Features of VirusScan

- **VirusScan** gives you unmatched control over your scanning operations. You can initiate a scan operation at any time—a feature known as "on-demand" scanning—specify local and network disks as scan targets, choose how VirusScan will respond to any infections it finds, and see reports on its actions.
- **VShield** gives you continuous anti-virus protection from viruses borne on floppy disks, brought in from your network, or loaded into memory. VShield starts when you start your computer, and stays in memory until you shut down. A flexible set of property pages allows you to tell VShield which parts of your system to scan, when to scan them, which parts to leave alone, and how to respond to any infected files it finds. In addition, VShield can alert you when it finds a virus, and can generate reports that summarize each of its actions.
- **VirusScan Console** lets you create tasks for VirusScan to perform. A "task" can include anything from running a scan operation on a set of disks at a specific time or interval, to setting up VShield to run with particular options. The VirusScan Console comes with a preset list of tasks that ensures a minimal level of protection for your system—you can, for example, immediately scan and clean your C: drive or all disks on your computer, and enable or disable VShield.
- **Updates of virus signatures** are included with your purchase of VirusScan to assure the best detection and removal rates. See Keeping VirusScan updated.

See Also

About viruses
Types of viruses
Why scan for viruses
About Network Associates

About viruses

If you've ever lost important files stored on your hard disk, watched in dismay as your computer ground to a halt only to display a prankster's juvenile greeting on your monitor, or found yourself having to apologize for abusive e-mail messages you never sent, you know first-hand how computer viruses and other harmful programs can disrupt your productivity. If you haven't yet suffered from a virus "infection," count yourself lucky. But with more than 24,500 known viruses in circulation capable of attacking Windows- and DOS-based computer systems, it really is only a matter of time before you do.

The good news is that of those thousands of circulating viruses, only a comparatively few have the means to do real damage to your data. In fact, the term "computer virus" identifies a broad array of programs that have only one feature in common: they "reproduce" themselves automatically by attaching themselves to host software or disk sectors on your computer, usually without your knowledge. Most viruses cause relatively trivial problems, ranging from the merely annoying to the downright insignificant. Often, the primary consequence of a virus infection is the cost you incur in time and effort to track down the source of the infection and eradicate all of its traces.

Why worry?

So why worry about virus infections, if most attacks do little harm? The problem is twofold: First, although relatively few viruses have destructive effects, that fact says nothing about how widespread the malicious viruses are. In many cases, viruses with the most debilitating effects are the hardest to detect—the virus programmer bent on causing harm will take extra steps to avoid discovery. Second, even relatively "benign" viruses can interfere with the normal operation of your computer and can cause unpredictable behavior in other software. Some viruses contain bugs, poorly written code, or other problems severe enough to cause crashes when they run. Other times, legitimate software has problems running when a virus has, intentionally or otherwise, altered system parameters or other aspects of the computing environment. Tracking down the source of resulting system freezes or crashes drains time and money from more productive activities.

Beyond these problems lies a problem of perception: once infected, your computer can serve as a source of infection for other computers. If you regularly exchange data with colleagues or customers, you could unwittingly pass on a virus that could do more damage to your reputation or your dealings with others than it does to your computer.

The threat from viruses and other malicious software is real, and it is growing worse. The International Computer Security Association has estimated the total worldwide cost of detecting and cleaning virus infections at $1 billion per year in time and lost productivity—a figure that doesn't include the costs of data loss and recovery in the wake of attacks that destroyed data.

Where do viruses come from?

As you or one of your colleagues recovers from a virus attack or hears about new forms of malicious software appearing in commonly used programs, you've probably asked yourself a number of questions about how we as computer users got to this point. Where do viruses and other malicious programs come from? Who writes them? Why do those who write them seek to interrupt workflows, destroy data, or cost people the time and money necessary to eradicate them? What can stop them?

Why did this happen to me?

It probably doesn't console you much to hear that the programmer who wrote the virus that erased your hard disk's file allocation table didn't target you or your computer specifically. Nor will it cheer you up to learn that the virus problem will probably always be with us. But knowing a bit about the history of computer viruses and how they work can help you better protect yourself against them.

Virus prehistory

Historians have identified a number of programs that served as virus precursors, or that incorporated features now associated with virus software. Canadian researcher and educator Robert M. Slade traces virus lineage back to special-purpose utilities used to reclaim unused file space and perform other useful tasks in the earliest networked computers. Slade reports that computer scientists at a Xerox Corporation research facility called programs like these "worms," a term coined after the scientists noticed "holes" in printouts from computer memory maps that looked as though worms had eaten them. The term survives to this day to describe programs that make copies of themselves, but without altering host software.

A strong academic tradition of computer prank playing most likely contributed to the shift away from utility programs

and toward more malicious uses of the programming techniques found in worm software. Computer science students, often to test their programming abilities, would construct rogue worm programs and unleash them to "fight" against each other, competing to see whose program could "survive" while shutting down rivals. Those same students also found uses for worm programs in practical jokes they played on unsuspecting colleagues.

Some of these students soon discovered that they could use certain features of the host computer's operating system to give them unauthorized access to computer resources. Others took advantage of users who had relatively little computer knowledge to substitute their own programs—written for their own purposes—in place of common or innocuous utilities. These unsophisticated users would run what they thought was their usual software only to find their files erased, to have their account passwords stolen, or to suffer other unpleasant consequences. Such "Trojan horse" programs or "Trojans," so dubbed for their metaphorical resemblance to the ancient Greek gift to the city of Troy, remain a significant threat to computer users today.

Viruses and the PC revolution

What we now think of as true computer viruses first appeared, according to Robert Slade, soon after the first personal computers reached the mass market in the early 1980s. Other researchers date the advent of virus programs to 1986, with the appearance of the "Brain" virus. Whichever date has the better claim, the link between the virus threat and the personal computer is not coincidental.

The new mass distribution of computers meant that viruses could spread to many more hosts than before, when a comparatively few, closely guarded mainframe systems dominated the computing world from their bastions in large corporations and universities. Nor did the individual users who bought PCs have much use for the sophisticated security measures needed to protect sensitive data in those environments. Most particularly, virus writers found it relatively easy to exploit some PC technologies to serve their own ends.

On the frontier

Malicious software has even begun intruding into areas once thought completely out of bounds. Users of the mIRC Internet Relay Chat client, for example, have reported encountering viruses constructed from the mIRC scripting language. The chat client sends script viruses as plain text, which would ordinarily preclude them from infecting systems, but older versions of the mIRC client software would interpret the instructions coded into the script and perform unwanted actions on the recipient's computer. The vendors moved quickly to disable this capability in updated versions of the software, but the mIRC incident illustrates the general rule that where a way exists to exploit a software security hole, someone will find it and use it.

