NORMAN

Norman Virus Control for DOS and Windows 3.1x

User's Guide

Version 4.70

Norman ASA
Mailing address: P.O. Box 43, N-1324 Lysaker, Norway Physical address: Strandveien 37, Lysaker
Tel. +47 10 97 00 Fax. +47 67 58 99 40 E-mail: norman@norman.no

Norman Data Defense Systems Inc
9302 Lee Highway Suite 950a, Fairfax, VA 22031, USA
Tel. +1703 267 6109 Fax. +1703 934 6367 E-mail: norman@norman.com

Norman Data Defense Systems GmbH
Kieler Str. 15, D-42697 Solingen, Germany
Tel. +49 212/26718 0 Fax. +49 212/26718 15 E-mail: norman@norman.de

Norman/SHARK BV
Mailing address: P.O. Box 159, NL-2130 AD Hoofddorp, The Netherlands
Tel. +31 23 563 3960 Fax. +31 23 561 3165 E-mail: sales@shark.nl

Norman Data Defense Systems AG
Postfach, CH-4015 Basel, Switzerland
Tel. +41 61 487 25 00 Fax. +41 61 487 25 01 E-mail: norman@norman.ch

Norman Data Defense Systems Pty. Ltd.
6 Sarton Road, Clayton, Victoria, 3168 Australia
Tel. +61 3 9562-7655 Fax. +61 3 9562-9663 E-mail: norman@norman.com.au

Limited warranty

Norman guarantees that the enclosed diskette/CD-ROM and documentation do not have production flaws. If you report a flaw within 30 days of purchase, Norman will replace the defective diskette/CD-ROM and/or documentation at no charge. Proof of purchase must be enclosed with any claim.

This warranty is limited to replacement of the product. Norman is not liable for any other form of loss or damage arising from use of the software or documentation or from errors or deficiencies therein, including but not limited to loss of earnings.

With regard to defects or flaws in the diskette/CD-ROM or documentation, or this licensing agreement, this warranty supersedes any other warranties, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

In particular, and without the limitations imposed by the licensing agreement with regard to any special use or purpose, Norman will in no event be liable for loss of profits or other commercial damage including but not limited to incidental or consequential damages.

This warranty expires 30 days after purchase.

The information in this document as well as the functionality of the software is subject to change without notice. The software may be used in accordance with the terms of the license agreement. The purchaser may make one copy of the software for backup purposes. No part of this documentation may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the explicit written permission of Norman.

Who Should Read This Manual?

This manual is intended for users familiar with the DOS and Windows user interface. Please refer to the *Administrator's Guide* for details about network use and communication.

Reference to the Modules

NVC is made up of modules with different functions. In this manual we refer to the specific modules by specifying the program's file name. The file names and their corresponding modules are:

CLAW31.EXE	Cat's Claw, see page 38.
NVC.SYS	The Smart Behavior Blocker, see page 16.
NVCSYS.EXE	Message Control, see page 36.
NVC32X.EXE	Command Line Scanner, see page 108.
NVCW.EXE	Menu-driven interface for Windows scanner, see page 66.
BG.EXE	BootGuard, see page 52.

Conventions

Throughout this manual, we use several typeface conventions.

Examples of commands that should be typed or messages that appear on the screen look like this:

```
format a: /s /u [Enter]
```

If certain keys should be used, they will appear with square brackets around the name of the key, as in:

[Ctrl]

When we describe a series of menu choices for you to choose, we will use the following:

Start|Run

Important notes appear as:

Note: This is important...

And particularly important text appears in **bold**.

About This Version

The Scanning Engine

The scanning engine has yet again undergone substantial changes. The most prominent improvement is boot sector cleaning. In previous versions, we used the DOS-based program NVCLEAN for removal of boot sector viruses. As of this version, the scanning engine itself can repair infected boot sectors. NVCLEAN is removed altogether.

Removing boot sector viruses is not riskier than removing a binary file virus, for example. However, if things go wrong, a damaged boot sector is a serious situation. For this reason we do not allow *automatic* repair of boot sector viruses on hard drives. Whenever you order NVC to remove a boot sector virus, you will be prompted for backing up your current boot sector. We'll spare you the details until the situation occurs, and guide you from there.

Other changes to the scanning engine are:

- Support for Excel Formula viruses
- Extended detection of polymorphic macro viruses

General

As always, there are a number of bug fixes and minor changes to the program. Please refer to the readme text file for an overview.

Table of Contents

Introduction

About Norman

Norman is a multi-national company that was established in Norway in 1984. Then, as today, Norman's business was developing and selling security software for PCs and data security consulting. We also offer protection with FireWall in an integrated software/hardware solution. Over the years, Norman has opened offices in the United States, Germany, Australia, the Netherlands, Switzerland, Sweden, Finland, and the UK, and has partners in the Far East.

