e-mail scan will respond when it detects a virus. By default**, Prompt for user action** appears as the selected response.
2. Click the down arrow if you want to select a different VirusScan response to virus detection. The display in the **Possible actions** varies in accordance with the response you select. If you leave the selected response as **Prompt for user action**, you will be given an opportunity to select any one of the possible actions each time a virus is detected. If you select one of the other options from the drop-down list, that option will operate automatically each time a virus is detected.
    - If you leave the selected response as **Prompt for user action**, clear the possible actions that you do not want to apply. Leave the checkmark for actions that you want to apply.
    - If you select **Clean infected attachment automatically**, VirusScan will attempt to remove the virus from the e-mail attachment. If the virus cannot be cleaned, you will receive a message indicating that the virus cannot be cleaned. Under those circumstances, McAfee suggests that you not attempt to access the infected file, but delete it instead. If necessary, contact the sender and request a copy of the attachment that is not infected.
    - If you select **Move infected attachment automatically**, you are asked to provide the location and name of a folder to receive the file.
    - If you select **Delete infected attachment automatically** or **Continue scanning** a message appears explaining your choice.
3. If you select **Prompt for user action** VirusScan needs to know how to prompt you: with an on-screen message, a beep, or both. By default, the message appearing in the text box will appear dimmed.
    - To change the message, select the **Display custom message** checkbox and type a new message.
    - To omit the beep, clear the **Sound audible alert** checkbox.
4. Click **Apply** to save your changes without closing the dialog box. This completes the **Action** property page.
5. Click another tab to continue.

- **See Note**
- Related Topics

1. Select the **Alert** tab if you want VirusScan to send a message when it detects a virus.
2. Select the **Send network alert** checkbox if you want an alert to be posted to a network server. The **Browse** button is activated and you can browse for a location for the network alert. When selected, the path to the location appears in the text box.
3. If you want to send e-mail alerts, select **Return reply mail to sender** and/or **Send alert mail to user**.
4. Click the **Configure** button corresponding to you choice(s) to designate the addressee(s) and set up the message.
5. Click **Apply** to save your changes without closing the dialog box. This completes the **Alert** property page.
6. Click another tab to continue.

See Note

Related Topics

1. Select the **Report** tab if you want VirusScan to maintain a log of its activities. By default, VirusScan creates a file called Mailscan.txt, having a maximum size of 100 KB, and recording all of the available report options shown on the screen. The default location of the log file is C:\Program Files\Network Associates\McAfee Virus Scan\. If you want to change these defaults, you may:
   - Clear the **Log to file** checkbox, thus disabling the logging activity.
   - Type a new name or path for the text file generated. VirusScan will only generate a file in plain text format.
   - Click **Browse** to select a location for the file.
   - Clear the **Limit size of log file** checkbox to remove any size restriction.
   - Change the maximum size of the log file.
   - Clear the checkboxes for any of the elements of the report that you are not interested in seeing.
2. Click **Apply** to save your changes without closing the dialog box. This completes the **Report** property page.
3. Click another tab to continue.

See Note

Related Topics

The **E-mail Scan** for on-demand e-mail scanning can be accessed using the toolbar or Tools menu of your MAPI-compliant e-mail program, such as Microsoft Outlook.

Select **Tools → Scan for Viruses** or click . The **E-mail Scan** progress screen appears and scanning activity begins immediately. Here you will find buttons that allow you to pause, stop and restart scanning activity.

See Note

Related Topics

The most recent version of Lotus cc:Mail is a MAPI-compliant e-mail program. Earlier versions are not MAPI-compliant.

- If you use Lotus cc:Mail 8, see Configuring a Microsoft Exchange (MAPI) E-mail Client
- If you use an earlier version of cc:Mail, it is necessary to perform a Custom installation of VirusScan, and select **Lotus cc:Mail** during the installation process. These instructions are applicable only under those circumstances.

1. Click the **Enable Scanning of e-mail attachments** checkbox.
2. Click the **Enable Corporate Mail** checkbox.
3. Select the **Lotus cc:Mail** radio button.
4. In the **Check every … Seconds** section, enter the frequency, in seconds, with which VShield should check for new mail. This should be about twice as frequently as your mail server checks for new mail.
5. Click one of the buttons in the **Attachments** section of the screen to indicate whether all e-mail attachments should be scanned, or only Program files.
6. If you select **Program files only**, click **Extensions** to view a list of file extensions that VirusScan will scan. You can edit the list.
7. Select the **Compressed files** checkbox to include files created with file compression utilities. See Scanning Compressed Files for more information. Because VirusScan decompresses these file types in memory before checking for viruses, this option can lengthen the time it takes to scan your e-mail.
8. Click **Apply** to save your changes without closing the dialog box. This completes the **Detection** property page.
9. Click another tab to continue.

See Note

Related Topics

The instructions here relate only to ***on-access scanning*** of e-mail received via a ***POP-3 or proxy mail client*** such as America Online, Eudora Light, Netscape, and Outlook Express.

- For information relating to on-access scanning of e-mail received via a ***Microsoft Exchange or other MAPI compliant program***, such as Microsoft Outlook, and including Lotus cc:Mail 8, see Configuring a Microsoft Exchange (MAPI) E-mail Client.
- The **Download Scan** module, not the **E-mail Scan** module, controls the scanning of attachments received via these programs. Selecting **Internet Mail** automatically enables **Download Scan**

1. Select the **Internet Mail** checkbox.
2. Clear the **Enable scanning of e-mail attachments** checkbox.
3. Click **Apply** to save your changes without closing the dialog box.
4. Select the Download Scan tab to configure the properties for downloaded files, including e-mail attachments received via a POP-3 client.

See Note
Related Topics

1. Select the **Action** tab to specify how VShield will respond when it detects a virus. By default**, Prompt for user action** appears as the selected response.
2. Click the down arrow if you want to select a different VShield response to virus detection. The display in the **Possible actions** varies in accordance with the response you select. If you leave the selected response as **Prompt for user action**, you will be given an opportunity to select any one of the possible actions each time a virus is detected. If you select one of the other options from the drop-down list, that option will operate automatically each time a virus is detected.
   - If you leave the selected response as **Prompt for user action**, clear the possible actions that you do not want to apply. Leave the checkmark for actions that you want to apply.
   - If you select **Move infected files to a folder**, you are asked to provide the location and name of a folder to receive the file.
   - If you select **Delete infected files** or **Continue scanning** a message appears explaining your choice.
3. If you select **Prompt for user action** VirusScan needs to know how to prompt you: with an on-screen message, a beep, or both. By default, the message appearing in the text box will appear dimmed.
   - To change the message, select the **Display custom message** checkbox and type a new message.
   - To omit the beep, clear the **Sound audible alert** checkbox.
4. Click **Apply** to save your changes without closing the dialog box. This completes the **Action** property page.
5. Click another tab to continue.

- **See Note**
- Related Topics

1. Select the **Alert** tab if you want VirusScan to send a message when it detects a virus.
2. Select the **Send network alert** checkbox if you want an alert to be posted to a network server. The **Browse** button is activated and you can browse for a location for the network alert. When selected, the path to the location appears in the text box.
3. If you want to send e-mail alerts, select **Return reply to sender** and/or **Send alert mail to user**.
4. Click the **Configure** button corresponding to your choice(s) to designate the addressee(s) and set up the message.
5. Click **Apply** to save your changes without closing the dialog box. This completes the **Alert** property page.
6. Click another tab to continue.

See Note

Related Topics

1. Select the **Report** tab if you want VirusScan to maintain a log of its activities. By default, VirusScan creates a file called WebEmail.txt, having a maximum size of 100 KB, and recording all of the available report options shown on the screen. The default location of the log file is C:\Program Files\Network Associates\McAfee Virus Scan\. If you want to change these defaults, you may:
   - Clear the **Log to file** checkbox, thus disabling the logging activity.
   - Type a new name or path for the text file generated. VirusScan will only generate a file in plain text format.
   - Click **Browse** to select a location for the file.
   - Clear the **Limit size of log file** checkbox to remove any size restriction.
   - Change the maximum size of the log file.
   - Clear the checkboxes for any of the elements of the report that you are not interested in seeing.
2. Click **Apply** to save your changes without closing the dialog box. This completes the **Report** property page.
3. Click another tab to continue.

- **See Note**
- Related Topics

To configure VirusScan for Windows 95 and Windows 98 to look for viruses attached to files on a local or network drive:

1 Click **Start** on the bottom-left of your screen.

2 Select **Programs → McAfee VirusScan → VirusScan Central → VShield**. The VShield property pages appear.

{button ,JI(`vscan4.HLP>Third',`Navigate_to_the_VShield_Configuration_Pages')} Click for information on alternative approaches to accessing VShield property pages.

3 Select **System Scan** from the program components shown on the left side of the configuration screen

- By default, this is the first screen when opening VShield's configuration feature
- The **Enable System Scan** checkbox is selected and the rest of the property page is enabled.
- If you do not want System Scan to scan local or network drives, clear the **System Scan** checkbox.
- If you want System Scan to scan local or network drives, configure the properties on each of the tabbed pages.

{button ,JI(`vscan4.HLP',`Configuring_System_Scan_Detection_Properties')} Detection Tab

{button ,JI(`vscan4.HLP',`Configuring_System_Scan_Action_Properties')} Action Tab

{button ,JI(`vscan4.HLP',`Configuring_System_Scan_Alert_Properties')} Alert Tab

{button ,JI(`vscan4.HLP',`Configuring_System_Scan_Report_Properties')} Report Tab

{button ,JI(`vscan4.HLP',`Configuring_System_Scan_Exclusion_Properties')} Exclusion Tab

Related Topics

1. By default, files are scanned when they are run, copied, created, or renamed. If you want to exclude any of these on-access trigger-events, clear its corresponding checkbox in the **Scan files on** section of the screen.
2. By default, the boot sector of a floppy disk is scanned when the floppy disk drive is accessed, and when the system is shut down. If you want to exclude either of these scanning trigger-events, clear its corresponding checkbox in the **Scan floppies on** section of the screen.
3. Click a button in the **What to scan** section of the screen to indicate whether all files should be scanned, or only Program files.
   - If you select **Program files only**, click **Extensions** to view a list of file extensions that VShield will scan. You can edit the list by clicking **Add** or **Delete**.
4. Select the **Compressed files** checkbox to include files created with file compression utilities. See Scanning Compressed Files for more information. Because VirusScan decompresses these file types in memory before checking for viruses, this option can lengthen the time it takes to complete a scan.
5. By default, System Scan loads when your system starts up—can be disabled—and is represented by an icon on the taskbar. You may change any of these options by clearing it in the **General** section of the screen.
6. Click **Heuristics** to configure Heuristic Scanning.
7. Click **Apply** to save your changes without closing the dialog box. This completes the **Detection** property page.
8. Click another tab to continue.

See Note

Related Topics

1 Select the **Action** tab to specify how VShield will respond when it detects a virus. By default**, Prompt for user action** appears as the selected response.

2 Click the down arrow if you want to select a different VShield response to virus detection. The display in the **Possible actions** varies in accordance with the response you select. : If you leave the selected response as **Prompt for user action**, you will be given an opportunity to select any one of the possible actions each time a virus is detected. If you select one of the other options from the drop-down list, that option will operate automatically each time a virus is detected.

- If you leave the selected response as **Prompt for user action**, clear the possible actions that you do not want to apply. Leave the checkmark for actions that you want to apply.
- If you select **Move infected files automatically**, you are asked to provide the location and name of a folder to receive the file.
- If you select **Clean infected files automatically**, **Delete infected files automatically**, or **Deny access to infected files and continue**, a message appears explaining your choice.

3 Click **Apply** to save your changes without closing the dialog box. This completes the **Action** property page.

4 Click another tab to continue.

- **See Note**
- Related Topics

1. Select the **Alert** tab if you want VShield to send a message when it detects a virus.
2. Select the **Send network alert** checkbox if you want an alert to be posted to a network server. The **Browse** button is activated and you can browse for a location for the network alert. When selected, the path to the location appears in the text box.
3. Select the **DMI Alert** checkbox to send notification to network management or desktop management applications that comply with the **D**esktop **M**anagement **I**nterface standard.
4. If you selected **Prompt for user action** on the **Action** tab, VShield needs to know how to prompt you: with an on-screen message, a beep, or both. By default, the message in the text box will appear dimmed.
   - To change the message, select the **Display custom message** checkbox and type a new message.
   - To omit the beep, clear the **Sound audible alert** checkbox.
5. Click **Apply** to save your changes without closing the dialog box. This completes the **Alert** property page.
6. Click another tab to continue.

See Note

Related Topics

1. Select the **Report** tab if you want VShield to maintain a log of its activities. By default, VShield creates a file called VSHLog.txt, having a maximum size of 100 KB, and recording all of the available report options shown on the screen. The default location of the log file is C:\Program Files\Network Associates\McAfee Virus Scan\. If you want to change these defaults, you may:
   - Clear the **Log to file** checkbox, thus disabling the logging activity.
   - Type a new name or path for the text file generated. VirusScan will only generate a file in plain text format.
   - Click **Browse** to select a location for the file.
   - Clear the **Limit size of log file** checkbox to remove any size restriction.
   - Set the maximum size of the log file to a value between 10 and 999.
   - Clear the checkboxes for any of the elements of the report that you are not interested in seeing.
2. Click **Apply** to save your changes without closing the dialog box. This completes the **Reports** property page.
3. Click another tab to continue.

- **See Note**
- Related Topics

1. Select the **Exclusion** tab to specify folders to exclude from virus scanning. By default, VShield does not scan files in the Recycled folder.
   - Select **Add** to specify a folder to be excluded. Your are given the option of including subfolders and specifying whether the exclusion is from file scanning or boot sector scanning.
   - Select **Edit** to modify the instructions pertaining to a selected folder already listed.
   - Select **Remove** to delete a selected folder from the list.
2. Click **Apply** to save your changes without closing the dialog box. This completes the **Exclusion** property page.
3. Click another tab to continue.

See Note
Related Topics

To configure VShield for Windows 95 and Windows 98 to look for viruses attached to files that you download from the Internet, including attachments to e-mail received via America Online mail, Microsoft Outlook Express, Qualcomm Eudora v4.x, Netscape Mail (included with most versions of Netscape Navigator and Netscape Communicator.

1 Click **Start** on the bottom-left of your screen.

1 Select **Programs → McAfee VirusScan → VirusScan Central → VShield**. The VShield property pages appear.

{button ,JI(`vscan4.HLP>Third',`Navigate_to_the_VShield_Configuration_Pages')} Click for information on alternative approaches to accessing VShield property pages.

3 Select **Download Scan** from the program components shown on the left side of the VShield configuration screen.

The Download Scan configuration pages appear.

By default, the **Detection** tab is displayed.

4 Click the **Enable Internet download scanning** checkbox. The rest of the property page is enabled.

See Note

{button ,JI(`vscan4.HLP',`Configure_Download_Detection_Properties')} Detection Tab

{button ,JI(`vscan4.HLP',`Configuring_Download_Action_Properties')} Action Tab

{button ,JI(`vscan4.HLP',`Configuring_Download_Alert_Properties')} Alert Tab

{button ,JI(`vscan4.HLP',`Configuring_Download_Report_Properties')} Report Tab

Related Topics

1 Click a button in the **Attachments** section of the screen to indicate whether all files should be scanned, or only Program files.

   If you select **Program files only**, click **Extensions** to view a list of file extensions that VirusScan will scan. You can edit the list.

2 Select the **Scan compressed files** checkbox to include files created with file compression utilities. See Scanning Compressed Files for more information. Because VirusScan decompresses these file types in memory before checking for viruses, this option can lengthen the time it takes to scan your downloaded files.

3 Click **Apply** to save your changes without closing the dialog box. This completes the **Detection** property page.

4 Click another tab to continue

See Note

Related Topics

1 Select the **Action** tab to specify how VShield will respond when it detects a virus. By default**, Continue scanning** appears as the selected response.

2 Click the down arrow if you want to select a different VShield response to virus detection. The display in the **Possible actions** varies in accordance with the response you select. If you leave the selected response as **Prompt for user action**, you will be given an opportunity to select any one of the possible actions each time a virus is detected. If you select one of the other options from the drop-down list, that option will operate automatically each time a virus is detected.