Some virus writers do it for the thrill of it, some to gain notoriety in their own peer group. Still others do it to exact revenge against employers or others they believe have treated them badly. Whatever their motives, they continue to develop new ways to cause you trouble.

How to protect yourself

Network Associates anti-virus software already gives you an important bulwark against infection and damage to your data, but anti-virus software is only one part of the security measures you should take to protect yourself and your data. Most measures are common sense—checking disks you receive from unknown or questionable sources, either with anti-virus software or some kind of verification utility, is always a good idea. Malicious programmers have gone so far as to mimic the programs you trust to guard your computer, pasting a familiar face on software with a less-than-friendly purpose. Network Associates includes VALIDATE.EXE, a verification utility, with its distributions to prevent this type of manipulation, but neither it nor any anti-virus software can detect when someone substitutes a Trojan or other malicious program for one of your favorite shareware or commercial utilities.

Web and Internet access poses its own risks. Having a top-notch firewall in place to protect your network and implementing other network security measures is a necessity when unscrupulous attackers can penetrate your network from nearly any point on the globe, whether to steal sensitive data or implant malicious code. You should also make sure that your network is not accessible to unauthorized users, and that you have an adequate training program in place to teach and enforce security standards.

To learn about the origin, behavior and other characteristics of particular viruses, consult the Virus Info Library

maintained on the Network Associates website.

Network Associates can provide you with other software in the Total Virus Defense (TVD) suite, the most comprehensive anti-virus solution available, and Total Network Security (TNS), the industry's most advanced network security suite. Network Associates backs them both with outstanding support, training and a worldwide network of research and development teams. Contact your Network Associates representative, or visit the Network Associates website at http://www.nai.com, to find out how to enlist the power of Total Virus Defense onto your side.

See Also

Features of VirusScan
Types of viruses
Why scan for viruses?
About Network Associates

Boot-sector viruses

Early PCs, for example, "booted" or loaded their operating systems from floppy disks. The authors of the Brain virus discovered that they could substitute their own program for the executable code present on the boot sector of every floppy disk formatted with Microsoft's MS-DOS, whether or not it included system files. Users thereby loaded the virus into memory every time they started their computers with any formatted disk in their floppy drives. Once in memory, a virus can copy itself to boot sectors on other floppy or hard disks. Those who unintentionally loaded Brain from an infected floppy found themselves reading an ersatz "advertisement" for a computer consulting company in Pakistan.

With that advertisement, Brain pioneered another characteristic feature of modern viruses: the payload. The payload is the prank or malicious behavior that, if triggered, causes effects that range from annoying messages to data destruction. It's the virus characteristic that draws the most attention—many virus authors now write their viruses specifically to deliver their payloads to as many computers as possible.

For a time, sophisticated descendants of this first boot-sector virus represented the most serious virus threat to computer users. Variants of boot sector viruses also infect the Master Boot Record (MBR), which stores the partition information your computer needs to figure out where to find each of your hard disk partitions and the boot sector itself.

Realistically, nearly every step in the boot process, from reading the MBR to loading the operating system, is vulnerable to viral sabotage. Some of the most tenacious and destructive viruses still include the ability to infect your computer's boot sector or MBR among their repertoire of tricks. Among other advantages, loading at boot time can give a virus a chance to do its work before your anti-virus software has a chance to run.

But boot sector and MBR viruses have a particular weakness: they must spread by means of floppy disks or other removable media, riding concealed in that first track of disk space. As fewer users exchange floppy disks and as software distribution has come to rely on other media, such as CD-ROMs, other virus types have recently eclipsed the boot sector threat. The popularity of large-capacity floppy disks like the Iomega Zip disk and similar disks from Syquest and others, however, could cause a resurgence.

File infector viruses

At about the same time as the authors of the Brain virus found vulnerabilities in the DOS boot sector, other virus writers found out how to use existing software to help replicate their creations. An early example of this type of virus showed up in computers at Lehigh University in Pennsylvania. The virus infected part of the DOS command interpreter COMMAND.COM, which it used to load itself into memory. Once there, it spread to other uninfected COMMAND.COM files each time a user entered any standard DOS command that involved disk access. This limited its spread to floppy disks that contained, usually, a full operating system.

Later viruses quickly overcame this limitation, sometimes with fairly clever programming. Virus writers might, for instance, have their virus add its code to the beginning of an executable file, so that when users start a program, the virus code executes immediately, then transfers control back to the legitimate software, which runs as though nothing unusual has happened. Once it activates, the virus "hooks" or "traps" requests that legitimate software makes to the operating system and substitutes its own responses. Particularly clever viruses can even subvert attempts to clear them from memory by trapping the **CTRL+ALT+DEL** keyboard sequence for a warm reboot, then faking a restart. Sometimes the only outward indication that anything on your system is amiss—before any payload detonates, that is—might be a small change in the file size of infected legitimate software.

Stealth, mutating, encrypted, and polymorphic viruses

Unobtrusive as they might be, changes in file size and other scant evidence of a virus infection usually gives most anti-virus software enough of a scent to locate and remove the offending code. One of the virus writer's principal challenges, therefore, is to find ways to hide his or her handiwork. The earliest disguises were a mixture of innovative programming and obvious giveaways. The Brain virus, for instance, redirected requests to see a disk's boot sector away from the actual location of the infected sector to the new location of the boot files, which the virus had moved. This "stealth" capability enabled this and other viruses to hide from conventional search techniques.

Because viruses needed to avoid continuously reinfecting host systems—doing so would quickly balloon an infected file's size to easily detectable proportions or would consume enough system resources to point to an obvious culprit—their authors also needed to tell them to leave certain files alone. They addressed this problem by having the virus write a code "signature" that would flag infected files with the software equivalent of a "do not disturb" sign. Although that kept the virus from giving itself away immediately, it opened the way for anti-virus software to use the code signatures themselves to find the virus.

In response, virus writers found ways to conceal the code signatures. Some viruses would "mutate" or write different code signatures with each new infection. Others encrypted most of the code signature or the virus itself, leaving only a couple of bytes to use as a key for decryption. The most sophisticated new viruses employed stealth, mutation and encryption to appear in an almost undetectable variety of new forms. Finding these "polymorphic" viruses required software engineers to develop very elaborate programming techniques for anti-virus software.