As computer use rises, so does our dependence on the information stored in those computers. The value of computers today must be measured not by the worth of the hardware but by the worth of the information inside. We have all heard the adage "an ounce of prevention is worth a pound of cure". If you are concerned about data integrity, this is advice truly worth heeding. To properly and efficiently defend your data, you must prevent unauthorized entry and action that can lead to data disaster. Norman provides computer users with a wide range of products designed to work together in order to prevent data loss both on workstations and network servers.

Norman's approach to data defense is based on a Cross-Platform Strategy, which includes security solutions for DOS, Windows, OS/2, Windows NT, Windows 9x and Novell NetWare.

Why Use Norman Virus Control

One of the most high-profile threats to data integrity is the computer virus. Computer viruses are an international problem, which is becoming more severe each year as the number of viruses written each year is growing exponentially. The effects of computer viruses can range from loss of productivity to data loss, but a computer virus incident almost always results in high levels of frustration and most importantly, gross expenditures for virus removal. Norman Virus Control products prevent against, detect and recover from virus infections.

Flexibility

Norman Virus Control (NVC) for DOS and Windows 3.1x does not simply scan your systems like other products — it protects your systems from known and unknown viruses. NVC achieves this feat by using several integrated modules designed to work with other Norman products, including our anti-virus protection for NetWare. You may configure NVC's modules to best suit your environment's needs. Included in NVC are:

- Smart Behavior Blocker©
- Cat's Claw
- generic file virus protection
- virus scanner
- virus remover

Together, these components protect memory, boot areas, and files from infection by computer viruses.

In addition, NVC's DOS based modules are self-protecting so that they can be run in an already-infected environment.

Quality

Norman software is of high quality, based on advanced technology, but we realize that no software is perfect.

Through feedback from our customers and cultivation of new techniques, we continuously seek to improve the quality of our products.

Support

Understanding viruses and how to deal with them is not always easy. Having Norman products installed helps, but sometimes you may need some assistance with a virus or with deciding what the best configuration is for you. That's why we provide you with solid technical support, whether you simply have a question about how to use our products or whether a virus is making the rounds in your organization.

Preparing to Use NVC

What's in the Package

NVC is a set of integrated modules that you may use in whichever combination that is best for you. The following table charts out the modules and their functions.

Cat's Claw (CLAW31.EXE)

Cat's Claw is an application specially designed to monitor and protect your system against viruses.

Cat's Claw will scan for viruses in files as they are being opened. Whenever possible, an infected file is repaired before the file is handed over to the application. If repair is not possible, you will receive a message and access to the infected file is blocked.

See "Cat's Claw" on page 38.

Menu-driven scanner

For Windows.

See "The Windows Scanner" on page 66.

Command line scanner

For DOS

See "Command Line Scanning" on page 108.

Smart Behavior Blocker

Resident, behavior blocking device driver. Monitors activity and intercepts virus-like behavior. Protects against known and unknown file viruses. Detects known and unknown boot viruses. Also detects and removes known and unknown boot viruses on diskettes.

NVC.SYS is the cornerstone of NVC's anti-virus protection.

Does not identify viruses by name. Use one of Norman's scanners for identification.

See "NVC.SYS, Norman's Smart Behavior Blocker" on page 16.

BootGuard

Generic boot area protection and restoration.

See "Boot Guard, Generic Boot Area Protection" on page 52.

Canary

Non-resident, early warning detector of file viruses.

See "Generic Detection with Canary" on page 58.

Scheduler

Schedules scans in the Windows environment.

See "Scheduling" on page 115.

Note: If you are planning on installing Windows 9x, then you should uninstall NVC for DOS/Windows 3.1x first. After the installation, we recommend that you install NVC for Windows 9x.

We also recommend that you disable NVC.SYS (The Smart Behavior Blocker) before you install new programs on your PC.

This does not apply for NVC upgrades.

Understanding How the Modules Work Together

Now that you know what each module does, you should know more about how the modules work together in order to decide which ones to use.

Module	Works with...
Cat's Claw	Standalone program using the same virus definition file as the scanners.
NVC.SYS	**FireBreak**: NVC.SYS sends virus alert messages to FireBreak, which in turn, sends messages to the user, a NetWare group, the server console, and a network printer. FireBreak can also send this alert along as an SNMP trap. **BootGuard**: NVC.SYS protects memory for BootGuard. However, neither requires the other. **Windows message control**: NVC.SYS leaves virus alert messages for the Windows message control to pick up.
BootGuard	**NVC.SYS**: NVC.SYS protects memory for BootGuard. However, neither requires the other.
Canary	Standalone program.