- If you leave the selected response as **Continue scanning,** a message appears explaining your choice.
- If you select **Prompt for user action**, clear the possible actions that you do not want to apply. Leave the checkmark for actions that you want to apply.
- If you select **Move infected files to a folder**, you are asked to provide the location and name of a folder to receive the file.
- If you select **Delete infected files**, or **Continue scanning**, a message appears explaining your choice

3 If you select **Prompt for user action** VShield needs to know how to prompt you: with an on-screen message, a beep, or both. By default, the message in the text box will appear dimmed.

- To change the message, select the **Display custom message** checkbox and type a new message.
- To omit the beep, clear the **Sound audible alert** checkbox.

4 Click **Apply** to save your changes without closing the dialog box. This completes the **Action** property page.

5 Click another tab to continue.

See Note

Related Topics

1. Select the **Alert** tab if you want VShield to send a message when it detects a virus.
2. Select the **Send network alert** checkbox if you want an alert to be posted to a network server. The **Browse** button is activated and you can browse for a location for the network alert. When selected, the path to the location appears in the text box.
3. Click **Apply** to save your changes without closing the dialog box. This completes the **Alert** property page.
4. Click another tab to continue.

See Note
Related Topics

1. Select the **Report** tab if you want VShield to maintain a log of its activities. By default, VShield creates a file called WebInet.txt, having a maximum size of 100 KB, and recording all of the available report options shown on the screen. The default location of the log file is C:\Program Files\Network Associates\McAfee Virus Scan\. If you want to change these defaults, you may:
   - Clear the **Log to file** checkbox, thus disabling the logging activity.
   - Type a new name or path for the text file generated. VShield will only generate a file in plain text format.
   - Click **Browse** to select a location for the file.
   - Clear the **Limit size of log file** checkbox to remove any size restriction.
   - Change the maximum size of the log file.
   - Clear the checkboxes for any of the elements of the report that you are not interested in seeing.
2. When you are finished configuring this and all other program components, click **OK**.
3. Click **Apply** to save your changes without closing the dialog box. This completes the **Report** property page.
4. Click another tab to continue.

See Note

Related Topics

The versions of Netscape Navigator and Microsoft Internet Explorer that have been tested and are known to work correctly with VShield are:

- Netscape Navigator v3.x, and v4.0.x, and v4.5.
- Microsoft Internet Explorer v3.x, and v4.x

To configure VShield to filter potentially dangerous Java and ActiveX objects, or to prohibit access to potentially risky Internet sites:

1. Click **Start** on the bottom-left of your screen.
2. Select **Programs → McAfee VirusScan → VirusScan Central → VShield.** The VShield property pages appear.

   {button ,JI(`vscan4.HLP>third',`Navigate_to_the_VShield_Configuration_Pages')} Click for information on alternative approaches to accessing VShield property pages.
3. Select **Internet Filter** from the program components shown on the left side of the VShield configuration screen.

   - The Internet Filter configuration pages appear.
   - By default, the **Detection** tab is displayed.
4. Click the **Enable Java & ActiveX filter** checkbox. The rest of the property page is enabled.
5. Configure the properties on each of the tabbed pages.

   {button ,JI(`vscan4.HLP',`Configuring_Internet_Filter_Detection_Properties')} Detection Tab

   {button ,JI(`vscan4.HLP',`Configuring_Internet_Filter_Action_Properties')} Action Tab

   {button ,JI(`vscan4.HLP',`Configuring_Internet_Filter_Alert_Properties')} Alert Tab

   {button ,JI(`vscan4.HLP',`Configuring_Internet_Filter_Report_Properties')} Report Tab

Related Topics

1. Select the **ActiveX Controls** checkbox and/or the **Java classes** checkbox to include them in the scan.
2. Click **Configure** next to **IP Addresses** if you want to prohibit access to a particular Internet IP address. If there are no IP addresses that you want to ban, clear the **IP Addresses to block** checkbox.
3. Click the **Configure** button next to **Internet Host Names to block** if you want to prohibit access to a particular Internet domain. If there are no domains that you want to ban, clear the **Internet Host Names to block** checkbox.
4. Click **Apply** to save your changes without closing the dialog box. This completes the **Detection** property page.
5. Click another tab to continue.

See Note

Related Topics

1. Select the **Action** tab to specify how VirusScan will respond when it detects a virus. By default**, Prompt for user action** appears as the selected response. Alternatively, if you would prefer not to be prompted for action when a virus is encountered in an ActiveX or Java feature, click the down arrow and select **Deny access to objects**.
2. If you select **Prompt for user action** VirusScan needs to know how to prompt you: with an on-screen message, a beep, or both. By default, the message in the text box will appear dimmed.
   - To change the message, select the **Display custom message** checkbox and type a new message.
   - To omit the beep, clear the **Sound audible alert** checkbox.
3. Click **Apply** to save your changes without closing the dialog box. This completes the **Action** property page.
4. Click another tab to continue

See Note

Related Topics

1. Select the **Alert** tab if you want VirusScan to send a message when it encounters a hostile Java applet, ActiveX control, or banned website..
2. Select the **Send network alert** checkbox if you want an alert to be posted to a network server. The **Browse** button is activated and you can browse for a location for the network alert. When selected, the path to the location appears in the text box.
3. Click **Apply** to save your changes without closing the dialog box. This completes the **Alert** property page.
4. Click another tab to continue

See Note
Related Topics

1. Select the **Report** tab if you want VirusScan to maintain a log of its activities. By default, VirusScan creates a file called WebFiltrl.txt, having a maximum size of 100 KB, and recording all of the available report options shown on the screen. The default location of the log file is C:\Program Files\Network Associates\McAfee Virus Scan\. If you want to change these defaults, you may:
   - Clear the **Log to file** checkbox, thus disabling the logging activity.
   - Type a new name or path for the text file generated. VirusScan will only generate a file in plain text format.
   - Click **Browse** to select a location for the file.
   - Clear the Limit size of log file checkbox to remove any size restriction.
   - Change the maximum size of the log file.
   - Clear the checkboxes for any of the elements of the report that you are not interested in seeing.
2. Click **Apply** to save your changes without closing the dialog box. This completes the **Report** property page.
3. Click another tab to continue

- **See Note**
- Related Topics

To configure VShield to password protect selected configuration pages to protect them from unauthorized changes:

1 Select **Security** from the program components shown on the left side of the configuration screen. The Security configuration pages appear. By default, the **Password** tab is displayed.

See Note

2 If you want to password protect all or some of the options, select **Enable password protection**.

3 You may select **Password-protect all options on all property pages**. In that case, no one can change any of the options that you have selected on any of the configuration pages without the password you designate. If you leave **Password-protect selected options only**, you may then designate password protected options for each of the program components: **System Scan**, **E-mail Scan**, **Download Scan**, and **Internet Filter**.

4 Enter a password.

5 Re-enter the password exactly as entered above.

6 Click **Apply** to save your password.

7 Select a tab representing a program component that contains options that you want to password protect. A list of option categories is displayed.

8 Select the pages to be password protected. The graphic representation of an open lock changes to a closed lock, indicating that the option is “locked down.”

9 When finished selecting options for the program category, click **Apply** to save your changes.

10 Repeat steps 6-8 for each program component until you have completed making your selections.

10 Click **OK**.

11 When you have finished configuring this and all other program components, click **OK**.

Related Topics

The virus “signatures ,” or characteristic code sequences, that VirusScan searches for generally appear only in files attached to e-mail messages, rather than in the messages themselves. Although code for a virus could appear in the text of an e-mail message, perhaps because of a mail transmission error, such a virus could not infect your computer system because e-mail software transmits messages as text. To function as a virus, the code sequence must be able to run as a program or as part of another program.

To detect viruses attached to your e-mail, access the appropriate E-mail Scan Property Page by following the instructions for on-demand e-mail scanning or for on-access e-mail scanning.

{button ,JI(`vscan4.HLP',`Detecting_E_Mail_Viruses_On_Demand')} For On-Demand Scanning

{button ,JI(`vscan4.HLP',`Detecting_E_Mail_Viruses_On_Access')} For On-Access Scanning

Related Topics

1 Click **Start** on the bottom-left of your screen.

1 Select **Programs → McAfee VirusScan → McAfee VirusScan Launcher → VShield**. The VShield property pages appear.

3 Select **E-mail Scan** in the components box on the left side of the configuration pages. The on-access E-mail Scan property pages appear.

4 Select the **Detection** tab. By default, this tab is active when you access the E-mail Scan property pages.

5 Select the **Enable Scanning of e-mail attachments** checkbox.

6 Select the button representing the type of e-mail system you use, MAPI or cc:Mail:

- If you use Lotus cc:Mail 8 select Microsoft Mail (MAPI.) Lotus cc:Mail 8 is MAPI-compliant.
- If you use AOL, Eudora Light, Netscape, or any other POP-3 or proxy mail client, use VirusScan's **Download Scan** component instead of the **E-mail Scan** component to configure your virus scanning preferences.

7 Tell VirusScan where, or how often to look for mail:

- If you use Microsoft Mail (MAPI):
  - Ø Click **All new mail**. to search for viruses in all e-mail message attachments as they reach your mailbox; or
  - Ø Click **Select Folder** to look for all message attachments in a specific location. Next, click **Browse** to choose the folder VirusScan should search.
- If you use Lotus cc:Mail, simply tell VirusScan how often it should scan incoming e-mail attachments for viruses. In the text box provided, enter the number of seconds, (at least 60 seconds) VirusScan should wait before performing a scan.

8 Tell VirusScan which attachments to scan:

- Choose **All attachments** to have VirusScan search for viruses in all files attached to e-mail messages. Although this option provides the best protection, it may have an impact on your computer's performance if you receive a large volume of e-mail.
- Choose **Program files only** to scan only for those attachments most susceptible to virus infection.
- Click **Extensions** to see or edit the list of file types to be scanned. The default list shows those file types that are most susceptible to virus infection.
- To change the list of file extensions VirusScan uses, see Add Program File Extension

9 Select the **Compressed files** checkbox to have VirusScan search files created with file compression utilities. See Scanning Compressed Files for more information. Because VirusScan decompresses these files in memory before scanning, this option can increase the time it takes to scan your e-mail.

10 When finished:

- Click **Apply** to save the detection options you chose without leaving the **E-mail Scan** property page, or.
- Click **OK** to save any changes you made in this or any other property page and close the VirusScan Properties dialog box, or
- Click **Cancel** to close the dialog box without saving any changes.

Related Topics

1 Open Microsoft Outlook, or other Microsoft Exchange e-mail client.

2 Select **Tools → E-mail Scan Properties** or click on the toolbar. The on-demand E-mail Scan property pages appear.

3 Tell VirusScan which attachments to scan:

- Choose **All attachments** to have VirusScan search for viruses in all files attached to e-mail messages. Although this option provides the best protection, it may have an impact on your computer's performance if you receive a large volume of e-mail.
- Choose **Program files only** to scan only for those attachments most susceptible to virus infection.
- Click **Extensions** to see or edit the list of file types to be scanned. The default list shows those file types that are most susceptible to virus infection.
- To change the list of file extensions VirusScan uses, see Add Program File Extension

4 Select the **Compressed files** checkbox to have VirusScan search files created with file compression utilities. See Scanning Compressed Files for more information. Because VirusScan decompresses these files in memory before scanning, this option can increase the time it takes to scan your e-mail.

5 When finished:

- Click **Apply** to save the detection options you chose without leaving the **E-mail Scan** property page, or.
- Click **OK** to save any changes you made in this or any other property page and close the VirusScan Properties dialog box, or
- Click **Cancel** to close the dialog box without saving any changes.

Related Topics

To tell VirusScan what to do about viruses it finds attached to your e-mail:

1 Access the appropriate E-mail Scan Property Page

For On-Access Scanning

§ Click **Start** on the bottom-left of your screen.

§ Select **Programs → McAfee VirusScan → McAfee VirusScan Launcher → VShield**. The VShield property pages appear.

§ Select **E-mail Scan** in the components box on the left side of the configuration pages. The on-access E-mail Scan property pages appear.

For On-Demand Scanning

§ Open Microsoft Outlook, or other Microsoft Exchange e-mail client.

§ Select **Tools → E-mail Scan Properties** or click on the toolbar.

§ The on-demand E-mail Scan property pages appear.

2 Select the **Action** tab.

3 Click to select a response. The options are:

Prompt for user action. When a virus is detected, VirusScan displays an alert box asking you how to handle the detected virus. Use this option if you want to decide how to handle each virus detected individually. If you want to handle all infected files in the same way, and automatically, choose a different option. If you are using cc:Mail, the action you take regarding the first virus detected applies to all subsequent virus detections during the current scanning session.

Move infected files automatically. VirusScan moves all infected file attachments to a quarantine folder that you designate.

Clean infected files automatically. This option is only available for on-demand e-mail scanning. VirusScan attempts to clean the virus and notifies you if it cannot be cleaned.

Delete infected files automatically. VirusScan deletes infected files when it detects them.

Continue scanning. VirusScan ignores infected files and proceeds with scanning.

4 Depending on your selection of response in Step 4, the display of **Possible actions** varies:

If you chose **Prompt for user action**, select the actions(s) you want to be able to take when a virus is detected.

- Next, select the **Alert** tab. The bottom portion of the screen, labeled **If 'Prompt for Action' is selected**, is active. The text box displays the default message VirusScan displays.
- Select Display custom message to edit the message.
- By default, VirusScan beeps when it prompts you for action. If you do not want to hear an audible beep, clear **Sound audible alert**.

If you chose **Move infected files automatically**, click **Browse** to select a folder for the quarantined file(s).

If you chose **Clean infected files automatically**, **Delete infected files automatically** or **Continue scanning**, a message appears explaining your choice.

5 When finished:

Click **Apply** to save the alert options you chose without leaving the **E-mail Scan** property page, or.

Click **OK** to save any changes you made in this or any other property page and close the E-mailScan Properties dialog box, or

Click **Cancel** to close the dialog box without saving any changes.

Related Topics

VirusScan for Windows 95 and Windows 98 offers you three ways to alert others about infected files that you have found in your e-mail. Click any of the topics below to learn how to

{button ,JI(`VScan4.hlp',`Notifying_sender_of_e_mail_infection')} Notify the person who sent you a message with an infected attachment

{button ,JI(`VScan4.hlp',`Notifying_othere_mail_users_aboutl_infection')} Notify other e-mail users about an infected attachment

{button ,JI(`VScan4.hlp',`Notifying_the_network_administrator_about_infected_e_mail')} Notify the network administrator about an infected attachment

To compose a standard reply to the person who sent you a message with an infected attachment:

1 Access the appropriate E-mail Scan Property Page

For On-Access Scanning

§ Click **Start** on the bottom-left of your screen.

§ Select **Programs → McAfee VirusScan → McAfee VirusScan Launcher → VShield**. The VShield property pages appear.

§ Select **E-mail Scan** in the components box on the left side of the configuration pages. The on-access E-mail Scan property pages appear.

For On-Demand Scanning

§ Open Microsoft Outlook, or other Microsoft Exchange e-mail client.

§ Select **Tools → E-mail Scan Properties** or click on the toolbar.

§ The on-demand E-mail Scan property pages appear.

2 Select the **Alert** tab.

3 Use the **E-mail alert** section located in the center portion of the screen.

4 Select **Return reply mail to sender**.

5 Click **Configure**. The **Return mail configuration** screen appears.

6 VirusScan automatically selects the sender as the addressee of the notification; identifies the virus and the affected file in the area immediately below the subject line.

7 To send a copy of this message to someone else, enter an e-mail address in the text box labeled **Cc:**, or click **Cc:** to choose a recipient from your mail system's user directory or address book

8 Enter any appropriate text in the **Subject** section and in the message section of the screen.

9 Click **OK** to save your message. You return to the **Alert** tab.

10 When finished:

Click **Apply** to save the detection options you chose without leaving the **E-mail Scan** property page, or.

Click **OK** to save any changes you made in this or any other property page and close the E-mailScan Properties dialog box, or

Click **Cancel** to close the dialog box without saving any changes.

Related Topics

To compose a warning about the infected e-mail attachment to the other e-mail users :

1 Access the appropriate E-mail Scan Property Page

For On-Access Scanning

§ Click **Start** on the bottom-left of your screen.

§ Select **Programs → McAfee VirusScan → McAfee VirusScan Launcher → VShield**. The VShield property pages appear.

§ Select **E-mail Scan** in the components box on the left side of the configuration pages. The on-access E-mail Scan property pages appear.

For On-Demand Scanning

§ Open Microsoft Outlook, or other Microsoft Exchange e-mail client.

§ Select **Tools → E-mail Scan Properties** or click on the toolbar.