Macro viruses

By 1995 or so, the virus war had come to something of a standstill. New viruses appeared continuously, prompted in part by the availability of ready-made virus "kits" that enabled even some non-programmers to whip up a new virus in no time. Most existing anti-virus software, however, could easily be updated to detect and dispose of the new virus variants, which consisted primarily of minor tweaks to well-known templates.

But 1995 marked the emergence of the Concept virus, which added a new and surprising twist to virus history. Before Concept, most virus researchers thought of data files—the text, spreadsheet, or drawing documents created by the software you use—as immune to infection. Viruses, after all, are programs and, as such, needed to be able to run in the same way executable software did in order to do their damage. Data files, on the other hand, simply stored information that you entered when you worked with your software.

That distinction melted away when Microsoft began adding macro capabilities to Word and Excel, its flagship applications in its Office suite. Using the stripped-down version of its Visual BASIC language included with the suite, users could create document templates that would automatically format and add other features to documents created with Word and Excel. Virus writers seized the opportunity that this presented to conceal and spread viruses in documents that you, the user, created yourself.

The exploding popularity of the Internet and of e-mail software that allowed users to attach files to messages ensured that macro viruses would spread very quickly and very widely. Within a year, macro viruses became the most potent virus threat ever.

Types of computer viruses

A virus is a software program that attaches itself to another program on a disk or lurks in a computer's memory and spreads from one program to another.

In addition to self-replication, viruses have the capability to damage data, cause computers to crash, and display offending or bothersome messages.

- Boot virus
- File virus
- Stealth virus
- Multi-partite virus
- Mutating virus
- Encrypted virus
- Polymorphic virus

See Also

About viruses
Features of VirusScan
Why scan for viruses
About Network Associates

Boot virus

A boot virus copies itself from the boot sector of one drive to another (e.g. floppy drive to hard drive).

File virus

A file virus attaches itself to a program. Whenever the program runs, the virus attaches itself to other programs.

Stealth virus

A stealth virus hides itself to evade detection. A stealth virus may be a boot virus or a file virus.

Multi-partite virus

A multi-partite virus acts like a boot virus and a file virus by spreading through boot sectors and files.

Mutating virus

Mutating viruses change their shape to avoid detection. Many mutating viruses are also encrypted viruses.

Encrypted virus

Encrypted viruses encrypt part of their code to avoid detection. Many encrypted viruses are also mutating viruses.

Polymorphic virus

Polymorphic viruses are similar to mutating viruses. Upon each instance of copying itself, a polymorphic virus slightly changes its code to avoid detection.

Why scan for viruses?

In today's environment, safe computing practices are no longer a luxury—they are a necessity. Although relatively few viruses have destructive effects, that fact says nothing about how widespread the malicious viruses are. In many cases, viruses with the most debilitating effects are the hardest to detect—the virus programmer bent on causing harm will take extra steps to avoid discovery. In addition, even relatively "benign" viruses can interfere with the normal operation of your computer and can cause unpredictable behavior in other software. Some viruses contain bugs, poorly written code, or other problems severe enough to cause crashes when they run. Other times, legitimate software has problems running when a virus has, intentionally or otherwise, altered system parameters or other aspects of the computing environment. Tracking down the source of resulting system freezes or crashes drains time and money from more productive activities.

Beyond these problems lies a problem of perception: once infected, your computer can serve as a source of infection for other computers. If you regularly exchange data with colleagues or customers, you could unwittingly pass on a virus that could do more damage to your reputation or your dealings with others than it does to your computer.

The threat from viruses and other malicious software is real, and it is growing worse. The International Computer Security Association has estimated the total worldwide cost in time and lost productivity simply of detecting and cleaning virus infections at $1 billion per year, a figure that doesn't include the costs of data loss and recovery in the wake of attacks that destroyed data.

Network Associates' virus scanning solutions should top your list of safe computing practices. Scheduled periodic scans of your computer offer added assurance you are taking precautions against virus infection.

See Also

About viruses
Features of VirusScan
Types of viruses
About Network Associates

About Network Associates

Founded in 1989 as McAfee Inc., Network Associates 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 our network of authorized agent offices in more than 50 countries worldwide.

See Also

About viruses
Features of VirusScan
Types of viruses
Why scan for viruses

Removing a virus found in memory

If VirusScan discovers a virus in memory, follow these steps:

1. Turn off your computer. *Do not reboot using the reset button or CTRL+ALT+DELETE.* If you do, some viruses might remain intact or drop their destructive payloads.
2. Place the emergency disk into the floppy disk drive. See Making an emergency disk.
3. Turn on your computer.
4. Follow the on-screen instructions and remove any viruses found.

If viruses were not removed

If VirusScan could not remove a virus, the following message is displayed:

> *Virus could not be removed.*

If the virus was found in a file, delete that file and repeat steps 1 through 4 above.

If the virus was found in the Master Boot Record, see the Network Associates website for information about manually removing viruses. For more information, see Contacting Network Associates.

If viruses were removed

If VirusScan successfully removes all the viruses:

1. Shut down your computer and remove the emergency disk.
2. Follow the installation procedure described in Chapter 2 of the *VirusScan for Windows 3.1*x *User's Manual*.
3. Scan your diskettes immediately after installation to find and eliminate the source of infection.

Understanding false alarms

A false alarm is a report of a virus in a file or in memory when no virus actually exists. False alarms can occur if you are using more than one brand of virus detection software, because some anti-virus programs store their virus signature strings unprotected in memory. As a result, VirusScan may "detect" them falsely as a virus. Your system's BIOS, use of validation codes, and other factors may also produce false alarms.

Always assume that any virus found by VirusScan is real and dangerous, and take necessary steps to remove it from your system. If, however, you believe that VirusScan is generating a false alarm (for example, it has detected a virus in a file that you have been using safely for years), refer to the list of potential sources below:

- VirusScan may report a false alarm if more than one anti-virus program is running. Set up your computer so that only one anti-virus program is running at a time. Remark out lines in the AUTOEXEC.BAT file that refer to other anti-virus programs. Turn off your computer, wait a few seconds, and turn it on again to make sure that all code from other anti-virus programs is cleared from memory.
- Some BIOS chips include an anti-virus feature that could be the source of false alarms. Refer to your computer's reference manual for details.
- If you set up validation/recovery codes, subsequent scans can detect changes in validated files. This can trigger false alarms if the executable files are self-modifying or self-checking. When using validation codes, specify an exceptions list to exclude such files from checking.
- Some older Hewlett-Packard and Zenith PCs modify the boot sector each time the system is booted. VirusScan may detect these modifications as a possible infection, even though no virus may be present. Check your computer's reference manual to determine whether your PC has self-modifying boot code.
- VirusScan may report viruses in the boot sector or Master Boot Record of certain copy-protected diskettes.