Module	Works with...
Command line scanner	**FireBreak**: The command line scanner sends virus alert messages to FireBreak, which in turn, sends messages to the user, a NetWare group, the server console, and a network printer. FireBreak can also send this alert along as an SNMP trap.
Menu-driven scanner	**FireBreak**: The Windows menu-driven scanner sends virus alert messages to FireBreak, which in turn, sends messages to the user, a NetWare group, the server console, and a network printer. FireBreak can also send this alert along as an SNMP trap. **SNMP**: If you have the SNMP extension for our Windows scanner installed, you can send messages over the network as SNMP traps.
Scheduler	**Windows menu-driven scanner**: The scheduler scans periodically, at the user's discretion.

Installing

Before Installing

There are three situations that you should address before installing NVC:

1. If you have a version of an anti-virus product installed, you should uninstall this before installing NVC.
2. If you are planning on installing Windows 9x after installing NVC, then please be aware that the current version of NVC.SYS is incompatible with Windows 9x and must be disabled **before** installing Windows 9x. (Either REM out the `device=c:\norman\nvc.sys` line in `CONFIG.SYS` or delete the line altogether and then reboot)

Note: You should **always** disable NVC.SYS when you install upgrades of the operating system or add new applications.

---

3. If you have a version of BootGuard installed from a version of NVC prior to v3.48 and you are going to install Windows 9x, you must disable BootGuard before installing Windows 9x. (Either REM out the `c:\norman\bg.exe` line in `AUTOEXEC.BAT` or delete the line altogether and then reboot.)

Note: If you abort the setup program during the installation, the files already copied to your hard drive will **not** be automatically removed

---

Step by Step

Note: If you receive your NVC version on CD-ROM, then follow the installation procedure in the CD booklet.

1. Close all Windows applications. From Program Manager you choose File|Run. On the command line, type:

   ```
   a:setup
   ```

2. Norman Virus Control will start to install.
3. Follow the instructions on the screen.

Note: When the **Back** button is active during the installation procedure, you can click on this to return to the previous screen. You can therefore go back to check on the choices you made and, if necessary, make changes.

4. You will see following screen:

If you want to create an Emergency scan diskette, you should do it now. Check the [ ] **Emergency** radio button and let setup copy the files you need onto a diskette. Label

the diskette properly, write-protect it and store it a safe place.

The default installation is **Typical**. This choice provides the basic level of protection and is sufficient for most users. The following modules are included in the **Typical** installation:

- Cat's Claw
- Smart Behavior Blocker for DOS
- Norman Virus Control (NVC), which includes the following functions:
  - scanner
  - scheduler
- BootGuard for DOS
- Help Files for NVC

Check the [ ] **Custom** radio button and click on **Next** if you want to customize your installation. Then you can choose which modules you want to install in addition to the default modules:

- Canary for DOS
- Norman Virus Control (NVC) Command Line
- The Norman Book on Viruses

Please refer to the section "Understanding How the Modules Work Together" on page 5 for an explanation of the functionality.

Currently installed components of Norman Virus Control will be updated.

Note: If you selected [ ] **Custom** install, then you can change the destination directory from this display. Click on the **Browse** button and choose directory for installation.

If you specify a non-existent directory, setup will create it for you.

---

5. If you selected [ ] **Typical** install, you can choose directory for the NVC files from the display "Choose Destination Location". Click on the **Browse** button and choose directory for installation.

   By default, NVC's executable files are installed to C:\NORMAN\WIN16 and C:\NORMAN\DOS. Other files, like readme, configuration and definition files, will be copied to C:\NORMAN.
6. In the next screen, "Select Program Folder", you can decide where to install the program icons. You can view existing program folders displayed in a list. If you specify a new program group name, then the setup program will create this.
7. Unless you have specified another directory, NVC's will copy files to the C:\NORMAN directory and necessary subdirectories, dependent on the modules you selected.

Note: Setup will erase all files from the installation directory before copying the new files. If you are updating from a previous version which resides in the installation directory and this directory holds files you want to keep, you should exit setup now, back up the files you want to keep, and then resume setup.

---

8. When the installation is completed, the screen "Modifying File" appears. This display informs you that the setup program will change the path in one or more of your system files. Depending on your choices in the display "Setup Type", these files could be `win.ini`, `autoexec.bat` and/or `config.sys`. You can let setup make these changes, save changes in a backup file or not make any changes at all.
9. Setup is now complete. From the final display you can browse the Read Me file and launch Norman Virus Control.

In the chapter “Getting Started with NVC for Windows 3.1x” we will give you useful hints about all the functions in Norman Virus Control for Windows 3.1x.