§ The on-demand E-mail Scan property pages appear.

2 Select the **Alert** tab.

3 Use the **E-mail alert** section located in the center portion of the screen.

4 Select **Send alert mail to user**.

5 Click **Configure**. The **Send mail configuration** screen appears.

6 Enter an e-mail address in the text box labeled **To**, or click the button labeled **To** and choose a recipient from your mail system's user directory or address book. Virus scan identifies the virus and the affected file in the area immediately below the subject line.

7 To send a copy of this message to someone else, enter an e-mail address in the text box labeled **Cc:**, or click **Cc:** to choose a recipient from your mail system's user directory or address book.

8 Enter any appropriate text in the **Subject** section and in the message section of the screen.

9 Click **OK** to save your message. You return to the **Alert** tab.

10 When finished:

Click **Apply** to save the detection options you chose without leaving the **E-mail Scan** property page, or.

Click **OK** to save any changes you made in this or any other property page and close the VirusScan Properties dialog box, or

Click **Cancel** to close the dialog box without saving any changes.

Related Topics

VirusScan works in conjunction with a network server running Network Associates NetShield to notify your network system administrator whenever it detects a virus. The notification consists of a report form, or "network alert," that VirusScan generates automatically and sends to a specific location for NetShield to read.

1 Access the appropriate E-mail Scan Property Page

For On-Access Scanning

§ Click **Start** on the bottom-left of your screen.

§ Select **Programs → McAfee VirusScan → McAfee VirusScan Launcher → VShield**. The VShield property pages appear.

§ Select **E-mail Scan** in the components box on the left side of the configuration pages. The on-access E-mail Scan property pages appear.

For On-Demand Scanning

§ Open Microsoft Outlook, or other Microsoft Exchange e-mail client.

§ Select **Tools → E-mail Scan Properties** or click on the toolbar.

§ The on-demand E-mail Scan property pages appear.

2 Select the **Alert** tab.

3 Use the **Network alert** section located in the center portion of the screen.

4 Select **Send network alert**.

5 Click **Browse**. The **Browse for folder** dialog box appears.

6 Select the folder in which NetShield should look for warning messages.

7 Click **OK**. You return to the **Alert** tab.

8 When finished:

Click **Apply** to save the detection options you chose without leaving the **E-mail Scan** property page, or.

Click **OK** to save any changes you made in this or any other property page and close the E-mailScan Properties dialog box, or

Click **Cancel** to close the dialog box without saving any changes.

Related Topics

VirusScan can record the actions it takes when it scans for infected attachments, along with other information useful for tracking infections. The information is saved to a text file that you can open in any standard word processing software. Tracking information in a log file enables you to see the number of files VirusScan examined, determine which files carried viruses, and note the VirusScan settings you used to detect and respond to them. You should, therefore, activate this function.

1 Access the appropriate E-mail Scan Property Page

For On-Access Scanning

§ Click **Start** on the bottom-left of your screen.

§ Select **Programs → McAfee VirusScan → McAfee VirusScan Launcher → VShield**. The VShield property pages appear.

§ Select **E-mail Scan** in the components box on the left side of the configuration pages. The on-access E-mail Scan property pages appear.

For On-Demand Scanning

§ Open Microsoft Outlook, or other Microsoft Exchange e-mail client.

§ Select **Tools → E-mail Scan Properties** or click on the toolbar.

§ The on-demand E-mail Scan property pages appear.

2 Select the **Report** tab.

3 Select **Log to file**. The options on the screen are enabled. The text box displays the name of the activity log file. By default, the file is stored in the folder whose pathname is C:\Program Files\Network Associates\McAfee VirusScan.

4 If you want to designate a different filename or folder, click **Browse**. The **Activity Log Filename** dialog box appears.

5 Select the folder in which you want to save the log file:

- By default the log file for on-access e-mail scanning is called **WebEmail.txt**. For on-demand scanning, the log file is called **MailScan.txt**.
- You may change the name of the file by typing a new name in the **File name** box.
- Do not change the **.txt** filename extension shown in the **File of type box**.
- You may select a new folder. If the folder does not exist, you are prompted to create it.

7 Click **Open**. You return to the **Report** page. The pathname of the log file appears in the text box. When VirusScan stores data from a scanning operation in the log file, the file appears in the location to which you saved it. To view the log file, open it in any standard text editor, such as Notepad or WordPad.

8 To minimize the log file size, select the Limit size of log file to checkbox, then enter a value for the file size, in kilobytes, in the text box provided. The range available is from 10 kilobytes to 999 kilobytes.

9 Select the checkboxes beside each set of data you want VirusScan to collect and log.

10 Click **OK**. You return to the **Report** tab.

11 When finished:

- Click **Apply** to save the detection options you chose without leaving the **E-mail Scan** property page, or.
- Click **OK** to save any changes you made in this or any other property page and close the EmailScan Properties dialog box, or
- Click **Cancel** to close the dialog box without saving any changes.

Related Topics

VShield's Internet Download module can detect virus signatures that appear in files downloaded from the Internet. This includes attachments to e-mail messages downloaded from AOL, Eudora Light, Netscape, or any other POP-3 or proxy mail client. (If you use Microsoft Exchange (MAPI), or Lotus cc:Mail, use the **E-mail Scan** component instead of the **Download Scan** component to configure your preferences.)

1 Click **Start** on the bottom-left of your screen.

2 Select **Programs → McAfee VirusScan → VirusScan Central → VShield**. The VShield property pages appear.

{button ,JI(`vscan4.HLP>Third',`Navigate_to_the_VShield_Configuration_Pages')} Click for information on alternative approaches to accessing VShield property pages.

3 Select **Download Scan** in the components box on the left side of the configuration pages. The Download Scan property pages appear.

4 Select the **Enable Internet download scanning** checkbox.

5 Select the **Detection** tab. By default, this tab is active when you access the **Download Scan** property pages.

6 Tell VShield which files to scan:

- Choose **All files** to have VShield search for viruses in all downloaded files, and in all files attached to e-mail messages received via AOL, Eudora Light, Netscape, or any other POP-3 or proxy mail client. Although this option provides the best protection, it may have an impact on your computer's performance if you download a large number of files and/or receive a large volume of e-mail.
- Choose **Program files only** to scan only for those attachments most susceptible to virus infection.
- Click **Extensions** to see or edit the list of file types to be scanned. The default list shows those file types that are most susceptible to virus infection.
- To change the list of file extensions VShield uses, see Add Program File Extension.

7 Select the **Compressed files** checkbox to have VirusScan search files created with file compression utilities. See Scanning Compressed Files for more information. Because VirusScan decompresses these files in memory before scanning, this options can increase the time it takes to scan your download.

6 When finished:

- Click **Apply** to save the detection options you chose without leaving the **Download Scan** property page, or.
- Click **OK** to save any changes you made in this or any other property page and close the VShield Properties dialog box, or
- Click **Cancel** to close the dialog box without saving any changes.

Related Topics

To tell VShield what to do about viruses it finds in downloaded files:

1 Click **Start** on the bottom-left of your screen.

2 Select **Programs → McAfee VirusScan → VirusScan Central → VShield**. The VShield property pages appear.

{button ,JI(`vscan4.HLP>Third',`Navigate_to_the_VShield_Configuration_Pages')} Click for information on alternative approaches to accessing VShield property pages.

3 Select **Download Scan** in the components box on the left side of the configuration pages. The Download Scan property pages appear.

4 Select the **Action** tab.

5 Click to select a response. The options are:

Prompt for user action. When a virus is detected, VShield displays an alert box asking you how to handle the detected virus. Use this option if you want to decide how to handle each virus detected individually. If you want to handle all infected files in the same way, and automatically, choose a different option.

Move infected files to a folder. VShield moves all infected file attachments to a quarantine file that you designate.

Delete infected files. VShield deletes infected files when it detects them.

Continue scanning. VShield ignores infected files and proceeds with scanning.

6 Depending on your selection of response in Step 4, the display of **Possible actions** varies:

If you chose **Prompt for user action**, select the actions(s) you want to be able to take when a virus is detected.

- Next, select the **Alert** tab. The bottom portion of the screen, labeled **If 'Prompt for Action' is selected**, is active. The text box displays the default message VShield displays.
- Select **Display custom message** to edit the message.
- By default, VShield beeps when it prompts you for action. If you do not want to hear an audible beep, clear **Sound audible alert**.

If you chose **Move infected files to a folder**, click **Browse** to select a folder for the quarantined file.

If you chose **Delete infected files** or **Continue scanning**, a message appears explaining your choice.

7 When finished:

Click **Apply** to save the detection options you chose without leaving the **Download Scan** property page, or.

Click **OK** to save any changes you made in this or any other property page and close the VShield Properties dialog box, or

Click **Cancel** to close the dialog box without saving any changes.

Related Topics

VShield works in conjunction with a network server running Network Associates NetShield to notify your network system administrator whenever it detects a virus. The notification consists of a report form, or “network alert,” that VShield generates automatically and sends to a specific location for NetShield to read.

1 Click **Start** on the bottom-left of your screen.

1 Select **Programs → McAfee VirusScan → VirusScan Central → VShield**. The VShield property pages appear.

{button ,JI(`vscan4.HLP>Third',`Navigate_to_the_VShield_Configuration_Pages')} Click for information on alternative approaches to accessing VShield property pages.

3 Select **Internet Download** in the components box on the left side of the configuration pages. The Download Scan property pages appear.

4 Select the **Alert** tab.

5 Select **Send network alert**.

6 Click **Browse**. The **Browse for folder** dialog box appears.

7 Select the folder in which NetShield should look for warning messages.

8 Click **OK**. You return to the **Alert** tab.

9 When finished:

Click **Apply** to save the detection options you chose without leaving the **Download Scan** property page, or.

Click **OK** to save any changes you made in this or any other property page and close the VShield Properties dialog box, or

Click **Cancel** to close the dialog box without saving any changes.

Related Topics

VShield can record the actions it takes when it scans for infected attachments, along with other information useful for tracking infections. The information is saved to a text file that you can open in any standard word processing software. Tracking information in a log file enables you to see the number of files VShield examined, determine which files carried viruses, and note the VShield settings you used to detect and respond to them. You should, therefore, activate this function.

1 Click **Start** on the bottom-left of your screen.

1 Select **Programs → McAfee VirusScan → VirusScan Central → VShield**. The VShield property pages appear.

{button ,JI(`vscan4.HLP>Third',`Navigate_to_the_VShield_Configuration_Pages')} Click for information on alternative approaches to accessing VShield property pages.

3 Select **Download Scan** in the components box on the left side of the configuration pages. The Download Scan property pages appear.

4 Select the **Report** tab.

5 Select **Log to file**. The options on the screen are enabled. The text box displays the name of the activity log file. By default, the file is stored in C:\Program Files\Network Associates\McAfee VirusScan..

6 If you want to designate a different filename or folder, click **Browse**. The **Activity Log Filename** dialog box appears.

7 Select the folder in which you want to save the log file

- By default, the log file is called **WebInet.txt**
- You may change the name of the file by typing a new name in the File name box.
- Do not change the **.txt** filename extension shown in the **File of type box**.
- You may select a new folder. If the folder does not exist, you are prompted to create it.

7 Click **Open**. You return to the **Report** page. The pathname of the log file appears in the text box. When VShield stores data from a scanning operation in the log file, the file appears in the location to which you saved it. To view the log file, open it in any standard text editor, such as Notepad or WordPad.

8 To minimize the log file size, select the Limit size of log file to checkbox, then enter a value for the file size, in kilobytes, in the text box provided.

9 Select the checkboxes beside each set of data you want VirusScan to collect and log.

10 Click **OK**. You return to the **Report** tab.

11 When finished:

- Click **Apply** to save the detection options you chose without leaving the **Download Scan** property page, or.
- Click **OK** to save any changes you made in this or any other property page and close the VShield Properties dialog box, or
- Click **Cancel** to close the dialog box without saving any changes.

Related Topics

Java classes and ActiveX controls are small, special-purpose programs written in the Java programming language developed by Sun Microsystems or developed using Microsoft ActiveX technology. These programs, or "objects," often work as building blocks for constructing larger programs, or serve to add capabilities to existing programs. Many websites use Java classes or ActiveX controls to display animations or forms, run queries, and manipulate data.

Both technologies include safeguards designed to protect you from data loss or other types of harm. Nevertheless, determined programmers can exploit Java or ActiveX features to learn about the contents of your hard disk or corrupt your data. VirusScan for Windows 95 and Windows 98 includes a database of classes and controls known to cause harm, and can block their actions.

Related topics

To scan Java or ActiveX objects you encounter when visiting a website:

1 Click **Start** on the bottom-left of your screen.

2 Select **Programs → McAfee VirusScan → VirusScan Central → VShield.** The VShield property pages appear.

{button ,JI(`vscan4.HLP>Third',`Navigate_to_the_VShield_Configuration_Pages')} Click for information on alternative approaches to accessing VShield property pages.

3 Select **Internet Filter** in the components box on the left side of the configuration pages. The Internet Filter property pages appear.

4 Select the **Enable Java & ActiveX filter** checkbox.

5 Tell VirusScan which objects to scan.

- Select the **ActiveX Controls** checkbox to have it scan for harmful ActiveX or OCX controls.
- Select the **Java Classes** checkbox to have it scan Java classes, or applets written in Java.

6 When finished:

- Click **Apply** to save the detection options you chose without leaving the **E-mail Scan** property page, or.
- Click **OK** to save any changes you made in this or any other property page and close the VirusScan Properties dialog box, or
- Click **Cancel** to close the dialog box without saving any changes.

Related Topics

VShield gives you the choice to respond to potentially harmful objects:

1 Click **Start** on the bottom-left of your screen.

2 Select **Programs → McAfee VirusScan → VirusScan Central → VShield.** The VShield property pages appear.

{button ,JI(`vscan4.HLP>Third',`Navigate_to_the_VShield_Configuration_Pages')} Click for information on alternative approaches to accessing VShield property pages.

3 Select **Internet Filter** in the components box on the left side of the configuration pages. The Internet Filter property pages appear.

4 Select the **Enable Java & ActiveX filter** checkbox.

5 Click the **Action** tab.

6 Click to select a response. The options are:

- Prompt for user action.
- Deny access to objects.

7 If you chose **Prompt for user action**, select the **Alert** tab now. The bottom portion of the screen, labeled **If 'Prompt for Action' is selected**, is active. The text box displays the default message VShield displays.

- Select **Display custom message** to edit the message.
- By default, VirusScan beeps when it prompts you for action. If you do not want to hear an audible beep, clear **Sound audible alert**.

8 When finished:

- Click **Apply** to save the detection options you chose without leaving the **Internet Filter** property page, or.
- Click **OK** to save any changes you made in this or any other property page and close the VShield Properties dialog box, or
- Click **Cancel** to close the dialog box without saving any changes.

Related Topics

VShield works in conjunction with a network server running Network Associates NetShield to notify your network system administrator whenever it detects a virus. The notification consists of a report form, or “network alert,” that VirusScan generates automatically and sends to a specific location for NetShield to read.

1 Click **Start** on the bottom-left of your screen.

1 Select **Programs → McAfee VirusScan → VirusScan Central → VShield.** The VShield property pages appear.

{button ,JI(`vscan4.HLP>Third',`Navigate_to_the_VShield_Configuration_Pages')} Click for information on alternative approaches to accessing VShield property pages.

3 Select **Internet Filter** in the components box on the left side of the configuration pages. The Internet Filter property pages appear.

4 Select the **Alert** tab.

5 Select **Send network alert**.

6 Click **Browse**. The **Browse for folder** dialog box appears.

7 Select the folder in which NetShield should look for warning messages.

8 Click **OK**. You return to the **Alert** tab.

9 When finished:

- Click **Apply** to save the detection options you chose without leaving the **Internet Filter** property page, or.
- Click **OK** to save any changes you made in this or any other property page and close the VShield Properties dialog box, or
- Click **Cancel** to close the dialog box without saving any changes.

Related Topics

VShield can record the actions it takes when it encounters potentially harmful ActiveX or Java objects. The information is saved to a text file that you can open in any standard word processing software. Tracking information in a log file enables you to see the number of number and characteristics of objects examined, determine which objects were potentially harmful, and note the VShield settings you used to detect and respond to them. You should, therefore, activate this function.

1 Click **Start** on the bottom-left of your screen.

1 Select **Programs → McAfee VirusScan → VirusScan Central → VShield.** The VShield property pages appear.

{button ,JI(`vscan4.HLP>Third',`Navigate_to_the_VShield_Configuration_Pages')} Click for information on alternative approaches to accessing VShield property pages.