Keeping VirusScan updated

To offer the best virus protection possible, Network Associates continually updates the VirusScan's virus information (.DAT) files, and makes improvements to the VirusScan program itself.

New viruses are discovered at a rate of more than 100 per month. Often, these viruses are not detected using older data files. The data files and scan engine that came with your copy of VirusScan may not detect a virus that was discovered after you bought the product.

See Also

Updating the virus information (.DAT) files
Upgrading the VirusScan software

Updating the virus information (.DAT) files (AutoUpdate)

VirusScan protects your system most effectively when it is using the most up-to-date virus information (.DAT) files. To ensure that this is the case, VirusScan can update these files automatically.

To configure and customize AutoUpdate, follow these steps when the Task Properties window appears:

1. Select the Program page.

4. If desired, type another name for the AutoUpdate in the **Description** text box.

5. The Program text box shows the default location of the AutoUpdate executable file (C:\NETA\ViruScan\MCUPDATE.EXE). If you want to use a different location, enter that path in the text box or browse for the location.

6. The **Start in** text box shows the default starting directory (C:\NETA\ViruScan). If desired, enter another path in the text box or browse for the location.

7. The **Parameters** text box lets you enter the name of a text file that you want to be opened when AutoUpdate is run. For example, you could enter `whatsnew.txt`.

8. Select the size of the window where AutoUpdate will run (**Normal**, **Maximized**, or **Minimized**).

9. Click **Configure** to set additional options for AutoUpdate. See Configuring an update.

10. Click **Run Now** if you want AutoUpdate to run immediately.

11. Click one of the following:

    OK saves the changes and returns to the VirusScan Console.

    Cancel abandons the changes and returns to the VirusScan Console.

    Apply applies the changes. You can then select another page. (If you want to schedule the update, see Scheduling an update.)

Note

Your ability to access updates is legally restricted by the maintenance terms outlined in the README.1ST file accompanying the software and detailed in the software license agreement.

See Also

Upgrading the VirusScan software

Configuring an update

1. Click **Configure** on the Task Properties window.
2. When the Automatic Update page appears, select one or more of the following options:

   To add a site, click **Add**. The McUpdate Configuration window appears. See Selecting update options and Selecting advanced update options for more information.

   To edit a site, select the site name and click **Edit**. The McUpdate Configuration window appears. See Selecting update options and Selecting advanced update options for more information.

   To delete a site, select the site name and click **Delete**.

   To move a site up in the list, select the site name and click **Move Up**.

   To move a site down in the list, select the site name and click **Move Down**.

   To update the virus information files, click **Update now**.
3. Select the Log Activities page.
4. Select the **Log activity into the Activity Log File** check box.
5. Enter the path for the activity log or browse to the desired path. The default path is C:\NETA\ViruScan\ MCUPDATE.LOG.
6. If you want to limit the size of the log file, click the **Limit size of log file** check box. If needed, enter a size (in kilobyte) in the text box.
7. Click one of the following:

   OK saves your changes and returns to the Automatic Upgrade window.

   Cancel returns to the Automatic Upgrade window without saving your changes.

   Apply saves your changes.

See Also

Scheduling an update

Scheduling an update

To schedule this task, follow these steps on the Task Properties window:

1. Select the Schedule page.
2. Select the **Enable** check box.
3. Select when you want the task to run:

    Once
    Hourly
    Daily
    Weekly
    Monthly

See Also

Configuring an update

Selecting update options

When the Update Options page appears, follow these steps:

1. In the **Site Name** text box, type a name that will identify this update site in the list on the Automatic Update page.
2. Clear the **Enabled** check box if you do not want this site to be enabled.
3. Select the transfer method for the update:

   Copy from a local network computer gets the updated virus information files from a computer on your network.

   FTP from a remote network computer gets the updated virus information files from a remote computer via FTP.
4. Enter the path for the network computer or click **Default** to use the default path. (If you chose FTP in Step 1, the default is ftp.nai.com/pub/antivirus/datfiles/4.x.)
5. If the network server requires login information, clear the **Use anonymous FTP login** check box and click **FTP Login Information**. When the dialog box appears, enter your username and password, then click **OK** to return to the Update Options page.
6. If you want to use a proxy server, click the **Use proxy server** check box. Then type the name of the server in the text box and (if needed) a port number in the **Port** text box.
7. Click one of the following:

   OK saves your changes and returns to the Automatic Update window.

   Cancel returns you to the Automatic Update window without saving your changes.

   Apply saves your changes.

See Also

Scheduling an update

Selecting advanced update options

1. On the Advanced Update page, select one or more of these options:

   Backup the existing .DAT files makes a backup copy of the virus information files currently used by VirusScan.

   Retrieve the Update file but do not perform the update.

   Force update .DAT files updates the existing .DAT files even if the downloaded files are no newer than the existing ones. You might use this option if you believe that the existing .DAT files are corrupt.

2. Some updates have components that will not work until your system is rebooted. Select **Reboot system, if needed, after a successful update** to have your system reboot itself automatically.
3. If you want to use the update file later, select **Save the update file for later usage**. Then enter a path in the text box or browse for the location where you want to save the update file.
4. If you want to run a program after the update finishes, select **Run a program after a successful update**. Then enter a path in the text box or browse for the location of the program.
5. Click one of the following:

   OK saves your changes and returns to the Automatic Update window.

   Cancel returns you to the Automatic Update window without saving your changes.

   Apply saves your changes.

Upgrading the VirusScan software (AutoUpgrade)

VirusScan protects your system most effectively when you are running the most up-to-date version of the program. To ensure that this is the case, VirusScan can upgrade itself automatically.

To configure and customize AutoUpgrade, follow these steps when the Task Properties window appears:

1. Select the Program page.
2. If desired, type another name for the AutoUpgrade task in the **Description** text box.
3. The **Program** text box shows the default location of the AutoUpgrade executable file (C:\NETA\ViruScan\MCUPGRADE.EXE). If you want to use a different location, enter that path in the text box or browse for the location.
4. The **Start in** text box shows the default starting directory (C:\NETA\ViruScan). If desired, enter another path in the text box or browse for the location.
5. The **Parameters** text box lets you enter the name of a text file that you want to be opened when AutoUpgrade is run. For example, you could enter `whatsnew.txt`.
6. Select the size of the window where AutoUpgrade will run (**Normal**, **Maximized**, or **Minimized**).
7. Click **Configure** to select the scanning options for AutoUpgrade. See Configuring an upgrade.
8. Click **Run Now** if you want AutoUpgrade to run immediately.
9. Click one of the following:

   OK saves the changes and returns to the VirusScan Console.