Recovering from Virus Infections

Each day, many PC users get infected by one or more computer viruses. Although some viruses are admittedly dangerous, most that are "in the wild" are harmless. While viruses are cause for concern, please do not panic. A few deep breaths combined with the following few steps will get you through this.

1. Do not begin deleting files. Chances are good that removal of the virus from files is possible.
2. Backup critical data.

Note: If you think (or know) that you have a virus, then you should first backup your critical data to a diskette or whichever backup media you are using. Since some of the files being backed up may be infected, label the backups "possibly infected" and include the date as well as a note that associates it with the machine in question.

Note: You should use fresh backup media instead of overwriting previously used backup media.

---

3. Boot from an uninfected, write-protected bootable diskette so that we can bypass the virus that is on your machine.

You should have an uninfected, bootable diskette from which you can boot your machine. If you have not made one for yourself, then your operating system installation diskettes will most probably be bootable.

Note: If your bootable diskette is infected with a boot virus, you will end up infecting your machine. If you are not sure

about the state of your bootable diskette, run one of our scanners against it.

If you do not have copies of your operating system installation diskettes, you can make a bootable diskette from an uninfected machine:

a. Obtain a diskette that is the correct size for the `A:` drive in the infected machine.

b. Take this diskette to an uninfected machine that is running the same version of DOS as the infected machine.

c. For DOS versions up to, but not including 5.0, type:

```
format a: /s [Enter]
```

d. For DOS versions 5.0 or higher, type:

```
format a: /s /u [Enter]
```

e. After this is complete, write-protect the diskette.

Diskettes are write-protected in different ways, depending on whether they are of the 3.5" or 5.25" format. To write-protect a 5.25" diskette, put an opaque write-protect tab over the little notch on the uppermost (right) part of the disk. To write-protect a 3.5" diskette, move the notch on the uppermost (left) part at the back side of the diskette so that it creates an opening.

Note: Be sure the bootable diskette is write-protected whenever you use it. Write-protecting diskettes is an important defense against infection of the diskettes by both file and boot viruses.

---

f. Label the diskette in such a way that makes it impossible to confuse this diskette with other diskettes. You don't want to boot with anything but your trusted, protected bootable diskette.

g. Insert the diskette in A: and boot the infected machine.

h. Insert the **last** NVC for DOS diskette or the Emergency Scan Diskette and run

```
nvc32x c: /cl
```

See for more details about this function.

i. Repeat this operation for all hard drives.

j. Reboot the machine.

k. Insert the first NVC for DOS/Windows 3.1x diskette and run

```
a:setup
```

Prevention

Norman's Main Philosophy

Norman believes that preventing virus infections is of utmost importance. As a result, two of the major components in NVC are:

1. A smart behavior blocker which prevents infections from known and unknown boot and file viruses.
2. Cat’s Claw which detects and removes viruses from files before the file is handed over to the application.

Although we place much emphasis on these preventive components, we employ other methods of prevention that rely on generic protection of boot areas and executable files.

Tie these two concepts together with identification and removal of viruses, and you have an all-around anti-virus product.

Behavior Blocking Concepts

Behavior blocking is a relatively new technique in the fight against viruses. One of the reasons Norman uses behavior blocking is because it protects users by warning when an infection is attempted and not simply alerting after an infection has occurred.

Behavior blocking is technically defined as the process of dynamic code analysis. The sequence of actions in a program are monitored to determine if the actions are consistent with the behavior of viruses. The technique used by one behavior blocker may differ from the one used by another, but the underlying principle will be the same: a

sequence of code execution will be monitored until it is determined that the sequence is safe or is harmful. If harmful, the code will not be permitted to actually execute and the user will be notified.

Note: Do not confuse behavior blocking with resident scanning. Behavior blocking does not rely on virus scan strings (i.e. previous knowledge of the virus), whereas resident scanning does.

Norman's Smart Behavior Blocker is "smart" in terms of using statistical analysis to determine the probabilities that particular behavior sequences are those of a virus rather than those of a user. If this statistical analysis were not done, then a behavior blocker might simply halt any action that writes to a .COM file. The problem with this is that the action might be valid. A simplified view of Norman's Smart Behavior Blocker's reasoning:

Action	Analysis
A process opens a .COM file.	Nothing suspicious so far.
The process reads to the end of the file and then adds to the end, increasing its size.	Becoming suspicious.
The process returns to the beginning of the file and patches the code to point to the segment that was appended to the file.	Definitely something wrong. Virus-like activity that must be halted, reversed, and reported.

Another advantage of behavior blocking is its long life. Norman's Smart Behavior Blocker uses advanced algorithms so that it need not be updated with the same frequency as with scan string virus scanners. That is, because the Smart Behavior Blocker monitors behavior, it

does not warrant upgrades each time a new virus is detected.