3 Select **Internet Filter** in the components box on the left side of the configuration pages. The Internet Filter configuration screens appear.

4 Select the **Report** tab.

5 Select **Log to file**. The options on the screen are enabled. The text box displays the name of the activity log file. By default, the file is stored in C:\Program Files\Network Associates\McAfee VirusScan.

6 If you want to designate a different filename or folder, click **Browse**. The **Activity Log Filename** dialog box appears.

7 Select the folder in which you want to save the log file

- By default the log file is called WebFiltr.txt
- You may change the name of the file by typing a new name in the File name box.
- Do not change the .txt filename extension shown in the File of type box.
- You may select a new folder. If the folder does not exist, you are prompted to create it.

8 Click **Open**. You return to the **Report** page. The pathname of the log file appears in the text box. When VShield stores data from a scanning operation in the log file, the file appears in the location to which you saved it. To view the log file, open it in any standard text editor, such as Notepad or WordPad.

9 To minimize the log file size, select the Limit size of log file to checkbox, then enter a value for the file size, in kilobytes, in the text box provided. The range available is from 10 KB to 999 KB.

10 Click **OK**. You return to the **Report** tab.

11 When finished:

- Click **Apply** to save the detection options you chose without leaving the **Internet Filter Scan** property page, or.
- Click **OK** to save any changes you made in this or any other property page and close the VirusScan Properties dialog box, or
- Click **Cancel** to close the dialog box without saving any changes.

Related Topics

If VirusScan detects a virus in memory, follow these steps:

1 Exit all programs and shut down your computer completely. Do not use the reset button or **Ctrl+Alt+Delete** to restart the computer.

2 Place the Emergency Diskette into the floppy disk drive. See Making and Using an Emergency Disk.

3 Turn on your computer.

4 Follow the on-screen instructions and remove any viruses found.

} If you receive the message **Traces of Virus in Memory**, see the additional information available at the Network Associates web page on this subject.

If VirusScan successfully removes all viruses from memory, shut down your computer, remove the emergency diskette, and then restart your computer. Restore the deleted file from a backup copy. As a precaution against reinfection, scan your diskettes immediately after inserting them into the floppy disk drive.

If VirusScan cannot remove a virus from memory, you will see the message **Virus could not be removed**. Perform a scan following the instructions found at Perform a Classic On-Demand Scanor Perform an Advanced On-Demand Scan. Select **Delete infected files automatically** on the **Action** tab.

OR

Perform a scan from the DOS command line using the command **SCAN /DEL**.

Having an Emergency Disk available for use is an essential part of an effective virus prevention program. If your system becomes infected, or if you cannot access your hard drive, or cannot load Windows, the Emergency Disk will, at a minimum, diagnose and resolve infections in the boot sector of your hard drive, enabling you to start your computer from a clean environment.

Use VirusScan's Emergency Disk utility to create an Emergency Disk. If you ever need to boot your computer from the Emergency Disk, Network Associates recommends that you perform a scan of your system and of the contents of your e-mail in-box immediately after starting your computer.

To create and Emergency Disk, follow these steps:

1 Have ready a formatted 3.5" high-density diskette containing the system files necessary to boot your PC.

There are two approaches to formatting a system diskette.

{button ,JI(`vscan4.HLP',`Formatting_a_Diskette_from_the_DOS_Command_Line')} From the **DOS Command Line**.

{button ,JI(`vscan4.HLP',`Formatting_a_Diskette_from_My_Computer_or_Windows_Explorer')} From **My Computer** or **Windows Explorer**

2 Click **Start** on the bottom left of your screen.

3 Select **Programs → McAfee VirusScan → McAfee VirusScan Central**. The McAfee launcher screen appears.

4 Click **Tools**. The utility toolbox appears.

5 Click **Emergency Disk**. The McAfee Emergency Disk Creation Utility screen appears.

6 Click **Continue**. You are instructed to insert the diskette into your computer's A: drive.

7 Click **OK**. The emergency disk utility scans the diskette for viruses and copies the files necessary to scan your system for viruses. A dialog box informs you when the process is done.

8 Click **OK**.

9 Remove the diskette from the A: drive, write-protect it, and label it **VirusScan Emergency Disk.**

10 Test the Emergency Disk by shutting down your system and restarting it while the Emergency Disk is in you floppy disk drive.

- This must be a cold reboot, meaning you must power off your system completely before restarting it.
- Do not use the **Restart** command from the **Start → Shut Down** menu.
- Do not use your computer's reset button.

Related Topics

Write-protecting a diskette makes it unlikely that the data on a diskette will be overwritten or damaged inadvertently. It also makes the diskette somewhat less vulnerable to viral infection since it will not accept additional data while write-protection is active.

To write-protect a 3.5" floppy disk:

1 Hold the diskette so that:

- the arrow indicating the direction for inserting the disk into the floppy drive is facing toward you.
- the side that accommodates a label faces away from you.

2 Find the small rectangular hole in the upper left corner of the diskette that has a plastic tab in it. If there is no tab present and the hole is open, the diskette is already write-protected.

3 Slide the plastic tab upward toward the edge of the diskette so that the hole is open. The disk is now write-protected.

Related Topics

Write-protecting a diskette makes it unlikely that the data on a diskette will be overwritten or damaged inadvertently. It also makes the diskette somewhat less vulnerable to viral infection since it will not accept additional data while write-protection is active.

To write-protect a 3.5" floppy disk:

1 Hold the diskette so that:

- the arrow indicating the direction for inserting the disk into the floppy drive is facing toward you.
- the side that accommodates a label faces away from you.

2 Find the small rectangular hole in the upper left corner of the diskette that has a plastic tab in it. If there is no tab present and the hole is open, the diskette is already write-protected.

3 Slide the plastic tab upward toward the edge of the diskette so that the hole is open. The disk is now write-protected.

Related Topics

The Launcher screen provides access to the main components of VirusScan for Windows 95 and Windows 98 as well as important information and tips about the status and configuration of the program and its components.

To access a component:

1 Click **Start** on the bottom-left of your screen.

1 Select **Programs → McAfee VirusScan → McAfee VirusScan Central.** The VirusScan Launcher appears.

3 Click **Scan** to configure and perform on-demand scanning. See Configuring VirusScan Properties for more information.

4 Click **VShield** to configure on-access scanning. The scanning activity occurs based on the trigger events and under the conditions you define. See Configuring System Scan Properties for more information.

5 Click **Schedule** to set a timetable for automatic scanning. See Scheduling On-Demand Scans and Tasks to Run Automatically for more information.

6 Click **Tools** to access:

- the **Submit to McAfee** Wizard, which facilitates notifying Network Associates of new viruses that you encounter.
- the **Emergency Disk** creation utility. See Making and Using an Emergency_Disk for more information.
- A list of the viruses recognized by your VirusScan software. See View a List of Viruses Currently Recognized by Your VirusScan Software for more information.

Related Topics

Messaging Application Programming Interface (MAPI)

MAPI is a Microsoft standard that governs how communications applications pass data back and forth between themselves. To install and work with MAPI-compliant applications, you must first set up Microsoft Messaging, a standard Windows component. To learn more, consult the documentation for Microsoft Exchange.

If you have found what you suspect to be a new or unidentified virus, send the infected file to McAfee Labs Anti-Virus Emergency Response Team for analysis using the **Submit to McAfee** Wizard. Please note that Network Associates reserves the right to use any information you supply as it deems appropriate without incurring any obligations whatsoever.

1 Click **Start** on the bottom-left of your screen.

2 Select **Programs → McAfee VirusScan → McAfee VirusScan Launcher.** The VirusScan Launcher appears.

3 Click **Tools.** The available tools menu appears.

4 Click to **Submit to McAfee.** The McAfee Labs A.V.E.R.T Wizard appears.

5 Click **Next**. A page appears on which you may type a message to the A.V.E.R.T team. If you want, include your personal contact information. This information is helpful, but optional.

6 Click **Next**. A submission list appears.

7 Click **Add** to select the file(s) to be submitted.

- Alternatively, you can drag and drop a file from **My Computer** or **Windows Explorer** to the list box.
- If you want to remove a file from the list, select it and click **Delete**.

8 Click **Next.** The **Choose Upload Options** page appears.

9 Select **Remove Data From File** if you want to preserve the confidentiality of your data.

10 If you are outside the United States, replace the default Network Associates e-mail address with the appropriate local e-mail address.

11 Click **Next**. The e-mail subsystem page appears.

- If required by your system configuration, select SMTP and enter the name of your SMTP server.
- Select Send mail through MAPI if you use a MAPI compliant mail server such as Microsoft Outlook.

12 Click **Finish** to submit the file.

{button ,JI(`vscan4.HLP',`Reporting_New_Viruses_or_Objects')} Click for additional information on reporting new viruses or dangerous objects.

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

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

Network Associates
Austria
Pulvermuehlstrasse 17
Linz, Austria
Postal Code A-4040
Phone: 43-732-757-244
Fax: 43-732-757-244-20

Network Associates
Belgium
Bessenveldtstraat 25a
Diegem
Belgium - 1831
Phone: 32-2-716-4070
Fax: 32-2-716-4770

Network Associates
do Brasil
Rua Geraldo Flausino Gomez 78
Cj. - 51 Brooklin Novo - São Paulo
SP - 04575-060 - Brasil
Phone: (55 11) 5505 1009
Fax: (55 11) 5505 1006

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

Network Associates
People's Republic of China
New Century Office Tower, Room 1557
No. 6 Southern Road Capitol Gym
Beijing
People's Republic of China 100044
Phone: 8610-6849-2650
Fax: 8610-6849-2069

NA Network Associates
Oy
Kielotie 14 B
01300 Vantaa
Finland
Phone: 358 9 836 2620
Fax: 358 9 836 26222

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

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

Network Associates Hong Kong
19/F, Matheson Centre
3 Matheson Street
Causeway Bay
Hong Kong
Phone: 852-2832-9525
Fax: 852-2832-9530

Network Associates Srl
Centro Direzionale Summit
Palazzo D/1

Network Associates Japan, Inc.
Toranomon 33 Mori Bldg.
3-8-21 Toranomon Minato-Ku

Via Brescia, 28
20063 - Cernusco sul Naviglio (MI)
Italy
Phone: 39 (0)2 9214 1555
Fax: 39 (0)2 9214 1644

Tokyo 105-0001 Japan
Phone: 81 3 5408 0700
Fax: 81 3 5408 0781

Network Associates
Latin America
150 South Pine Island Road, Suite 205
Plantation, Florida 33324
United States
Phone: (954) 452-1731
Fax: (954) 236-8031

Network Associates
de Mexico
Andres Bello No. 10, 4 Piso
4th Floor
Col. Polanco
Mexico City, Mexico D.F. 11560
Phone: (525) 282-9180
Fax: (525) 282-9183

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

Network Associates
Portugal
Rua Gen. Ferreira Martins, 10-6°c
1495 Algés
Portugal
Phone: 351 1 412 1077
Fax: 351 1 412 1488

Net Tools Network Associates
South Africa
Bardev House, St. Andrews
Meadowbrook Lane
Epson Downs, P.O. Box 7062
Bryanston, Johannesburg
South Africa 2021
Phone: 27 11 706-1629
Fax: 27 11 706-1569

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

Network Associates
Spain
Orense 4, 4th Floor
Edificio Trieste
28020 Madrid
Spain
Phone: 34 91 598 18 00
Fax: 34 91 556 14 01

Network Associates
Sweden
Datavägen 3A
Box 596
S-175 26 Järfälla
Sweden
Phone: 46 (0) 8 580 100 00
Fax: 46 (0) 8 580 100 05

Network Associates
AG
Baeulerwisenstrasse 3
8152 Glattbrugg
Switzerland

Network Associates
International Ltd.
Minton Place, Victoria Street
Windsor, Berkshire
SL4 1EF

Phone: 0041 1 808 99 66
Fax: 0041 1 808 99 77

United Kingdom
Phone: 44 (0)1753 827 500
Fax: 44 (0)1753 827 520

Related Topics

Note

Use the Download Scan page to have VirusScan examine mail you receive via America Online, Eudora Light, Netscape, Internet Explorer or other supported mail client applications. If you use VirusScan from home, the settings on this page will meet most of your e-mail scanning needs.

Use the E-mail Scan page to scan mail you receive via cc:Mail, Microsoft Exchange, or other MAPI -compliant mail programs. Usually, but not always, you will use these mail programs to receive mail over a local-area network or in a similar environment.

Lotus cc:Mail 8 is MAPI-compliant. Earlier versions are not.

Note

At any time you may:

- click **OK** at the bottom of the screen to save your changes and close the dialog box, or
- click **Cancel** to close the dialog box without saving your changes, or
- click **Apply** to save your changes but leave the dialog box open.

Note

Network Associates cannot guarantee that future data file releases will remain compatible with earlier versions of its products.

Note

Network Associates suggests that you use a site's URL designation, rather than its IP address, to add it to VirusScan's *banned* list. URL addresses are generally a more reliable way to keep track of a site's actual location on the Internet than a fixed IP address is, because the domain name server system gives you access to a site's current IP address even when it has changed or moved.

Note

You must have a dial-up or direct-access Internet account with a service provider in order to link to Network Associates. Contact an Internet service provider to obtain account information.

Note

Contact each vendor directly to learn more about access options using file transfer protocol (FTP) client software or other ways to obtain browser software.

Note

Your access to these updates is legally restricted by the maintenance terms outlined in the README.1ST file accompanying the software or detailed in the software license agreement.

Note

If the program component is active, the button reads **Disable**. If the program component is inactive, the same button reads **Enable**.

Using the button to enable or disable a program component is equivalent to selecting or clearing the **Enable** checkbox on the component's property page.

Note

To change the options associated with an item already included in the list, select the item and click **Edit**. The **Edit Scan Item** screen appears.

To delete an item from the list, select the item and click **Remove**.

Note

There are two other ways to copy a task:

1 Select a task. Next, select menu choice **Edit → Copy**. Then select menu **Edit → Paste**.

OR

2 Select a task. Next, press **Ctrl + C** on your keyboard. Then press **Ctrl +V**.

Note

These instructions do not apply to VirusScan on-demand scans, (scan32.exe). To configure on-demand scans, see Configuring VirusScan Properties

To format a diskette for use as an Emergency Disk using the DOS command line:

1 Place a diskette in your computer's **A** drive.

2 Click **Start** on the bottom-left of your screen.

3 Select **Programs**.

4 Select **MS-DOS Prompt**. The DOS command-line screen appears displaying **C:\Windows** as the current directory.

5 Type **FORMAT A:/S /U** and press **Enter**. DOS formats the diskette and copies the necessary system files to it.

6 When the formatting is complete and the **C:\ Windows** prompt is displayed, type **EXIT** to close the MS-DOS command-line screen.

Related Topics

Note

If you receive e-mail via America Online, Eudora Light, Netscape Mail, or other POP-3 or proxy mail clients, you must enable **Download Scan** if you want to scan e-mail attachments.

Note

Some Microsoft Exchange mail clients may not display the toolbar icons. However, the **E-mail Scan Properties** and **Scan for viruses** options are still available on the application's **Tools** menu.

If Microsoft Exchange is your e-mail client, on-demand e-mail scanning will be unavailable if VirusScan is installed before Microsoft Exchange. If you want to install Microsoft Exchange after you have installed VirusScan:

1 Uninstall VirusScan.
2 Install Microsoft Exchange.
3 Reinstall VirusScan.

Note

The update procedure includes options for upgrading your VirusScan software as well.

To format a diskette for use as an Emergency Disk using **My Computer** or **Windows Explorer**:

1. Place a diskette in your computer's **A** drive.
2. Using **My Computer** or **Windows Explorer**, select the **A** drive.
3. Right-click and select **Format**. The **Format** dialog box appears.
4. In the **Format type** portion of the dialog box, select **Full**.
5. In the **Other options** portion of the dialog box, select **Copy system files**.
6. Click **Start**. Windows formats the diskette and copies the necessary system files to it.

Related Topics

There are three ways to access the VShield property configuration pages.

From the VirusScan Launcher:

1. Click **Start** on the bottom-left of your screen.
2. Select **Programs → McAfee VirusScan → VirusScan Central → VShield.** The VShield property pages appear.

From the VShield Status pages:

1. Right-click the in the system tray at the bottom-right of your screen, in the same location as the current time.
2. Select **Status**. The **VShield Status** screen appears.
3. Click **Properties**. The **VShield** property pages appear.