   Cancel abandons the changes and returns to the VirusScan Console.

   Apply applies the changes. You can then select another page. (If you want to schedule the upgrade, see Scheduling an upgrade.)

Note

Your ability to access software upgrades is legally restricted by the maintenance terms outlined in the README.1ST file accompanying the software and detailed in the software license agreement.

See Also

Updating the virus information (.DAT) files

Configuring an upgrade

1. When the Automatic Upgrade page appears, select one or more of the following options:

   To add a site, click **Add**. The McUpdate Configuration window appears. See Selecting upgrade options and Selecting advanced upgrade options for more information.

   To edit a site, select the site name and click **Edit**. The McUpdate Configuration window appears. See Selecting upgrade options and Selecting advanced upgrade options for more information.

   To delete a site, select the site name and click **Delete**.

   To move a site up in the list, select the site name and click **Move Up**.

   To move a site down in the list, select the site name and click **Move Down**.

   To update the VirusScan program files, click **Upgrade now**.

2. Select the Log Activities page.
3. Select the **Log activity into the Activity Log File** check box.
4. Enter the path for the activity log or browse to the desired path. The default path is C:\NETA\ViruScan\ MCUPGRADE.LOG.
5. If you want to limit the size of the log file, click the **Limit size of log file** check box. If needed, enter a size (in kilobyte) in the text box.
6. Click one of the following:

   OK saves your changes and returns to the Automatic Upgrade window.

   Cancel returns to the Automatic Upgrade window without saving your changes.

   Apply saves your changes.

Selecting upgrade options

When the Upgrade Options page appears, follow these steps:

1. In the **Site Name** text box, type a name that will identify this upgrade site in the list on the Automatic Upgrade page.
2. Clear the **Enabled** check box if you do not want this site to be enabled.
3. Select the transfer method for the update:

   Copy from a local network computer gets the upgraded program files from a computer on your network.

   FTP from a remote network computer gets the upgraded program files from a remote computer via FTP.
4. Enter the path for the network computer or click **Browse** to browse to the desired path.
5. If the network server requires login information, clear the **Use anonymous FTP login** check box and click **FTP Login Information**. When the dialog box appears, enter your username and password, then click **OK** to return to the Upgrade Options page.
6. If you want to use a proxy server, click the **Use proxy server** check box. Then type the name of the server in the text box and (if needed) a port number in the **Port** text box.
7. Click one of the following:

   OK saves your changes and returns to the Automatic Upgrade window.

   Cancel returns you to the Automatic Upgrade window without saving your changes.

   Apply saves your changes.

See Also

Scheduling an upgrade

Scheduling an upgrade

To schedule this task, follow these steps on the Task Properties window:

1. Select the Schedule page.
2. Select the **Enable** check box.
3. Select when you want the task to run:

    Once
    Hourly
    Daily
    Weekly
    Monthly

See Also

Configuring an upgrade

Selecting advanced upgrade options

On the Advanced Upgrade page, follow these steps:

1. If you do not want to upgrade VirusScan immediately, select the **Retrieve the Upgrade file but do not perform the upgrade** check box.
2. If you want to use the upgrade file later, select **Save the upgrade files for later usage**. Then enter a path in the text box or browse for the location where you want to save the upgrade file.
3. The upgraded program can not run until your system is rebooted. Select **Reboot system after a successful upgrade** to have your system reboot itself automatically.
4. Click one of the following:

   OK saves your changes and returns to the Automatic Upgrade window.

   Cancel returns to the Automatic Upgrade window without saving your changes.

   Apply saves your changes.

Schedule once

1. Type the time when the task should run, in 24-hour format. For example, 3 P.M. should be entered as 15:00, not as 3:00.
2. Select the month when the task should run.
3. Type the date and year when the task should run. Enter the date as two digits. For example, the fifth day of the month should be entered as "05."

Schedule hourly

Type the number of minutes after the hour when the task should run.

Schedule daily

1. Type the time when the task should run, in 24-hour format. For example, 3 P.M. should be entered as 15:00, not as 3:00.
2. Select the check box(es) for the day(s) when the task should run.

Schedule weekly

1. Type the time when the task should run, in 24-hour format. For example, 3 P.M. should be entered as 15:00, not as 3:00.
2. Select the day of the week when the task should run.

Schedule monthly

1. Type the time when the task should run, in 24-hour format. For example, 3 P.M. should be entered as 15:00, not as 3:00.
2. Type the day of the month when the task should run in two-digit format. For example, the fifth day of the month should be entered as "05."

Contacting Network Associates

Select from the following:

- Customer service
- Technical support
- Training

Customer service

To order 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.

See Also

Technical support
Training

Technical support

Network Associates is famous for its dedication to customer satisfaction. The company has continued this tradition by making the Network Associates site on the World Wide Web a valuable resource for answers to technical support issues. Bookmark this site so that you can make it your first stop for answers to frequently asked questions, for updates to Network Associates software, and for access to Network Associates news and virus information.

World Wide Web	http://support.nai.com

To access the Network Associates web site, click here.

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

Internet e-mail	support@nai.com
CompuServe	GO NAI
America Online	Keyword MCAFEE

If the automated services did not solve your problem, you may contact Network Associates Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

For corporate-licensed customers:

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

For retail-licensed customers:

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

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

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

See Also

Customer service
Training

Network Associates Training

For information about scheduling on-site training for any Network Associates product, call (800) 395-3151.

See Also

Customer service
Technical support

Preventing virus infection

VirusScan is an effective tool for preventing, detecting, and recovering from virus infection. However, it is most effective when part of a comprehensive computing security program that includes a variety of safety measures, such as regular backups, meaningful password protection, user training, and awareness.

To create a secure system environment and minimize your chance of infection, Network Associates recommends that you review the following topics:

Making an emergency disk

The emergency disk is a very important part of proper virus prevention. Should your system become infected, an emergency disk will enable you to start your computer from a clean environment.