NVC.SYS is Norman's Smart Behavior Blocker, a device driver that is loaded from `config.sys`. Following is a detailed discussion about NVC.SYS.

NVC.SYS, Norman's Smart Behavior Blocker

Interdependence with other NVC modules:

NVC.SYS is the cornerstone of the NVC package and therefore is recommended for use in all cases. However, the functioning of other modules is not dependent upon NVC.SYS. It also passes virus alert information to Norman FireBreak and Novell NetWare through IPX communications (see "Norman Programs and IPX Communications" in the *Administrator's Guide*).

Background

As mentioned above, NVC.SYS does not scan for specific virus patterns in files being run or in system areas. Instead, NVC.SYS monitors all activities in the system and is able to recognize all program behavior that represents typical virus techniques. In this way, NVC.SYS detects both known and unknown viruses and prevents viruses from infecting.

Therefore, we recommend that you use NVC.SYS.

Note: Because of the way it works, it is important to disable NVC.SYS before you install any new software, except for upgrading to a new version of NVC.

Protects Memory, Files, and the Boot Area

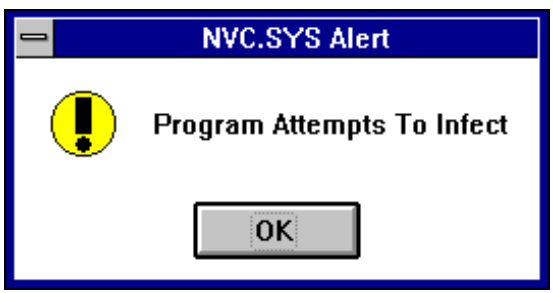
There are three areas on your PC that are vulnerable to viruses: memory, the boot area, and files.

NVC.SYS protects all three areas from becoming infected, and it displays options for next steps appropriate to the type of virus-like behavior that is found.

Because NVC.SYS does not rely on specific scan strings to detect viruses, NVC.SYS does not provide the name of the virus when it issues an alarm. Instead, you are informed of which program is infected or that a boot virus is present.

In the case of file viruses, NVC.SYS attempts to obtain the name of the infected program that is running, and you will receive a warning such as this:

In the case of file viruses, NVC.SYS attempts to obtain the name of the infected program that is running, and you will receive a warning such as this:



However, the name may not always be available. In this case, NVC.SYS will provide the memory location of the infected program.

As with file viruses, NVC.SYS does not display the name of the boot virus but rather that a boot virus is detected.

Note: To obtain the name of the virus, you must run one of our scanners. See “Scanning” on page 63 for more information on how to use Norman scanners and “Messages from NVC.SYS in DOS” on page 24 for information on what to do when NVC.SYS issues a warning.

NVC.SYS can remove a boot virus from memory diskettes, but it does not remove boot viruses from hard drives or viruses from files.

To remove a boot virus from a hard drive or from a file, you must choose repair after the virus has been detected (see "Managing Infections" on page 74), or run NVC32X.EXE with the /CL parameter (see "Command Line Scanning" on page 108).

User Interaction

When NVC.SYS intercepts suspicious behavior, it issues audible and visual warnings. In DOS, all warnings are accompanied with up to 3 choices for next steps, based upon the virus activity that is detected. See "Messages from NVC.SYS in DOS" on page 24 for information.

In Windows, all warnings are audible, but they are only visible if one of three Norman Windows programs is active. See "Messages from NVC.SYS in Windows" on page 35 for information. If Windows is running, NVC.SYS automatically performs the most suitable action.

Loading NVC.SYS

If you allow the setup program to modify your startup files, then NVC.SYS is already loaded in `config.sys`. However, you may have chosen to make modifications to `config.sys` manually. In this case, you should have a better understanding of the issues regarding loading NVC.SYS in `config.sys`.

Configuring NVC.SYS

During installation, it is recommended that NVC.SYS be added to `C` without any parameters. There are, however, several parameters that you can use in order to optimize NVC.SYS's performance for your environment.

To use any of NVC.SYS's parameters, simply add them to the end of the line that calls NVC.SYS in `config.sys`. If you are using more than one parameter, remember to add spaces in between the parameters, such as:

```
devicehigh=c:\norman\nvc.sys /t /f
```

The available parameters are:

`/A Allow boot programs to pass`

Purpose	When to use
/A causes NVC.SYS to ignore programs which are loaded before DOS.	• When NVC.SYS is running concurrently with security programs that reside in the Master Boot Sector or System Boot Sector. • When QEMM without the ST: parameter is being used.