From the Properties menu

1. Right-click the in the system tray at the bottom-right of your screen.
2. Select **Properties**. A sub-menu appears from which you may select the particular property page you want to view.

From the Scheduler:

1. Click **Start** on the bottom-left of your screen.
2. Select **Programs → McAfee VirusScan → VirusScan Central → Schedule**. The Virus Scan Scheduler appears.
3. Select **McAfee VShield** from the list of tasks.
4. Click . The **VShield** property pages appear.

   Note: Alternatively, *double-click* the in the system tray at the bottom-right of your screen. Then proceed with steps 3 and 4.

Boot Sector

The boot sector is the first logical division of a hard or floppy disk. Your computer's BIOS looks here soon after you turn it on to find the files and programs it needs to start operations.

Boot Virus

A boot virus copies itself from the boot sector of one drive to that of another (e.g., from a floppy disk to a hard disk).

Trojan

A program whose features appear to be innocent or beneficial, but which contain a damaging payload. These are not viruses. They do not replicate. They are also called “Trojan Horses.”

File Virus

A file virus attaches itself to an executable program. Whenever the program runs, the virus attaches itself to other executable programs.

Stealth Virus

A stealth virus hides itself to evade detection. A stealth virus may be either a boot virus or a file virus.

Multi-partite Virus

A multi-partite virus acts like both a boot virus and a file virus by spreading through disk boot sectors and executable files.

Mutating Virus

Mutating viruses change their code signature to avoid detection. Many mutating viruses are also encrypted viruses.

Encrypted Virus

Encrypted viruses encrypt part of their code signature to avoid detection. Many encrypted viruses are also mutating viruses.

Polymorphic Virus

Polymorphic viruses act somewhat like mutating viruses, but each time a polymorphic virus copies itself, it changes its code signature slightly to avoid detection.

Macro Virus

A virus written in a macro language or attached to macros included in a program's data files. Microsoft Word and Microsoft Excel data files and template files, for example, can include such viruses.

See Heuristic Scanning for information on evaluating the probability that a macro in a Microsoft Office application is a virus.

Uniform Resource Locator

One of the standard methods of specifying the location of an object on the Internet. In VirusScan for Windows 95 and Windows 98, URLs are also referred to as **Host Names** or **Domains**.

www.nai.com/ is an example of a Uniform Resource Locator.

Another method of locating an Internet site employs the IP Address.

IP Address

The Internet host address defined by the **I**nternet **P**rotocol. It is usually represented in dotted decimal notation.
128.121.4.5. is an example of an IP address.
Another method of locating an Internet site employs its URL.

Scanning Session

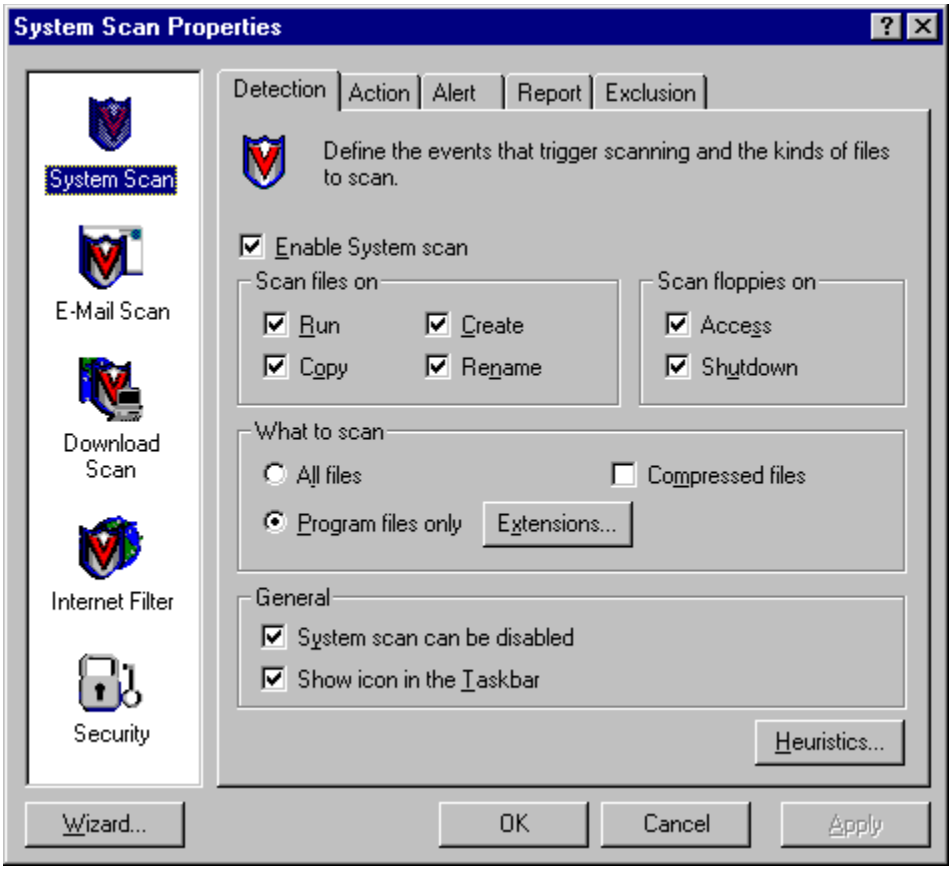
The period of time VirusScan remains active in your computer's memory. A scanning session ends when you quit VirusScan or restart your computer.

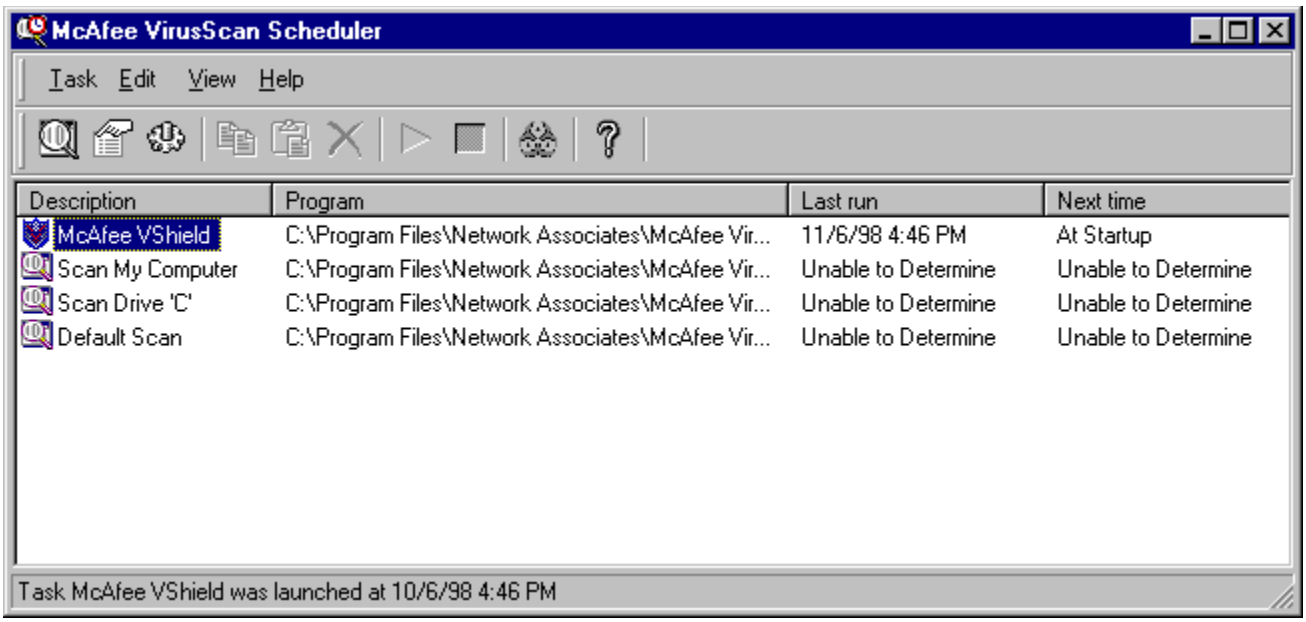
Virus Signature

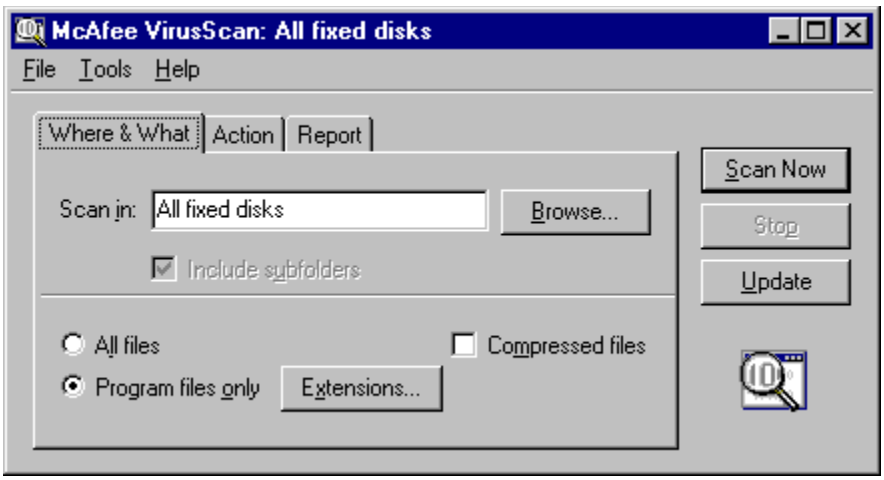
The code sequences that are characteristic of viruses. VirusScan searches for these strings. They can be found in executable files, such as those that might be downloaded from the Internet, or attached to an e-mail message. To function as a virus, the code sequence must be able to run as a program or as part of another program.

OCX

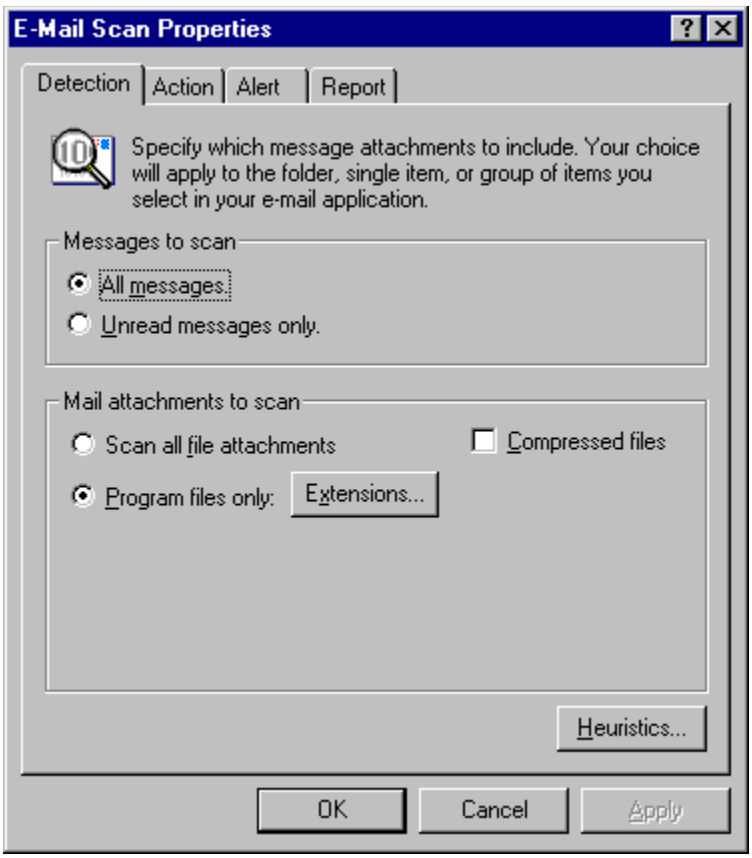
An ActiveX control that incorporates a user interface.


System Scan Properties
System Scan
E-Mail Scan
Download Scan
Internet Filter
Security
Detection
Action
Alert
Report
Exclusion
Define the events that trigger scanning and the kinds of files to scan.
Enable System scan
Scan files on
Run
Create
Copy
Rename
Scan floppies on
Access
Shutdown
What to scan
All files
Compressed files
Program files only
Extensions...
General
System scan can be disabled
Show icon in the Taskbar
Heuristics...
Wizard...
OK
Cancel
Apply


McAfee VirusScan Scheduler
Task Edit View Help
Description Program Last run Next time
McAfee VShield C:\Program Files\Network Associates\McAfee Vir... 11/6/98 4:46 PM At Startup
Scan My Computer C:\Program Files\Network Associates\McAfee Vir... Unable to Determine Unable to Determine
Scan Drive 'C' C:\Program Files\Network Associates\McAfee Vir... Unable to Determine Unable to Determine
Default Scan C:\Program Files\Network Associates\McAfee Vir... Unable to Determine Unable to Determine
Task McAfee VShield was launched at 10/6/98 4:46 PM


McAfee VirusScan: All fixed disks
File
Tools
Help
Where & What
Action
Report
Scan in:
All fixed disks
Browse...
Include subfolders
All files
Compressed files
Program files only
Extensions...
Scan Now
Stop
Update

Scan
VShield
Schedule
Tools
VirusScan
MCAFEE
Update
Since Last
Update


E-Mail Scan Properties
Detection
Action
Alert
Report
Specify which message attachments to include. Your choice will apply to the folder, single item, or group of items you select in your e-mail application.
Messages to scan
All messages
Unread messages only.
Mail attachments to scan
Scan all file attachments
Compressed files
Program files only:
Extensions...
Heuristics...
OK
Cancel
Apply

Depending on your selection of frequency in the **Run** portion of the screen, this portion of the screen displays appropriate clock and calendar choices from which you may choose.

- Enter the time, number of minutes, day of the month, and year, as appropriate.
- Enter clock times based on a 24-hour clock. If you want the task to run at 9:30 p.m., enter **21:30**.
- Names of months can be selected from a drop-down list.
- Names of days can be selected from drop-down lists or selected by clicking corresponding buttons.

Click this button to locate and select the scanning program file, Scan32.exe. After you select it, the path to the file appears in the text box.

Click this button to locate and select the folder containing the scanning program file, Scan32.exe. After you select it, the path to the file appears in the text box.

Click this button to configure the task.

Click this button to perform the selected task now, based on the properties and configuration options selected.

- If the selected task is a scan and you selected the **Start Automatically** checkbox on the VirusScan Detection property page, the scan will begin immediately. (See Help topic **Configuring VirusScan On-Demand Detection Properties for details**.)
- If the selected task is a scan but you did not select **Start Automatically**, the on-demand scanning screen is launched. You can then start scanning from there.

Click this button to stop a scan that is in progress.

The program may run in a normal window, a maximized window, or a minimized window. Click the to select one of these options.

Displays the description of the selected task. To change the description, edit the contents of the text box and click **Apply**. Click **OK** to see the description change in the **Scheduler** screen.

Use this text box to specify additional parameters that you want to apply to the execution of the file. This box may be left blank.

This window displays the path to the scanning program file, Scan32.exe. If you have installed VirusScan for Windows 95 and Windows 98 to a location different from the default installation location, click **Browse** to locate and select the file.

This window displays the path to the folder containing the scanning program file, Scan32.exe. If you have installed VirusScan for Windows 95 and Windows 98 to a location different from the default installation location, click **Browse** to locate and select the folder containing the Scan32.exe file.

Click this button to enable **VShield**, the on-access scanning component

Click this button to disable **VShield**, the on-access scanning component

Click this button to set a password for protecting Update and Upgrade options.

Select this checkbox to enable scheduling of the task selected on the **Scheduler** screen.

Select this button if you want the scan to take place every hour. The **Start at** portion of the screen allows you to set the number of minutes past the hour for the scan to start.

Select this button if you want the scan to take place once a day. The **Start at** portion of the screen allows you to set the days of the week and the hour for the scan to start.

Select this button if you want the scan to take place once a day. The **Start at** portion of the screen allows you to set the day of the week and the hour for the scan to start.

Select this button if you want the scan to take place once a month. The **Start at** portion of the screen allows you to set the day of the month and the hour for the scan to start.

Displays the pathname of the last file scanned before you opened the Task Properties dialog box.

Specifies the next time the selected task will run, based on the choices you made on the **Schedule** tab.

Specifies the last time the selected task ran.

Displays the number of infected items that VShield had detected as of the moment that you opened the Task Properties dialog box.

Displays the number of infected files that VShield had cleaned as of the moment that you opened the Task Properties dialog box..