Your system must be virus free before you make an emergency disk, otherwise any virus residing in your system get onto the emergency disk and reinfect your system. If your computer is infected, go to another computer and scan it. If the computer is virus-free, complete one of the procedures below:

Automatically creating an emergency disk

To use VirusScan's utility for automatically creating an emergency disk, follow these steps:

1. Open the VirusScan program group and double-click the Create Emergency Disk icon.
2. Insert a blank diskette into the A: drive.
3. Click **OK**. The utility begins creating the emergency disk.
4. When the utility is finished, remove the disk, write-protect it, label it "VirusScan Emergency Disk", and store it in a safe place.

Manually creating an emergency disk

Start this procedure from a command prompt (C:\>). If you are in Windows, you must open a DOS shell to get the prompt.

5. Insert a blank, *unformatted* 1.44MB diskette into your floppy drive.
6. Type this command at the MS-DOS prompt, substituting the drive letter for your floppy drive in place of <*drive*>:

   ```
   format <drive>: /s/u/v
   ```

   If you are using DOS 5.0 or an earlier version of DOS, do not type the /u. If you are unsure of which version you are using, type **ver** at the C:\> prompt for version information.
7. Press **ENTER**. This tells your system to format the diskette you inserted, to overwrite any existing information on it, to copy DOS system files to it, and to have DOS prompt you to enter a volume label for it.
8. When DOS prompts you for a volume label, enter a name up to 11 characters long that distinguishes this disk from others.
9. If you have VirusScan installed on your computer and in its default program directory, change to the correct directory by typing this command at the MS-DOS prompt:

   ```
   cd\progra~1\neta~1\mcafee~1
   ```

   If you do not have VirusScan installed, change to the directory that contains the VirusScan files you extracted, or to the VirusScan directory on your CD-ROM drive.
10. Type the commands listed below at the MS-DOS prompt to copy the correct files to the emergency disk, substituting the drive letter for your floppy drive in place of <*drive*>:

    ```
    copy bootscan.exe <drive>:
    copy emscan.dat scan.dat <drive>:
    copy emnames.dat names.dat <drive>:
    copy emclean.dat clean.dat <drive>:
    copy license.dat <drive>:
    copy messages.dat <drive>:
    copy edwiz16.exe <drive>:
    ```
11. Copy to the emergency disk any other DOS utilities you need to start your computer, debug your system software, manage any extended or expanded memory you have, or perform other tasks at startup. If you use a disk compression utility, be sure to copy the drivers you need to uncompress your files.
12. When you have finished copying files to the emergency disk, label it, lock it, and store it in a safe place.

    A locked diskette shows two holes near the edge of the disk opposite the metal shutter. If you don't see two holes, look for a plastic sliding tab at one of the diskette corners, then slide the tab until it locks in an open position. Because no software can save to a locked diskette, viruses cannot infect files stored on one.

Write-protecting a diskette

1. Position the diskette face down with the metal slide facing you.
2. Examine the small rectangular hole on the upper-left side. There should be a square, plastic tab that you can slide up and down across the hole.
3. To write-protect the diskette, slide the plastic tab upward toward the edge of the diskette so that the hole is open.

Note

If there is no tab and the hole is open, the diskette is already write-protected.

Compressed files

When enabled, VirusScan unpacks files compressed with PKLite, LZEXE, Diet, and MSCompress scans the decompressed form. Files with .ZIP and .LZH extensions are not scanned for viruses.

Move infected files

When this option is selected, VirusScan automatically moves infected files to the specified directory. To select a directory, enter the directory location or click **Browse** to select a directory.

After the file is moved to the quarantine directory, you can clean the file or restore the file from backups and return it to its original location. To return the file to the original directory location, refer to the VShield log file (VSHLOG.TXT) or the VirusScan on-demand scanning log file (VSCLOG.TXT).

Clean infected files

When this option is selected, VirusScan automatically attempts to remove the virus from the infected file.

Delete infected files

When this option is selected, VirusScan automatically deletes infected files. After VirusScan deletes the infected files, you can restore them from backup.

If you select this option, make sure to enable report logging. This will ensure you have a record of which files were deleted, so you can restore them from backups.

Continue scanning

When this option is selected, VirusScan continues scanning without taking any action. When the scan is complete, you can manually respond to each infected file in the VirusScan Main window.

This option is not recommended for unattended machines.

Prompt for action

When this option is selected, VirusScan prompts you for action for each infected file.

Safe computing practices

Safe computing practices include:

- Virus protection
- Regular backups
- Meaningful password protection
- Training and awareness

Centralized Alerting

Centralized Alerting is 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.

To configure Centralized Alerting, do the following:

1. Ask a system administrator for the name of a server running NetShield and its Centralized Alerting directory.
2. Make sure you have rights to this directory.
3. Configure VShield and VirusScan tasks to send network messages to this directory.

Program files

To add or remove file types from the program files list, click **Extensions**. The Program File Extensions dialog box appears.

1. To add a file extension, click **Add**. Enter a new file extension to scan and click **OK**. Repeat this procedure until all desired file extensions are entered.
2. To delete an extension, select it and click **Delete**.
3. To return to the default extensions, click **Default**.
4. When you are finished editing the list of file extensions, click **OK**.

Virus name

Lists the name of the virus.

Infects

Indicates the types of files infected by this virus. This may include:

- Executables (.EXE)
- COM files (.COM)
- Microsoft Word files (.DO?)
- Microsoft Excel files (.XL?)

Virus size

Indicates the size of the virus in kilobytes.

Memory resident

Indicates whether the virus resides in memory.

Encrypted

Indicates whether this is an encrypted virus.

Polymorphic

Indicates whether this is a polymorphic virus.

Repairable

Indicates whether files infected by this virus are repairable.

Macro virus

Indicates whether this is a Word or Excel macro virus.

Type

Specifies the type of file that is infected (for example, executable, Word, or Excel files).

Location

Specifies the directory location of the infected file.

Size

Specifies the size of the infected file.

MS-DOS name

Specifies the name of the infected file.

Created

Specifies the date the infected file was created.

Modified

Specifies the date the infected file was last modified.

Accessed

Specifies the date the infected file was last accessed.

Read-only

Specifies whether the file is read-only.

Hidden

Specifies whether the file is hidden.

Archive

Specifies whether the file is an archive file.

System

Specifies whether the file is a system file.

VirusScan DOS error levels

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. For more information, see your DOS operating system documentation.

VirusScan can return the following error levels:

ERRORLEVEL	Description
0	No errors occurred; no viruses were found.
2	Data file integrity check failed.
6	A general problem.
8	Could not find a data file.
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 /FREQUENCY switch.
102	User quit via ESC-X, CTRL+C, or Exit button. This can be disabled with the /NOBREAK command-line option.