Note: When this parameter is used, NVC.SYS will not detect boot viruses in memory. The responsibility for disallowing boot viruses to infect the hard drive and then go into memory then lies with the security product.

/B Automatically press (B)

Purpose	When to use
/B forces NVC.SYS to automatically select option (B) each time NVC.SYS issues a warning. This means that any virus run will always be disabled in memory, and you will always be permitted to continue your work.	Use this parameter when you wish to always disable a virus in memory.

Note: This parameter only **disables** the virus **in memory**. You must still remove the virus by using the repair function or NVC32X.EXE with the /CL parameter.

/C Disable option (C)

Purpose	When to use
/C forces NVC.SYS to disable the "C" option when it displays its warning. Pressing (C) when NVC.SYS warns normally allows a virus to infect.	This is ideal for users who want to prevent accidentally (or intentionally) pressing this key.

Note: This is our recommendation for how NVC.SYS should be installed in most organizations. See "Messages from NVC.SYS in DOS" on page 24.

/D Prevent direct access to the BIOS disk I/O functions

Purpose	When to use
/D prevents programs from taking advantage of an undocumented DOS function and communicating directly with the hard drive.	When you do not want any programs bypassing your security implementations.

Note: If you use this parameter, you must turn off Windows 32 bit file and disk access.

/F Turn off file tracking

Purpose	When to use
/F prevents NVC.SYS from performing file tracking.	When you are experiencing false alarms with NVC.SYS.

/L Disable logging to local hard drive

Purpose	When to use
/L parameter prevents NVC.SYS from logging its activities to NVCSYS.LOG in the root of C:. By default, NVC.SYS will log virus warning information to C:\NVCSYS.LOG.	If you decide you have no need for a log of NVC.SYS's warnings.

/M Use monochrome

Purpose	When to use
/M forces NVC.SYS to handle the display as monochrome even though your machine may support color.	This can be useful on some laptops. This parameter is automatically enabled when NVC.SYS detects MDA (Mode 7) mode.

/S Suppress warning beep

Purpose	When to use
/S suppresses the beep that normally accompanies a message from NVC.SYS.	When you do not wish to hear the beep.

/T Disable virtual file testing on TSRs

Purpose	When to use
This parameter stops NVC.SYS from conducting a "virtual file" test on programs going TSR.	If a TSR hangs immediately on loading and NVC.SYS does not warn, the TSR might be trying to manipulate the virtual file.
Purpose	**When to use**
Normally, NVC.SYS performs various tests on programs that go resident in memory. One of these tests is called the Virtual File Test. The file used in the test does not actually exist, but to TSRs, it looks real. Some TSRs, like the EZLAN and SUN NFS redirector, however, attempt to manipulate the virtual file and end up hanging the computer. Viruses, on the other hand, never get confused by the virtual file.	If your machine is configured to be a NetWare Lite Server, you must use /T. If you do not, the computer hangs immediately after SERVER.EXE terminates. If you are loading any of the following programs: 386MAX.SYS, BLUEMAX.SYS, PCNFS.SYS, ELFAX.

Note: If you use the /T parameter for NVC.SYS, then NVC.SYS will not stop the majority of viruses at the moment that they attempt to go resident. However, NVC.SYS will detect the virus when it attempts to infect a file or boot area.

Preventing NVC.SYS from Loading

An easy way to disable NVC.SYS temporarily without changing `config.sys` is to reboot the computer by pressing [Ctrl][Alt][Del] and then pressing the [Ctrl][Alt] key combination after the ROM BIOS has completed the Power-On-Self-Test (POST).

In DOS 6.0+, you can also press [F8] during boot in order to run device drivers selectively.

We do not, however, recommend that you make this a regular practice.

Before Installing/Upgrading Software

The only time NVC.SYS might call a legitimate action a virus is during the installation/upgrade of new software. Therefore, before installing/upgrading new software (especially new operating systems), you should first scan the new software diskettes for possible viruses **and then you must temporarily disable NVC.SYS.**

This is not necessary when upgrading to new versions of NVC.

Messages from NVC.SYS in DOS

The current version of NVC.SYS is a 16 bit DOS device driver. As such it displays its messages in the DOS environment. For Windows 3.1 users, however, NVC.SYS will pass along its messages through one of three Norman Windows programs. See "Messages from NVC.SYS in

Windows” on page 35 for more details.

Boot Virus Detected in Memory

When this warning appears, you have booted from an infected diskette or infected hard drive, and there is now an active boot virus in memory. You now have 3 choices:

Choice	Description	Result
A	Solution (Reboot)	NVC.SYS will reboot the computer and clear the virus from memory. If you want to boot from a diskette, ensure that you are using an uninfected, write-protected bootable diskette and turn the machine on and off at the switch. Do not press [Ctrl][Alt][Del], for some "stealth" viruses cannot be removed this way.