Displays the number of infected files that VShield had deleted as of the moment that you opened the Task Properties dialog box..

Displays the number of infected files that VShield had moved to a quarantine folder as of the moment that you opened the Task Properties dialog box.

Displays the number of files that VShield had scanned as of the moment that you opened the Task Properties dialog box.

Select the frequency of the scheduled scan. Depending on your selection, the **Start at** portion of the screen displays appropriate clock and calendar choices from which you may choose.

When finished examining virus information, click this button to close the dialog box.

Displays the name of the selected virus.

Displays the kinds of files susceptible to this virus.

Displays the number of bytes occupied by the virus.

- Some viruses are retained in memory after they run, continuing to affect other files.

VirusScan selects this box if the virus encrypts part of its code signature to avoid detection.

VirusScan selects this box if the virus avoids detection by changing its code signature slightly each time it copies itself.

VirusScan selects this box if the virus can be cleaned.

VirusScan selects this box if the virus is written in a macro language or attached to macros included in a program's data files. Microsoft Word and Microsoft Excel data files and template files, for example, can include such viruses.

Click this button to move to the previous virus on the list.

Click this button to move to the next virus on the list.

Displays the pathname of the last local or network file scanned.

Displays the number of local or network files that VShield has scanned during the scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Displays the number of local or network files in which VShield has detected a virus during the scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Displays the number of infected files that VShield has cleaned during scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Displays the number of infected local or network files that VShield has deleted during the scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Displays the number of infected local or network files that VShield has moved to a quarantine folder during the scanning activity now in progress.
If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Click this button to enable or disable this program component.
If the component is running, the button reads **Disable**. If the component is idle, the button reads **Enable**.

Click this button to configure VShield property pages.

Click to close this dialog box.

Displays the IP address for the last web or Internet site that VShield had examined as of the moment you opened the Task Properties dialog box.

Displays the IP address for the last web or Internet site that VShield has examined during the scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Displays the name of the last Java class or ActiveX control that VShield had examined as of the moment you opened the Task Properties dialog box.

Displays the name of the last Java class or ActiveX control that VShield has examined during the scanning activity now in progress.

If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.!

Displays the number of Java applets that VShield had examined as of the moment that you opened the Task Properties dialog box.

Displays the number of Java applets that VShield has examined during the scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.!

Displays the number of Java applets that VShield had banned as of the moment that you opened the Task Properties dialog box.

Displays the number of Java applets that VShield has banned during the scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Displays the number of ActiveX controls that VShield had examined as of the moment that you opened the Task Properties dialog box.

Displays the number of ActiveX controls that VShield has examined during the scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Displays the number of ActiveX controls that VShield had banned as of the moment that you opened the Task Properties dialog box.

Displays the number of ActiveX controls that VShield has banned during the scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Displays the number of Internet sites that VShield had examined as of the moment that you opened the Task Properties dialog box.

Displays the number of Internet sites that VShield has examined during the scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Displays the number of Internet sites to which VShield had banned access as of the moment that you opened the Task Properties dialog box.

Displays the number of Internet sites to which VShield has banned access during the scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Click this button to enable or disable this program component.
If the component is running, the button reads **Disable**. If the component is idle, the button reads **Enable**.

Click this button to configure VShield property pages.

Click to close this dialog box.

Displays the number of mail items that VShield has examined during the scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Displays the number of e-mail items that VShield has found to be infected during the scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan

Displays the number of infected e-mail items that VShield has deleted during the scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Displays the number of infected e-mail items that VShield has moved to a quarantine folder during the scanning activity now in progress.
If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Click this button to enable or disable this program component.
If the component is running, the button reads **Disable**. If the component is idle, the button reads **Enable**.

Click this button to configure VShield property pages.

Click this button to close this dialog box.

Displays the last downloaded Internet file that VShield has examined during the scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Displays the number of downloaded Internet files that VShield has examined during the scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Displays the number of downloaded Internet files that VShield has found to be infected during the scanning activity now in progress.
If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Displays the number of infected downloaded Internet files that VShield has deleted during the scanning activity now in progress. If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Displays the number of infected downloaded Internet files that VShield has moved to a quarantine folder during the scanning activity now in progress.

If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

Click this button to enable or disable this program component.
If the component is running, the button reads **Disable**. If the component is idle, the button reads **Enable**.

Click this button to configure VShield property pages.

Click this button to close this dialog box.

Click this button to close the Virus List dialog box.

Click this button to view detailed information about the selected virus.

Click this button to locate a particular virus in the list of viruses.

Scroll to view the entire list of virus definitions currently defined in your system’s .DAT files.

Displays the identification number of the virus definition files your system is using.

Displays the date on which your system’s virus definition file was created.

Displays the version of the virus scan engine that your system is currently using.

Select this checkbox to record the date and time the scanning session began.
Clear this checkbox to disable recording of date and time.

Select this checkbox to record the names of any virus strains that VirusScan finds during a scanning session, and the number of times it finds them.

Clear this checkbox to disable logging of virus strains.

Select this checkbox to record the number of infected files VShield cleaned during a scanning session. Clear this checkbox to disable logging of virus cleaning.

Select this checkbox to record the number of infected files VShield deletes during a scanning session. Clear this checkbox to disable logging of infected file deletion.

Select this checkbox to record the number of infected files VShield moved to a quarantine directory during a scanning session. Clear this checkbox to disable logging of infected file relocation.

Select this checkbox to record the settings you chose for this scanning session.
This information is written to the designated log file when the scanning program is unloaded or you shut your system down.

Clear this checkbox to disable logging of session settings.

Select this checkbox to generate a summary of VShield's actions during this scanning session, including:

- The number of files examined for viruses.
- The number of infected files cleaned.
- The number of infected files deleted.
- The number of infected files moved.
- Other information about your VShield settings.
- Clear this checkbox to disable logging of session summary information.

These data are written to the designated log file when the scanning program is unloaded or you shut your system down.

Clear this checkbox to disable logging of session summary information.

Select this checkbox to record the date and time the scanning session began.
Clear this checkbox to disable recording of date and time.

Select this checkbox to record the name of the user who performed the scan.
Clear this checkbox to disable recording of the user's name.

Select the VShield property pages that you want to protect from unauthorized changes.

You may select all property pages in the list box or any individual option. A appears to the left of protected pages.

Click this button to save your changes and close the dialog box.

Click this button to close the dialog box without saving your changes.

Click this button to enter your password.

Click this button for context-sensitive Help using this screen.

- Type a password that you will be able to remember.

- Re-type the password exactly as typed above.

Click this button to save your password and close the dialog box.

Click this button to close the dialog box without saving your password.

Click this button to save your changes and close the dialog box.

Click this button to close the dialog box without saving your changes.

Click this button for context-sensitive Help using this screen.

Select this checkbox to include in the scan all subfolders found in the location selected for scanning.

Click this button to locate the drive or folder you want to add to the scan. When selected, the path will appear in the text box above.

Select this button if you want to add all items:

- on My Computer
- on all removable drives
- on all fixed drives
- on all network drives.

Next, click the and select one of the available item-types.

Select this button if you want to select a drive or folder to add.

- Next, click **Browse** to locate the drive or folder you want to add to the scan.
- When selected, the path will appear in the text box above.

Use this screen to enable, and configure **Heuristics**. This feature evaluates the probability that a macro in a Microsoft Office application, or an executable program file is a virus or contains a virus.

This box lists the files, folders and drives that have been included in virus detection. Information about the item is displayed, including the **name** of the item, whether its **subfolders** are included, and its type.

- To add items to the list, click **Add** at the bottom of the screen.
- To edit items on the list, click **Edit**.
- To remove an item from the list, select the item and click **Remove**.

Click this button to add an item to the list, above.

Click this button to edit an item on the list, above.

Click this button to delete a selected item from the list, above.

Select this checkbox to give yourself the option of cleaning infected files when a virus is found. When selected, this option appears as a button in the Alert dialog box.

Select this checkbox to give yourself the option of deleting infected files from your system as VShield detects them. When selected, this option appears as a button in the Alert dialog box.

Select this checkbox to give yourself the option of excluding this file from the scan. When selected, this option appears as a button in the Alert dialog box.

Select this checkbox to give yourself the option of moving infected files to a quarantine directory. Then, click **Browse** to select a location to which the file should be moved.

When selected, this option appears as a button in the Alert dialog box.

Select this checkbox to give yourself the option of ignoring infected files and continuing the scan. When selected, this option appears as a button in the Alert dialog box.

Select this checkbox to give yourself the option of halting the scan immediately. When selected, this option appears as a button in the Alert dialog box.

This box lists the files, folders and drives excluded from virus detection.

- Items are added to the list using the **Add Exclude Item** dialog box, which becomes available when you click **Add** at the bottom of the screen.
- Information about the item is displayed in the box, including the **name** of the item, whether its **subfolders** are excluded, and whether it is excluded **from** file scanning, boot sector scanning, or both.

Click this button to open the **Add Exclude Item** dialog box.

Click this button to open the **Edit Exclude Item** dialog box.

Click this button to delete a selected item from the list of excluded items.

Select the **Send network alert** checkbox to alert your network administrator via NetShield when VShield finds an infected file.

- Next, click **Browse** to select a server to receive Centralized Alerting Message.
- When selected, the path to the message folder appears in the text box.

NetShield is a Network Associates server anti-virus solution.

Clear this checkbox to disable network alert.

Click this button to open the **Browse for Folder** dialog box, where you can select a server to receive Centralized Alerting Message. When selected, the path to the message folder appears in the text box.

Select this checkbox to send notification to network management or desktop management applications that comply with the **D**esktop **M**anagement **I**nterface standard.

Click this button to select a folder to exclude from virus scanning. When selected, the path to the folder appears in the text box.

Select this checkbox to exclude from virus scanning all subfolders associated with the folder designated for exclusion.

Select this checkbox to exclude the file or folder above from **File scanning** only.

Select this checkbox to exclude the file or folder above from **Boot sector scanning** only.

Click this button to save your changes and close the dialog box.

Click this button to close the dialog box without saving any changes you have made.

Click this button to close the dialog box and save any changes you have made.

Click this button to close the dialog box and save any changes you have made.

Click this button to open the **Add Program File Extension** dialog box.

Click this button to delete a selected program file extension from list.

Click this button to restore the VShield default extensions. All extensions that have been added by users will be removed from the list.

This box lists the extensions of all file types scanned for viruses.

- To add an extension, click **Add**. The **Add Program File Extension** dialog box appears.
- To delete an extension from the list, select the extension and click **Delete**.
- To restore the VShield default list of extensions, eliminating extensions that have been added by users, click **Default**.

Click this button to enter your password.

If you are configuring a task that was created by copying a previously existing task, select this checkbox to apply the security options of the original task to the new task. The checkbox is enabled after you select one of the property pages for password protection.

Click **Browse** to locate the drive or folder you want to add to the scan. When selected, the path will appear in this text box.

Select this checkbox to include in the scan all subfolders found in the location selected for scanning.

Click this button to locate the drive or folder you want to add to the scan. When selected, the path will appear in the text box above.

Select this button if you want to add all items:

- on My Computer
- on all removable drives
- on all fixed drives
- on all network drives.

Next, click the and select one of the available item-types.

Select this button if you want to select a drive or folder to add.

- Next, click **Browse** to locate the drive or folder you want to add to the scan.
- When selected, the path will appear in the text box above

Click the
and select one of the available item-types:

- My Computer
- All removable drives
- All fixed drives
- All network drives.

The numbers to the right represent the number of Java applets VShield had examined, and the number it had banned, as of the moment that you opened the Task Properties dialog box.

The numbers to the right represent the number of ActiveX controls VShield examined during the last scan, and the number banned.

The numbers to the right represent the number of Internet sites examined during the last scan, and the number banned.

The numbers to the right represent the number of Internet sites VShield has examined, and the number it has banned, during the scanning activity now in progress.

If no scanning activity is in progress now, the data reflect the results of VShield's most recent scan.

To view a list of the viruses defined in the .DAT files installed on your computer:

1 Click **Start** on the bottom-left of your screen.

1 Select **Programs → McAfee VirusScan → McAfee VirusScan Central.** The VirusScan launcher screen appears.

3 Click **Tools → Virus Info.** The list of viruses defined in the data files currently installed on your computer is displayed.

For information about keeping your data files up-to-date, see Updating VirusScan Data Files.

Select this button to specify on-access scanning of all e-mail attachments you receive.

Select this button to limit on-access scanning to only program files that you receive. Then click **Extensions** to see or edit the list of file types to be scanned. The default list shows those file types that are most susceptible to virus infection.

Select the **Send network alert** checkbox to alert your network administrator via NetShield when VShield finds an infected file.

- Next, click **Browse** to select a server to receive a Centralized Alerting Message.
- When selected, the path to the message folder appears in the text box.

NetShield is a Network Associates server anti-virus solution.

Clear this checkbox to disable network alert.

Select this checkbox to send an alert message to the person who sent you e-mail that carried a virus.
VShield will send a standard alert message each time it detects a virus. To see or compose your own message, click **Configure**.

Clear this checkbox to disable the reply to sender.

Select this checkbox to send notification to network management or desktop management applications that comply with the **Desktop Management Interface** standard.

Select this checkbox to enable log activity.

- Next, click **Browse** to select a file for the log. When selected, the path to the file appears in the text box.
- You can then set the maximum size of the log file.

Select this checkbox to record the settings you chose for this scanning session.
This information is written to the designated log file when the scanning program is unloaded or you shut your system down.

Clear this checkbox to disable logging of session settings.

Select this checkbox to send notification to network management or desktop management applications that comply with the **Desktop Management Interface** standard.

Select this checkbox to scan for harmful Java classes as you visit Internet sites.
VShield compares the Java classes you encounter with a database of classes known to cause harm. It alerts you when it finds a potentially harmful Java class.

Select this checkbox to tell VShield to block your browser software from visiting Internet sites that you designate with an IP Address.

Next, click **Configure** to see or edit the list that VShield uses to identify dangerous IP addresses.

{bmc onestep.bmp Select the **Send network alert** checkbox to alert your network administrator via NetShield when VShield encounters a hostile ActiveX control or Java class, or if an attempt is made to connect to a banned Internet site.

- Next, click **Browse** to select a server to receive Centralized Alerting messaging.
- When selected, the path to the message folder appears in the text box.

NetShield is a Network Associates server anti-virus solution.

Clear this checkbox to disable network alert.

Select the **Send network alert** checkbox to alert your network administrator via NetShield when VShield finds an infected file.

- Next, click **Browse** to select a server to receive Centralized Alerting messaging.
- When selected, the path to the message folder appears in this text box.

NetShield is a Network Associates server anti-virus solution.

Click this button to enter a password for protecting the configurations and options you have selected.

Select this checkbox to scan for viruses in e-mail files you receive from the Internet via Lotus cc:Mail, Microsoft Mail; or any MAPI-compliant e-mail client.

Clear this checkbox to disable e-mail scanning.

Select this button for Microsoft Mail or any MAPI-compliant e-mail client, including Lotus cc:Mail 8.

- If you use Lotus cc:Mail 8 select Microsoft Mail (MAPI.) Lotus cc:Mail 8 is MAPI-compliant.
- If you use America Online, Eudora Light, Netscape, or any other POP-3 or proxy mail client, use the **Download Scan** module instead of the **E-mail Scan** module to configure your virus scanning preferences.

Select this button for Lotus cc:Mail 6 or 7.

- If you use Lotus cc:Mail 8 select Microsoft Mail (MAPI) instead. Lotus cc:Mail 8 is MAPI-compliant.
- If you use America Online, Eudora Light, Netscape, or any other POP-3 or proxy mail client, use the **Download Scan** module instead of the **E-mail Scan** module to configure your virus scanning preferences.

Select this button to specify scanning of all new e-mail.

Select this button to specify scanning of new e-mail in a particular folder. Then click the adjacent **Browse** button to locate the folder containing the mail to be scanned.

If you have not yet logged on to your e-mail system, you are asked to choose or create a user profile for use with Microsoft Mail or a MAPI-compliant mail system. See the documentation for Microsoft Messaging for more details.

If you have chosen **Select Folder**, click this button to browse for the folder containing the mail to be scanned.

Enter how often, in seconds, VShield should check your mail server to see if new e-mail has arrived. This should be about twice as frequently as your mail server checks for new mail.

You may use the to select the number of seconds, or enter the number from your keyboard.

If you have chosen **Program files only**, click this button to see or edit the list of file types to be scanned. The default list shows those file types that are most susceptible to virus infection.