VSC file format

The VSC file is a configuration text file, similar in format to the Windows INI file, which outlines VirusScan's settings. Each variable in the file has a name followed by the equal sign (=) and a value. The values define which settings have been selected for VirusScan configuration. The variables are arranged in eight groups: ScanOptions, DetectionOptions, AlertOptions, ActionOptions, ReportOptions, ScanItems, SecurityOptions, and ExcludedItems. To edit the VSC file, open it with a text editor, such as Notepad.

Note

In Boolean variables, the possible values are 0 and 1. The 0 value instructs VirusScan to disable the setting, while 1 indicates that the setting is enabled.

ScanOptions (VSC)

Variable	Description
bAutoStart	Type: Boolean (0/1) Instructs VirusScan to automatically start scan when launched Default Value: 0
bAutoExit	Type: Boolean (0/1) Instructs VirusScan to exit automatically when finished scanning Default Value: 0
bAlwaysExit	Type: Boolean (0/1) Instructs VirusScan to always exit when finished scanning Default Value: 0
bSkipMemoryScan	Type: Boolean (0/1) Instructs VirusScan to skip memory scan Default Value: 0
bSkipBootScan	Type: Boolean (0/1) Instructs VirusScan to skip boot sector scanning Default Value: 0
bSkipSplash	Type: Boolean (0/1) Instructs VirusScan not to display the VirusScan splash screen on startup Default Value: 0

DetectionOptions (VSC)

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 inside compressed files Default value: 1
szProgramExtensions	Type: String Defines extensions to be scanned Default value: EXE COM DO? XL?
szDefaultProgram Extensions	Type: String Defines extensions to be used as default program extensions during scan configuration Default value: EXE COM DO? XL?

AlertOptions (VSC)

Variable	Description
bNetworkAlert	Type: Boolean (1/0) Instructs VirusScan to send a Centralized Alerting notification to a server running NetShield Default value: 0
szNetworkAlertPath	Type: String Defines the path to the server running NetShield Default value: none
bSoundAlert	Type: Boolean (1/0) Instructs VirusScan to sound an alert when a virus is detected Default value: 1

ActionOptions (VSC)

Variable	Description
bDisplayMessage	Type: Boolean (1/0) Defines if custom message should be displayed upon virus detection Default value: 0
ScanAction	Type: Integer (1-5) Instructs VirusScan to take the action specified when a virus is detected Possible values: 1 - Prompt for action 2 - Move infected files to a folder 3 - Clean infected files automatically 4 - Delete infected files automatically 5 - Continue scanning Default value: 2
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: 1
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: Your custom message

ReportOptions (VSC)

Variable	Description
bLogToFile	Type: Boolean (0/1) Instructs VirusScan to log scan activity to a file Default Value: 1
bLimitSize	Type: Boolean (0/1) Instructs VirusScan to limit the size of the log file Default Value: 1
uMaxKilobytes	Type: Integer (10-999) Specifies maximum size of log file in kilobytes Default Value: 10
bLogDetection	Type: Boolean (0/1) Instructs VirusScan to log virus detection Default Value: 1
bLogClean	Type: Boolean (0/1) Instructs VirusScan to log virus cleaning Default Value: 1
bLogDelete	Type: Boolean (0/1) Instructs VirusScan to log file deletions Default Value: 1
bLogMove	Type: Boolean (0/1) Instructs VirusScan to log file moves Default Value: 1
bLogSetting	Type: Boolean (0/1) Instructs VirusScan to log session settings Default Value: 1
bLogSummary	Type: Boolean (0/1) Instructs VirusScan to log session summaries Default Value: 1
bLogDateTime	Type: Boolean (0/1) Instructs VirusScan to log date and time of scan activity Default Value: 1
bLogUserName	Type: Boolean (0/1) Instructs VirusScan to log user name Default Value: 1
szLogFileName	Type: String

	Specifies path to log file Default Value: C:\NETA\Viruscan\VSCLOG.TXT

ScanItems (VSC)

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

SecurityOptions (VSC)

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

ExcludedItems (VSC)

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

VSH file format

The VSH file is a configuration text file, formatted similarly to the Windows .INI file, which outlines VShield's settings. Each variable in the file has a name followed by the equal sign (=) and a value. The values define which settings have been selected for VShield configuration. The variables are arranged in seven groups:

- General
- DetectionOptions
- AlertOptions
- Action Options
- ReportOptions
- SecurityOptions
- ExclusionOptions

To edit the VSH file, open it with a text editor, such as Notepad.

Note

In Boolean variables, the possible values are 0 and 1. The 0 value instructs VirusScan to disable the setting, while 1 indicates that the setting is enabled.

General (VSH)

Variable	Description
bLoadAtStartup	Type: Boolean (1/0) Defines if VShield should be loaded at system startup Default value: 1
bCanBeDisabled	Type: Boolean (1/0) Defines if VShield can be disabled Default value: 1
bShowTaskbarIcon	Type: Boolean (1/0) Defines whether VShield taskbar icon is displayed Default value: 1
bNoSplash	Type: Boolean (1/0) Instructs VShield to not show splash screen when program is launched Default value: 0

DetectionOptions (VSH)

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

AlertOptions (VSH)

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

ActionOptions (VSH)

Variable	Description
szCustomMessage	Type: String Defines custom message to be displayed upon virus detection if action is set to Prompt for Action Default value: Possible Virus Detected
szMoveToFolder	Type: String Defines folder to which infected files should be moved Default value: \Infected
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 for action 2 - Move infected files to a folder 3 - Clean infected files automatically (Deny access if files can't be cleaned) 4 - Delete infected files automatically 5 - Deny access to infected files Default value: 1
bButtonClean	Type: Boolean (1/0) Instructs VShield to give user option of cleaning file if Prompt for Action is selected and a virus is detected Default value: 1
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: 1

bButtonStop	Type: Boolean (1/0) Instructs VShield to give user option of denying access to the infected file if Prompt for Action is selected and a virus is detected Default value: 1

ReportOptions (VSH)

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) Defines if scanning results should be logged Default value: 1
bLogClean	Type: Boolean (1/0) Defines if cleaning results should be logged Default value: 1
bLogDelete	Type: Boolean (1/0) Defines if infected file delete operations should be logged Default value: 1
bLogMove	Type: Boolean (1/0) Defines if infected file move operations should be logged Default value: 1
bLogSettings	Type: Boolean (1/0) Defines if session settings should be logged on shutdown Default value: 1
bLogSummary	Type: Boolean (1/0) Defines if session summary should be logged on shutdown Default value: 1
bLogDateTime	Type: Boolean (1/0) Defines if time and date of an event should be logged Default value: 1
bLogUserName	Type: Boolean (1/0) Defines if user name should be logged

Default value: 1

szLogFileName Type: String
Defines log file name
Default value: C:\NETA\Viruscan\Vshlog.txt

SecurityOptions (VSH)

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

ExclusionOptions (VSH)

Variable	Description
szExclusionsFileName	Type: String This option is not user-configurable.
NumExcludedItems	Type: Integer (0-n) Defines the number of items excluded from on-access scanning Default value: 0
ExcludedItem_*x*, where *x* is a zero-based index	Type: String Instructs VShield to exclude the item from on-access scanning Default value: \Recycled|*.*|1|1 NOTE: 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 2 - Instructs VShield to not exclude subfolders

Centralized Alerting ALR file format

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	
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.