B	Disable It and Continue	NVC.SYS will eliminate the virus in memory by overwriting the virus code which hooks to the system interrupts and then allow the boot process to continue as usual but without the virus in memory.
C	Just Continue (At Your Own Risk)	NVC.SYS allows the boot virus to stay in memory when you press [C]. Since this is potentially very dangerous, we advise against pressing [C]. You may disable the availability of this option by installing NVC.SYS with the /C parameter. See the section "Configuring NVC.SYS" on page 18.

Note: For options A and B, although NVC.SYS has eliminated the virus from memory, it has not removed the virus from the hard drive. To do this, use either the repair function in the scanner (see "Managing Infections" on page 74) or NVC32X.EXE with the /CL parameter (see "Command Line Scanning" on page 108).

NVC.SYS reacts differently in situations when Windows is active: NVC.SYS does not offer you choices and instead automatically performs the "B" option. See "Messages from NVC.SYS in Windows" on page 35.

"Possible Virus" Attempts to Trace

When this warning appears, you have executed an infected program, and the virus is now trying to bypass NVC.SYS.)

You have three choices:

Choice	Description	Result
A	Solution (Reboot)	NVC.SYS will reboot the computer and stop the attempt to trace through.
B	Disable It And Continue	NVC.SYS will stop the tracing and let you continue with your work. Most viruses crash the computer when you choose this option because they do not expect anything to stop their tracing activities. If this happens, press the computer's RESET button or on/off switch.
C	Just Continue (At Your Own Risk)	NVC.SYS will allow the tracing to proceed when you press [C]. Do not press this key if you are unsure. You may disable the availability of this option by installing NVC.SYS with the /C parameter. See “Configuring NVC.SYS” on page 18 for detailed information on loading and configuring NVC.SYS and how this affects `config.sys`.

Note: For options A and B, although NVC.SYS has stopped the virus from tracing through, NVC.SYS does not remove the virus from the infected file.

NVC.SYS reacts differently in situations when Windows is active: NVC.SYS does not offer you choices and instead automatically performs the "B" option. See “Messages from NVC.SYS in Windows” on page 35.

"Possible Virus" Attempts to Infect

When this warning appears, you have executed an infected program and the virus is now trying to infect other files. This warning is normally generated by direct action (non-resident) file viruses. Such viruses usually search through directories and try to infect a few files before passing the control back to the original program. You have three choices:

Choice	Description	Result
A	Solution (Reboot)	NVC.SYS will reboot the computer and therefore disable the attempts to infect other files.
B	Disable it and continue	NVC.SYS will stop the virus from infecting other files and let you proceed with your work.
C	Just Continue (At Your Own Risk)	NVC.SYS will allow the virus to infect other files. Do not press [C] if you are unsure. You may disable the availability of this option by installing NVC.SYS with the /C parameter. See "Configuring NVC.SYS" on page 18 for detailed information on loading and configuring NVC.SYS and how this affects `config.sys`.

Note: For options A and B, although NVC.SYS has prevented the virus from infecting other files, NVC.SYS does not remove the virus from the infected program. You must clean the infected file by using the repair function in the scanner (see "Managing Infections" on page 74) or

NVC32X.EXE with the /CL parameter.
If NVC.SYS prompts you with this message 3 times, this means that the virus is trying to infect 3 different files. Sometimes a virus tries to infect ALL the files on a hard drive. If this happens, NVC.SYS will prompt you with this warning ceaselessly. At this point, the best solution is to press [A] and then run the scanner or NVC32X.EXE with the /CL parameter.

NVC.SYS reacts differently in situations when Windows is active: NVC.SYS does not offer you choices and instead automatically performs the [B] option. See “Messages from NVC.SYS in Windows” on page 35.

"PROGRAM.EXT" Is a Virus Carrier

When this warning appears, you have executed an infected file, and the virus is now trying to become resident in memory. NVC.SYS is able to differentiate between an uninfected TSR program and an infected TSR program, even though both of them stay resident. You have three choices:

Choice	Description	Result
A	Solution (Reboot)	NVC.SYS will reboot the computer and flush the virus out of memory.

B	Disable It And Continue	NVC.SYS will unhook the virus so that it cannot infect other files and let you continue with your work.
C	Just Continue (At Your Own Risk)	NVC.SYS will let the virus go memory resident. Do not press this key if you are unsure. You may disable the availability of this option by installing NVC.SYS with the /C parameter. See "Configuring NVC.SYS" on page 18 for detailed information.