Select this checkbox to include scanning of files created with file compression utilities. See **Help** topic “Scanning Compressed Files” for more information.

Clear this checkbox to disable scanning of compressed files.

Select this button for Microsoft Mail or any MAPI-compliant e-mail client.

- If you use Lotus cc:Mail 8 select Microsoft Mail (MAPI.) Lotus cc:Mail 8 is MAPI-compliant.
- If you use a version of Lotus cc:Mail earlier than version 8, you must perform a custom installation of VirusScan for Windows 95 and Windows 98.
- If you use America Online, Eudora Light, Netscape, or any other POP-3 or proxy mail client, use the **Download Scan** module instead of the **E-mail Scan** module to configure your virus scanning preferences.

Select this button if you use America Online, Eudora Light, Netscape, or any other POP-3 or proxy mail client. VShield uses the options you choose on the **Download Scan** property page to control scanning of attachments received via those e-mail clients.

If you are using a version of cc:Mail earlier than version 8, you must select this checkbox in order to enable selection of cc:Mail as your mail server.

Click this button to scan all messages in your in-box including those previously read or scanned.

Click this button to limit scanning to only those messages in your in-box that you have not yet read.

Click the
to select a response to virus detection.

Depending on your selection, the **Possible actions** section will display:

- additional options, or
- a text window for entering additional information, or
- a message describing the result of the action selected.

Depending on your selection of response, the **Possible actions** section will display:

- additional options, or
- a text window for entering additional information, or
- a message describing the result of the action selected.

If you selected **Prompt for Action** from the drop-down list above, you must indicate, on the **Alert** tab, whether you prefer a message, a beep, or both.

Select this checkbox to give yourself the option of deleting infected files from your system as they are detected. When selected, this option appears as a button in the Alert dialog box.

Select this checkbox to give yourself the option of ignoring infected files and continuing the scan. When selected, this option appears as a button in the Alert dialog box.

Select this checkbox to give yourself the option of moving infected files to a quarantine directory. Then, click **Browse** to select a location to which the file should be moved.

When selected, this option appears as a button in the Alert dialog box.

Select this checkbox to give yourself the option of halting the scan immediately. When selected, this option appears as a button in the Alert dialog box.

Select this checkbox to give yourself the option of cleaning infected files when a virus is found. When selected, this option appears as a button in the Alert dialog box.

Click this button to select the quarantine file in which to store the infected file.

Click **Browse** to select the quarantine file in which to store the infected file.

Select the **Send network alert** checkbox to alert your network administrator via NetShield when VShield finds an infected file. Next, click **Browse** to select a server to receive Centralized Alerting Message. When selected, the path to the message folder appears in the text box.

NetShield is a Network Associates server anti-virus solution.

Clear this checkbox to disable network alert.

Select the **Send network alert** checkbox to alert your network administrator via NetShield when VShield finds an infected file.

- Next, click **Browse** to select a server to receive a Centralized Alerting Message.
- When selected, the path to the message folder appears in this text box.

NetShield is a Network Associates server anti-virus solution.

Click this button to open the **Browse for Folder** dialog box, where you can select a server to receive Centralized Alerting Message. When selected, the path to the message folder appears in the text box.

Click this button to create the e-mail alert:

- provide the address of the person who sent you the infected e-mail;
- see the default message or compose your own message.

Click this button to create the e-mail alert:

- provide the address of the people you want to inform about the infected e-mail;
- see the default message or compose your own message.

Select this checkbox if you want to hear a beep when an infected file is found.
Clear this checkbox to disable audible beep.

Select this checkbox if you want to design a custom message to be displayed when a virus is found.

- Next, type the message in the text box, below.
- When selected, this option displays your message as alert text in the Alert dialog box.

Clear this checkbox to disable custom messaging.

- See the default message VShield displays when it detects a virus, or compose a new message.

Select the **Log to file** checkbox to enable log activity.

- Next, click **Browse** to select a folder in which the log file will be created.
- When selected, the path to the file appears in this text box.

Select this checkbox if you want to limit the size of the log file.

- Next, in the text box, enter the maximum size, in kilobytes, of the log file.
- You may use the to select the number of kilobytes, or enter the number from your keyboard.

Clear this checkbox to disable size limitation for the log file.

Enter the maximum size, in kilobytes, of the log file. You may use the
to select the number of kilobytes, or enter the number from your keyboard.

Enter the maximum size, in kilobytes, of the log file. You may use the
to select the number of kilobytes, or enter the number from your keyboard.

Click this button to select a file in which the log will be created. When selected, the path to the file appears in the text box.

Select this checkbox to record the names of any virus strains that VShield finds during a scanning session, and the number of times it finds them.

Clear this checkbox to disable logging of virus strains.

Select this checkbox to record the number of infected files cleaned during a scanning session.
Clear this checkbox to disable logging of virus cleaning.

Select this checkbox to record the number of infected files deleted during a scanning session.
Clear this checkbox to disable logging of infected file deletion.

Select this checkbox to record the number of infected files moved to a quarantine directory during a scanning session. Clear this checkbox to disable logging of infected file relocation.

Select this checkbox to generate a summary of actions taken during this scanning session, including:

- The number of files examined for viruses.
- The number of infected files cleaned.
- The number of infected files deleted.
- The number of infected files moved.
- Other information about your configuration settings.

These data are written to the designated log file when the scanning program is unloaded or you shut your system down.

Clear this checkbox to disable logging of session summary information.

Select the e-mail property pages, (tabs) that you want to protect from unauthorized changes.

You may select all the property pages in the list box or any individual property page. A appears to the left of protected pages.

Select the System Scan property pages, (tabs) that you want to protect from unauthorized changes.

You may select all the property pages in the list box or any individual property page. A appears to the left of protected pages.

Select the internet filter property pages, (tabs) that you want to protect from unauthorized changes.

You may select all the property pages in the list box or any individual property page. A appears to the left of protected pages.

This box lists the extensions of all file types scanned for viruses.

- To add an extension, click **Add**. The **Add Program File Extension** dialog box appears.
- To delete an extension from the list, select the extension and click **Delete**.
- To restore the default list of extensions, eliminating extensions that have been added by users, click **Default**.

Click this button to open the **Add Program File Extension** dialog box.

Click this button to delete a selected program file extension from list.

Click this button to restore the default extensions. All extensions that have been added by users will be removed from the list.

Type the extension of the file type to scan for viruses. Do not include the dot that normally precedes a file extension.

Click this button for context-sensitive Help using this screen.

Enter your password and click **OK**.

Click this button to open your e-mail server address book. Next, select the user(s) to whom you want to send the Alert.

The name(s) of the user(s) to whom you want to send the Alert will appear here after being selected from you e-mail address book. You can type the name(s) directly into this box.

Click this button to open your e-mail server address book. Next, select the user(s) to whom you want to send copies of the Alert.

The name(s) of the user(s) to whom you want to send the Alert will appear here after being selected from the cc:Mail Address Book. You can type the name(s) directly into this box.

Enter a brief statement summarizing the message.

Type the Alert message here.

- Type a password that you will be able to remember.

- Re-type the password exactly as typed above.

Enter your cc:Mail password.

Enter your cc:Mail user identification.

Enter your cc:Mail password.

Enter the path to cc:Mail.

Click this button for context-sensitive Help using this screen.

Type the name of the person to whom you want to send the Alert.
Next, click **Add** to put the name on the notification distribution list.

This box lists the names of people who are on the cc:Mail Alert notification list.

Click the
to select a name from another mailing list.

Click this button to add the name to the notification distribution list.

Click this button to delete a selected name from the notification distribution list.

Click this button for context-sensitive Help using this screen.

- Select the VShield module that you want to configure.

Use this page to set the properties of:

- the feature named on the tab
- the program component selected in the box on the left side of the screen.

Click this button to use the **Wizard** as a guide to configuring VShield.

Select this checkbox to enable log activity.

- Next, click **Browse** to select a file for the log.
- When selected, the path to the file appears in the text box.

You can then set the maximum size of the log file.

Select the **Log to file** checkbox, above to enable log activity. Next, click **Browse** to select a file in which the log will be created. When selected, the path to the log file appears in this text box.

If you want to limit the size of the log file, select the checkbox with that label. Next, in the adjoining text box, enter the maximum size, in kilobytes, of the log file. You may use the
to select the number of kilobytes, or enter the number from your keyboard.

Clear the **Limit size of log file to** checkbox to disable size limitation for the log file.

Enter the maximum size, in kilobytes, of the log file. You may use the
to select the number of kilobytes, or enter the number from your keyboard.

Click this button to select a file in which the log will be created. When selected, the path to the log file appears in the text box.

Select this checkbox to record the names of any virus strains found during a scanning session, and the number of times it finds them.

Clear this checkbox to disable logging of virus strains.

Select this checkbox to record the number of infected files moved to a quarantine directory during a scanning session. Clear this checkbox to disable logging of infected file relocation.

Select this checkbox to record the settings you chose for this scanning session.
Clear this checkbox to disable logging of session settings.

Select this checkbox to generate a summary of actions taken during this scanning session, including:

- The number of files examined for viruses.
- The number of infected files cleaned.
- The number of infected files deleted.
- The number of infected files moved.
- Other information about your configuration settings.
- Clear this checkbox to disable logging of session summary information.

Click the
to select a response when a virus is found.

Depending on your selection, the **Possible actions** section will display:

- additional options, or
- a text window for entering additional information, or
- a message describing the result of the action selected.

Select this checkbox to give yourself the option of cleaning infected files when a virus is found. When selected, this option appears as a button in the Alert dialog box.

Select this checkbox to give yourself the option of deleting infected files from your system as they are detected. When selected, this option appears as a button in the Alert dialog box.

Select this checkbox to give yourself the option of ignoring infected files and continuing the scan. When selected, this option appears as a button in the Alert dialog box.

Select this checkbox to give yourself the option of moving infected files to a quarantine directory. Then, click **Browse** to select a location to which the file should be moved.

When selected, this option appears as a button in the Alert dialog box.

Click the
to select a response when a virus is found.
Depending on your selection of response from the drop-down list, the **Possible actions** section will display:

- additional options, or
- a text window for entering additional information, or
- a message describing the result of the action selected.

Right-click on any of the options for additional information.

If you select **Prompt for Action** from the drop-down list, you will have to indicate, on the **Alert** tab, whether you prefer a message or a beep. You can design a custom message and/or specify that an audible beep be sounded when a virus is found.

Click this button to select the quarantine file in which to store the infected file.

Click **Browse** to select the quarantine file in which to store the infected file.

Select the **Send network alert** checkbox to alert your network administrator via NetShield when VShield finds an infected file. Next, click **Browse** to select a server to receive Centralized Alerting Message. When selected, the path to the message folder appears in the text box.

NetShield is a Network Associates server anti-virus solution.

Clear this checkbox to disable network alert.

Select the **Send network alert** checkbox to alert your network administrator via NetShield when VShield finds an infected file. Next, click **Browse** to select a server to receive Centralized Alerting Message. When selected, the path to the message folder appears in this text box.

NetShield is a Network Associates server anti-virus solution.

Click this button to open the **Browse for Folder** dialog box, where you can select a server to receive Centralized Alerting Message. When selected, the path to the message folder appears in the text box.

Select this checkbox if you want to hear to beep when an infected file is found.
Clear this checkbox to disable audible beep.

Select this checkbox if you want to design a custom message to be displayed when a virus is found. Next, type the message in the text box, below. When selected, this option displays your message as alert text in the Alert dialog box.

Clear this checkbox to disable custom messaging.

- See the message VShield displays when it detects a virus, or compose a new message.

Select this checkbox to perform virus scans on files you download from the Internet:

- including e-Mail you receive via America Online, Eudora Light, Netscape, or any other POP-3 or proxy mail client.
- not including e-Mail you receive via Lotus cc:Mail; Microsoft Mail; or any MAPI-compliant e-mail client. Scanning of these e-Mail messages is controlled by the **E-mail Scan** module, not by the **Internet Download** module.

Clear this checkbox to disable Internet download scanning.

Select this button to specify scanning of every file you download from the Internet.

Select this button to specify scanning of program files only.

Click this button to see the list of file types to be included in scanning. The default list shows those file types that are most susceptible to virus infection.

Select this checkbox to include scanning of files compressed with LHA, LZEXE, PkLite, PkZip, or WinZip. Clear this checkbox to disable scanning of compressed files.

Select the Download Scan property pages, (tabs) that you want to protect from unauthorized changes.
You may select all property pages in the list box or any individual property page. A appears to the left of protected pages.

Select this checkbox to scan for viruses in any file, except Internet and e-mail files.
Clear this checkbox to disable virus scanning.

Select this checkbox to scan executable files when they are run.
Clear this checkbox to disable scanning when running executable files.

Select this checkbox to scan files when they are copied.
Clear this checkbox to disable scanning when copying files.

Select this checkbox to scan files when they are created.
Clear this checkbox to disable scanning when creating files.

Select this checkbox to scan files when they are renamed.
Clear this checkbox to disable scanning when renaming files.

Select this checkbox to scan a floppy disk's boot sector when accessing the disk.
Clear this checkbox to disable on-access scanning of floppy disk boot sectors.

Select this checkbox to scan a floppy disk's boot sector when you shut the system down.
Clear this checkbox to disable scanning of floppy disk boot sector at time of system shutdown.

Select this button to specify scanning of every file.

Select this button to limit scanning to program files only. Then click **Extensions** to see the list of file types to be included in scanning. The default list shows those file types that are most susceptible to virus infection.

Click this button to see the list of file types to be included in scanning. The default list shows those file types that are most susceptible to virus infection.

Select this checkbox to include scanning of compressed files. See **Help** topic “Scanning Compressed Files” for more information. Clear this checkbox to disable scanning of compressed files.

Select this button to enable heuristic scanning of Microsoft Office macros, but not of executable program files.

Select this button to enable heuristic scanning of executable program files, but not of Microsoft Office macros.

Select this button to enable heuristic scanning of Microsoft Office macros and executable program files.

Select the **Log to file** checkbox to enable log activity.

- Next, click **Browse** to select a file for the log.
- When selected, the path to the file appears in this text box.

You can then set the maximum size of the log file.

Select this checkbox to allow VShield to be disabled from the taskbar or Scheduler.
Clear this checkbox to prevent disabling VShield from the taskbar or Scheduler.

Select this checkbox to display the VShield icon on the taskbar.

Click this button to configure **Macro Heuristics**. This feature evaluates the probability that a macro in a Microsoft Office application is a virus.

Click the
to select a response when a virus is found. Depending on your selection, the **Possible actions** section will display:

- additional options, or
- a text window for entering additional information, or
- a message describing the result of the action selected.

Select this checkbox to give yourself the option of cleaning infected files when a virus is found. When selected, this option appears as a button in the Alert dialog box.

Select this checkbox to give yourself the option of deleting infected files from your system when they are detected. When selected, this option appears as a button in the Alert dialog box.

Select this checkbox to give yourself the option of excluding from the scanning procedure a file in which a virus was found. When selected, this option appears as a button in the Alert dialog box.

Select this checkbox to give yourself the option of accessing a file even though VShield found a virus in the file. When selected, this option appears as a button in the Alert dialog box.

Select this checkbox to give yourself the option of preventing access to a file in which a virus was found. When selected, this option appears as a button in the Alert dialog box.

Click this button to select the quarantine file in which to store the infected file.

Click **Browse** to select the quarantine file in which to store the infected file.

Select the **Send network alert** checkbox to alert your network administrator via NetShield VShield detects an infected file. Next, click **Browse** to select a server to receive Centralized Alerting Message. When selected, the path to the message folder appears in the text box.

NetShield is a Network Associates server anti-virus solution.

Clear this checkbox to disable network alert.

Select the **Send network alert** checkbox to alert your network administrator via NetShield when VShield finds an infected file. Next, click **Browse** to select a server to receive Centralized Alerting Message. When selected, the path to the message folder appears in this text box.

NetShield is a Network Associates server anti-virus solution.

Click this button to open the **Browse for Folder** dialog box, where you can select a server to receive Centralized Alerting Message. When selected, the path to the message folder appears in the text box.

Select this checkbox if you want VShield to beep when it finds an infected file.
Clear this checkbox to disable audible beep.

Select this checkbox if you want to design a custom message for VShield to display when it finds a virus. Next, type the message in the text box, below. When selected, this option displays your message as alert text in the Alert dialog box.

Clear this checkbox to disable custom messaging.