Testing your installation

The Eicar Standard AntiVirus Test File is a combined effort by anti-virus vendors throughout the world to create a single standard by which customers can verify their anti-virus installations.

To test your installation:

1. Open a text editor (such as Notepad) and type the line below. (If you are reading this manual on your computer, you can copy and paste the line directly to Notepad.)

   ```
   X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
   ```

   Make sure that this character string appears on a single line in the actual file.

2. Save the file and name it EICAR.COM. The file size will be 69 or 70 bytes.

3. Start VirusScan and let it scan the directory that contains EICAR.COM. VirusScan will report finding the EICAR-STANDARD-AV-TEST-FILE virus.

   Despite what VirusScan reports, this file is not a virus. It cannot spread or harm your system.

4. Delete the EICAR.COM file when you have finished testing your installation so that you don't alarm other users.

Note

Because the Eicar Standard AntiVirus Test File is not a true virus infection, you will not be able to clean or repair the infected file.

Macros, below

Emergency disk creation utility

Please wait while the emergency disk creation utility loads.

Note

If this takes more than a few seconds, please start the emergency disk creation utility manually. To start the utility manually, open the VirusScan program group and double-click the **Create Emergency Disk** icon.

Network Associates website

Please wait while we access the Network Associates website.

Notes

To access the Network Associates website, you must have an active connection to the Internet and you must have a copy of Netscape Navigator or Microsoft Internet Explorer. If you do not have one of these browsers, but have access to the World Wide Web, you can access the website at http://support.nai.com.

VShield properties

Please wait while VShield loads.

Note

If this takes more than a few seconds, please start VShield manually. To start VShield manually, open the VirusScan program group and double-click the **VShield** icon.

VirusScan Console

Please wait while the VirusScan Console loads.

Note

If this takes more than a few seconds, please start the VirusScan Console manually. To start the VirusScan Console manually, open the VirusScan program group and double-click the **VirusScan Console** icon.

VirusScan's on-demand scanner

Please wait while VirusScan loads.

Note

If this takes more than a few seconds, please start VirusScan manually. To start VirusScan manually, open the VirusScan program group and double-click the **VirusScan** icon.

Adobe website

Please wait while we access the Adobe website.

Note

To access the Adobe website, you must have an active connection to the Internet and you must have a copy of Netscape Navigator or Microsoft Internet Explorer. If you do not have one of these browsers, but have access to the World Wide Web, you can access the website at http://www.adobe.com.

VShield Virus Activity log

Please wait while the activity log loads.

Note

If the activity log does not open, either the **Log to file** option is not active or you are not using the default log file name. To manually open the VShield activity log, simply open the file defined on the Report page with any text editor (such as Notepad).

Virus Activity log (On Demand)

Please wait while the activity log loads.

Note

If the activity log does not open, either the **Log to file** option is not active or you are not using the default log file name. To open the activity log, select **View Activity Log** from the File menu.

end macros

VirusScan User's Manual

The VirusScan User's Manual is in the Adobe Acrobat format (PDF) and is available on the VirusScan CD-ROM. To open the VirusScan User's Manual, start Adobe Acrobat and open WSCDOC31.PDF.

Note

You must have the Adobe Acrobat Reader version 3.0 installed to view the manual. The Acrobat reader is available on the CD-ROM version of this product or can be downloaded from www.adobe.com. To access the Adobe website, click here.

Context-sensitive, below

Program files

1. To add a file extension, click **Add**.
2. Enter a new file extension to scan and click **OK**.
3. Repeat Steps 1 and 2 until all desired file extensions are entered.
4. When you are finished editing the list of file extensions, click **OK**.

Tips

To delete an extension, select it and click **Delete**.
To return to the default extensions, click **Default**.

Adding a scan item

To add files, directories, or drives to a scan:

1. Select **Select item to scan**.
2. Select one of the following:

   To scan all drives attached to this select **My Computer**.
   To scan all removable media, including floppy drives, select **All Removable Media**.
   To scan all hard drives attached to this computer, select **All Fixed Disks**.
   To scan all mounted network drives, select **All Network Drives**.
3. Do one of the following:

   After selecting a scan item, click **OK**.
   To exit without adding a scan item, click **Cancel**.

To add an individual drive or directory to a scan:

1. Select **Select drive or directory to scan**.
2. Enter a path to the item to scan or click **Browse** to locate one.
3. Do one of the following:

   After selecting a scan item, click **OK**.
   To exit without adding a scan item, click **Cancel**.

Excluding items from a scan

1. Enter the full path to a file, drive, or directory or click **Browse** to locate one.
2. To exclude subdirectories from scanning, select the **Include subdirectories** check box.
3. To exclude the item from file scanning, select the **File scanning** check box.
4. To exclude the item from boot sector scanning, select the **Boot sector scanning** check box.
5. Do one of the following:

   After excluding the scan item, click **OK**.
   To exit without adding a scan item, click **Cancel**.

Notes

To edit a scan item, select the item and click **Edit**.
To remove a scan item, select the item and click **Remove**.

To change the password

1. Enter a new password.
2. Reenter the password.

Virus List

The Virus List helps you locate information about your virus. To find out about your virus, follow these steps:

1. Choose **Virus List** from the Tools menu.

   If VirusScan finds your web browser, a browser window will open at the Virus Info Library page of the Network Associates website.

   If VirusScan cannot find your web browser:

   Type its path in the dialog box that appears or browse to the browser location.

   Click **OK**. A browser window will open at the Virus Info Library page of the Network Associates website.

2. Select the type of virus information you want:

   By type

   By name

   By payload activation date