- See the message VShield displays when it detects a virus, or compose a new one.

Select this checkbox to send notification to network management or desktop management applications that comply with the **D**esktop **M**anagement **I**nterface standard.

Select this checkbox to enable log activity. Next, click **Browse** to select a file for the log. When selected, the path to the file appears in the text box. You can then set the maximum size of the log file.

Select the **Log to file** checkbox, above to activate download log activity. Next, click **Browse** to select a file in which the log will be created. When selected, the path to the log file appears in this text box.

Click this button to select a file in which the log will be created. When selected, the path to the log file appears in the text box.

Select this checkbox if you want to limit the size of the log file. Next, in the text box, enter the maximum size, in kilobytes, of the log file. You may use the
to select the number of kilobytes, or enter the number from your keyboard.
Clear this checkbox to disable size limitation for the log file.

Enter the maximum size, in kilobytes, of the log file. You may use the
to select the number of kilobytes, or enter the number from your keyboard.

Select this checkbox to record the names of any virus strains found during a scanning session, and the number of times it finds them.

Clear this checkbox to disable logging of virus strains.

Select this checkbox to record the number of infected files cleaned during a scanning session.
Clear this checkbox to disable logging of virus cleaning.

Select this checkbox to record the number of infected files deleted during a scanning session.
Clear this checkbox to disable logging of infected file deletion.

Select this checkbox to record the number of infected files moved to a quarantine directory during a scanning session. Clear this checkbox to disable logging of infected file relocation.

Select this checkbox to record the settings you chose for this scanning session.
Clear this checkbox to disable logging of session settings.

Select this checkbox to generate a summary of actions taken during this scanning session, including:

- The number of files examined for viruses.
- The number of infected files cleaned.
- The number of infected files deleted.
- The number of infected files moved.
- Other information about your scan settings.
- Clear this checkbox to disable logging of session summary information.

Select this checkbox to record the date and time the scanning session began.
Clear this checkbox to disable recording of date and time.

Select this checkbox to record the name of the user who performed the scan.
Clear this checkbox to disable recording of the user's name.

This box lists the files, folders and drives to exclude from virus detection. Items are added to the list using the **Add Exclude Item** dialog box, which becomes available when you click **Add** at the bottom of the screen. Information about the item is displayed in the box below, including the **name** of the item; whether its **subfolders** are excluded; and whether it is excluded **from** File scanning, Boot Sector scanning, or both.

Click this button to open the **Add Exclude Item** dialog box.

Click this button to open the **Edit Exclude Item** dialog box.

Click this button to delete a selected item from the list of excluded items, above.

Click **Browse** to select a folder to exclude from virus scanning. When selected, the path to the folder appears in this text box.

Click this button to select a folder to exclude from virus scanning. When selected, the path to the folder appears in the text box.

Select this checkbox to exclude from virus scanning all subfolders associated with the folder designated for exclusion.

Select this checkbox to exclude the file or folder above from **File scanning** only.

Select this checkbox to exclude the file or folder above from **Boot sector scanning** only.

Select this checkbox to scan for harmful Java classes, ActiveX controls or dangerous Internet sites.
Clear this checkbox to disable scanning for Java, ActiveX or other dangerous Internet features.

Select this checkbox to scan for harmful ActiveX controls as you visit Internet sites.

VShield compares the ActiveX controls you encounter with a database of controls known to cause harm. It alerts you when it finds a potentially harmful ActiveX control.

Click this button to see, or add to the list of IP addresses that VShield uses to identify dangerous Internet sites.

Select this checkbox to tell VShield to block your browser software from visiting Internet sites you designate with a Uniform Resource Locator (URL) or domain name.

Next, click **Configure** to see or add to the list VShield uses to identify dangerous Internet sites.

Click this button to see, or add to the list of URLs or domains that VShield uses to identify dangerous Internet sites.

Click the
to select a VShield response when it encounters a hostile ActiveX control or Java class, or if you attempt to connect to a banned Internet site. The **Possible actions** section will display a message describing the result of the action selected.

Click the
to select a VShield response when it finds a virus. The **Possible actions** section will display a message describing the result of the action selected.

Select this checkbox to enable log activity. Next, click **Browse** to select a file for the log. When selected, the path to the file appears in the text box. You can then set the maximum size of the log file.

Select the **Log to file** checkbox, above to enable log activity. Next, click **Browse** to select a file in which the log will be created. When selected, the path to the log file appears in this text box.

Select this checkbox if you want to limit the size of the log file. Next, in the text box, enter the maximum size, in kilobytes, of the log file. You may use the
to select the number of kilobytes, or enter the number from your keyboard.
Clear this checkbox to disable size limitation for the log file.

Enter the maximum size, in kilobytes, of the log file. You may use the
to select the number of kilobytes, or enter the number from your keyboard.

Click this button to open the **Browse for Folder** dialog box, where you can select a server to receive Centralized Alerting Message. When selected, the path to the message folder appears in the text box.

Select this checkbox if you want to hear a beep when a hostile ActiveX control or Java class is encountered, or when you attempt to connect to a banned Internet site.

Clear this checkbox to disable audible beep.

Select this checkbox if you want to design a custom message when a hostile ActiveX control or Java class is encountered, or when you attempt to connect to a banned Internet site. Next, type the message in the text box, below. When selected, this option displays your message as alert text in the Alert dialog box.

Clear this checkbox to disable custom messaging.

See the message to be displayed when a virus is detected, or compose a new one.

Select this checkbox to send notification to network management or desktop management applications that comply with the **D**esktop **M**anagement **I**nterface standard.

Click this button to open the **Add Domain Address** dialog box.

Click this button to delete a selected domain address from list of banned addresses.

This box lists the domain addresses that have been banned.

- To ban a domain address, click **Add**. The **Add domain address** dialog box appears.
- To delete a domain address from the list of banned addresses, select the address and click **Delete**.

Click this button to open the **Add IP Address** dialog box.

Click this button to delete a selected IP address from list of banned addresses.

This box lists the IP addresses that have been banned.

- To ban an IP address, click **Add**. The **Add IP address** dialog box appears.
- To delete an IP address from the list of banned addresses, select the address and click **Delete**.

Type the URL to be added to the list of banned domain addresses.

Click this button for context-sensitive Help using this screen.

Type the IP address to be added to the list of banned IP addresses.

Type the Subnet mask of the IP address that is to be added to the list of banned IP addresses.

Click this button for context-sensitive Help using this screen.

Select this checkbox to enable password-protection.

Select this button to password-protect all configuration and option choices you have made.

Select this button to password-protect only those options that you specify. Click each tab to view a list of the property pages that you may want to password-protect.

Enter a password to protect the configurations and options you have selected.

Re-enter the password you typed above.

Select this checkbox to enable **Macro Heuristics**. This feature evaluates the probability that an unrecognized characteristic in a Microsoft Office application is a virus.

Use the slider to set the sensitivity threshold for defining a macro as a virus.

- A low setting minimizes the number of macros interpreted as viruses.
- A high setting maximizes the number of macros interpreted as viruses.

Use the slider to set the sensitivity threshold for defining a macro as a virus.

- A low setting minimizes the number of macros interpreted as viruses.
- A high setting maximizes the number of macros interpreted as viruses.

Select this checkbox to delete macros from infected Microsoft Office documents while cleaning them. Clear this checkbox to disable macro deletion.

Click this button for context-sensitive Help using this screen.

Type the extension of the file type to add to list of types included in a scan. Do not include the dot that normally precedes a file extension.

Click this button to save your changes and close the dialog box.

Click this button to close the dialog box without saving your changes.

This screen displays detailed identification information about the infected file, its location, and its attributes.

Describes the file type of the infected file.

Shows the path to the infected file.

Shows the number of bytes in the infected file.

Shows the number of bytes in the infected file.

Displays the file name based on the DOS convention of 8 characters plus a 3-character extension. Long file names are truncated.

Displays the date the infected file was created.

Displays the date the infected file was last modified.

Displays the date the infected file was last opened, copied or run.

VirusScan selects this box if the infected file is a read-only file. See your operating system documentation for definitions of file attributes.

VirusScan selects this box if the infected file is a hidden file. See your operating system documentation for definitions of file attributes.

VirusScan selects this box if the infected file is an archive file. See your operating system documentation for definitions of file attributes.

VirusScan selects this box if the infected file is a system file. See your operating system documentation for definitions of file attributes.

VirusScan displays the attributes of the infected file by placing a mark next to each one that is applicable.

Indicates the current disposition of the virus.

Displays the name of the virus infecting the file.

Displays the name of the virus infecting the file.

Displays the kinds of files included in scanning. The default list shows those file types that are most susceptible to virus infection.

{bmc onestep.bmp Displays the kinds of files included in scanning. The default list shows those file types that are most susceptible to virus infection

Displays the kinds of files included in scanning. The default list shows those file types that are most susceptible to virus infection

The selected checkboxes describe the characteristics of the infecting virus.

VirusScan selects this box if the virus is retained in memory after it runs, continuing to affect other files.

VirusScan selects this box if the virus encrypts part of its code signature to avoid detection.

VirusScan selects this box if the virus avoids detection by changing its code signature slightly each time it copies itself.

VirusScan selects this box if the virus can be cleaned.

Click this button to attempt to clean the virus.

Click this button to delete the infected file.

Click this button to select a quarantine location for the infected file.

Click this button to start scanning based on the options you selected on tabbed property pages.

Click this button to stop a scan in progress.

Click this button to bring your data files up to date. For details, see Updating VirusScan Data Files.

Click **Browse** to select a drive, disk, folder or file to scan. The selected location appears in the text box.

Click this button to select a drive, disk, folder or file to scan. The selected location appears in the text box.

Select this checkbox to include scanning of subfolders in the drive or folder you selected.

Select this button to specify scanning of every file and file type.

Select this button to limit scanning to Program files only. Then click **Extensions** to see the list of file types to be included in scanning. The default list shows those file types that are most susceptible to virus infection.

Select this checkbox to include scanning of files compressed with LHA, LZEXE, PkLite, PkZip, or WinZip. Clear this checkbox to disable scanning of compressed files.

Click this button to see the list of file types to be included in scanning. The default list shows those file types that are most susceptible to virus infection.

Click the
to select a response when a virus is detected. Depending on your selection, the **Possible actions** section will display:

- additional options, or
- a text window for entering additional information, or
- a message describing the result of the action selected.

Click **Browse** to select the quarantine file in which to store the infected file.

Click this button to select a quarantine folder to store infected files. The path to the selected folder appears in the text box.

If you selected **Prompt for Action** on the **Action** tab, you must now indicate whether you prefer a message, a beep, or both.
Select this checkbox if you want a message displayed when a virus is detected. Next, enter a brief message in the text box.
Clear this checkbox to disable messaging.

If you selected **Prompt for Action** on the **Action** tab, you must now indicate whether you prefer a message, a beep, or both.
Select this checkbox if you want an audible beep when a virus is found.

Clear this checkbox to disable beeping.

Select this checkbox to enable log activity. Next, click **Browse** to select a file for the log. When selected, the path to the file appears in the text box. You can then set the maximum size of the log file.

Clear this checkbox to disable activity logging.

Click this button to select a file in which the log will be created. When selected, the path to the log file appears in the text box.

Select this checkbox if you want to limit the size of the log file.

- Next, in the text box, enter the maximum size, in kilobytes, of the log file.
- You may use the to select the number of kilobytes, or enter the number from your keyboard.

Clear this checkbox to disable size limitation for the log file.

Click **Continue** to proceed with scanning without taking any action now.

Click this button to stop scanning without taking any action now.

Click this button to attempt to clean the virus.

Click this button to delete the infected file.

Click this button to select a quarantine location to for the infected file.

Click this button to exclude the infected file from scanning.

Click this button to view additional information about the virus.

This area displays the name of the file that has a virus.

The name of the virus infecting the file is displayed here.

VirusScan makes a suggestion about how to deal with the virus that it found.

Enter your cc:Mail user identification.

Enter your cc:Mail password.

Enter the path to cc:Mail.

Enter your cc:Mail password.

Describes the file type of the infected file.

Shows the path to the infected file.

Shows the number of bytes in the infected file.

Displays the file name based on the DOS convention of 8 characters plus a 3 character extension. Long file names are truncated.

Displays the date the infected file was created.

Displays the date the infected file was last modified.

Displays the date the infected file was last opened, copied or run.

VirusScan selects this box if the infected file is a read-only file. See your operating system documentation for definitions of file attributes.

VirusScan selects this box if the infected file is an archive file. See your operating system documentation for definitions of file attributes.

VirusScan selects this box if the infected file is a hidden file. See your operating system documentation for definitions of file attributes.

Displays the name of the infected file.

This area displays the name of the infected file and the name of the infecting virus.

This area displays the subject of the infected e-mail, the name of the infected attachment and the name of the infecting virus.

Use this screen to select a location to which infected files are to be moved.

This area displays the warning message defined on the Alert property page.

Click this button to proceed with scanning without taking any action now.

Click this button to continue stop scanning without taking any action now.

Click this button to attempt to clean the virus.

Click this button to delete the infected file.

Click this button to move an infected file to a quarantine location designated on the **Action** property page.

Click this button to prohibit application of a potentially damaging ActiveX or Java object, or access to a potentially dangerous website.

Click this button to view additional information about the virus identified.

Indicates the current disposition of the virus.

Displays the name of the virus infecting the file.

Displays the kinds of files susceptible to this virus.

Displays the number of bytes occupied by the virus.

VirusScan selects this box if the virus is retained in memory after it runs, continuing to affect other files.

VirusScan selects this box if the virus encrypts part of its code signature to avoid detection.

VirusScan selects this box if the virus avoids detection by changing its code signature slightly each time it copies itself.

VirusScan selects this box if the virus can be cleaned.

Click this button to attempt to clean the virus.

Click this button to delete the infected file.

Click this button to select a quarantine location for the infected file.

VirusScan selects this box if the infected file is a system file. See your operating system documentation for definitions of file attributes.

Click this button to add to the list of items to scan.

To edit an item in the list of items to scan, select the item.

Next, click this button.

To delete an item from the list of items to scan, select the item and then click this button.

This box lists the items to scan. Items may be added, edited, or removed from the list using the buttons located beneath the box.

Select this checkbox if you want the scan to begin without any prompts, but based only on options selected on the **Scheduler**. Scheduled tasks run only if the **Scheduler** is open at the time specified for the scan.

Select this checkbox to include boot sector viruses in the scan.

The boot sector is the first logical division of a hard or floppy disk. Your computer's BIOS looks here soon after you turn it on to find the files and programs it needs to start operations.

Select this checkbox to include memory-resident viruses in the scan. These viruses are retained in memory after they run, continuing to affect other files.

Activates VShield at system startup

Click this button to select a file in which the log will be created. When selected, the path to the log file appears in the text box.

Select the **Enable logging of ScreenScan activities** checkbox, above to activate log activity.

- Next, click **Browse** to select a file in which the log will be created.
- When **selected**, the path to the log file appears in this text box.

Use the slider to set the priority for scanning activity relative to other activities that may be operating while your screen saver is displayed, (e.g., disk defragmentation.)

- A low setting gives priority to other activities. Scanning operates more slowly.
- A high setting gives priority to scanning. Other activities operate more slowly.

Click this button to configure advanced scanner settings where you can set the priority for scanning while your screen saver is displayed. You can also set up a file in which to record scanning activities.

Select this checkbox to enable scanning while your screen saver is displayed.
Clear this checkbox to disable scanning while your screen saver is displayed.

Click this checkbox if you want ScreenScan to continue scanning that was begun during an earlier screen-saver interlude, but subsequently interrupted by mouse movement or keystroke.

If this checkbox is not selected, ScreenScan will start from the beginning each time your screen saver appears.

Displays the name of the folder currently being scanned. If you have not selected a folder to scan, this field remains blank.

Displays the name of the file currently being scanned. If you have not selected a folder to scan, this field remains blank.

Click this button to save your changes and close the dialog box.

Click this button to close the dialog box without saving any changes you have made.

Click this button to save your settings without closing the dialog box.

Select this checkbox if you want to launch VShield every time you start or reboot your system.

Displays the identification of the person who sent the e-mail message.

Displays the subject of the e-mail message.

Displays the name of the file attached to the e-mail message.

Displays the name of the virus infecting the e-mail attachment. For more information about the virus, click **Info**.

Displays the viruses found in binder files that contain multiple sub-files

Click this button to upgrade from the Evaluation version to the fully-supported Retail version of VirusScan for Windows 95 and Windows 98.