Note: For options A and B, although NVC.SYS has prevented the virus from becoming resident, NVC.SYS has not removed the virus from the infected file. To do so, use either the scanner (see "Managing Infections" on page 74) or NVC32X.EXE with the /CL parameter (see "Command Line Scanning" on page 108).

NVC.SYS reacts differently in situations when Windows is active: NVC.SYS does not offer you choices and instead automatically performs the "B" option. See "Messages from NVC.SYS in Windows" on page 35.

If you use the /T parameter for NVC.SYS, then NVC.SYS will not stop the majority of viruses at the moment that they attempt to go resident. However, NVC.SYS will detect the virus when it attempts to infect a file or boot area.

"PROGRAM.EXT" Alter Boot Area

When this warning appears, a virus or a program (FORMAT, FDISK, or Norton Utilities, for example) is trying to change the contents of the hard drive's Master Boot Sector (MBS) or System Boot Sector (SBS). The information in these areas tells DOS how the hard drive

was formatted and configured. Writing the wrong data to this area can corrupt the entire hard drive. You have three choices:

Choice	Description	Result
A	Solution (Reboot)	NVC.SYS will reboot the computer and stop the virus or program from changing the boot area.
B	Disable It And Continue	NVC.SYS will stop the attempted infection and let you continue with your work.
Choice	**Description**	**Result**
C	Just Continue (At Your Own Risk)	NVC.SYS will let the virus or program change the Master Boot Sector or boot sector. Do not press this key if you are unsure. You may disable the availability of this option by installing NVC.SYS with the /C parameter. See “Configuring NVC.SYS” on page 18.

Note: For options A and B, although NVC.SYS has stopped the attempt to change the boot area, NVC.SYS does not remove the virus from the infected file.
Of course, if a disk utility such as FORMAT, FDISK, or the Norton Utilities is the cause of the alarm, then there is no need to run a virus remover.

NVC.SYS reacts differently in situations when Windows is active: NVC.SYS does not offer you choices and instead automatically performs the "B" option. See “Messages from NVC.SYS in Windows” on page 35.

"PROGRAM.EXT" Attempts to Format the Hard Drive

When this warning appears, a virus or a program is trying to perform a low-level physical format of the hard drive. Even DOS's FORMAT does not perform a low-level format, so this is highly suspicious behavior. You have three choices:

Choice	Description	Result
A	Solution (Reboot)	NVC.SYS will reboot the computer and stop the attempt by the virus or program to reformat the hard drive.
B	Disable It And Continue.	NVC.SYS will stop the program from reformatting the hard drive and let you continue with your work.
C	Just Continue (At Your Own Risk)	NVC.SYS will let the virus or program do its deed, reformatting the hard drive. Do not press this key if you are unsure. You may disable the availability of this option by installing NVC.SYS with the /C parameter. See "Messages from NVC.SYS in Windows" on page 35.

Note: For options A and B, although NVC.SYS has stopped the attempt to reformat the hard drive, NVC.SYS has not removed the virus from the infected file. To do this, use either the repair function in the scanner or NVC32X.EXE with the /CL parameter.

NVC.SYS reacts differently in situations when Windows is active: NVC.SYS does not offer you choices and instead automatically performs the "B" option. See “Messages from NVC.SYS in Windows” on page 35.

Diskette Boot Record Is Infected

When this warning appears, you have put an infected diskette into the diskette drive and accessed it in some fashion (DIR A:, B:, etc.). When NVC.SYS sees a diskette drive change, it uses an algorithm to look at the boot sector of the diskette in order to determine if it is infected. The algorithm does not rely on scan strings, so NVC.SYS can detect both known and unknown boot viruses on diskettes.

If a diskette is infected, NVC.SYS will issue a warning and offer to remove the boot virus from the diskette. The choices displayed are:

Choice	Description	Result
A	*option unavailable*	N/A
B	Clean It and Continue.	NVC.SYS will replace the infected diskette boot record with its own special boot record which contains anti-virus routines. If the disk is write-protected, NVC.SYS will refuse access until the write-protect tab is removed or option [C] is chosen, if it is available.
C	Just Continue (At Your Own Risk)	NVC.SYS lets you access the infected diskette until you access the other diskette drive, or any other diskette in the same drive. You may disable the availability of this option by installing NVC.SYS with the /C parameter. See "Configuring NVC.SYS" on page 18.

The boot record that NVC.SYS writes to the diskette when you press [B] is **not bootable**. Therefore, if the infected diskette was originally bootable, it will not be bootable after NVC.SYS removes the boot virus. To make the diskette bootable again, use the SYS command.

If this is too troublesome, then do not allow NVC.SYS to remove boot viruses from diskettes and instead use either

the repair function in the scanner or NVC32X.EXE with the /CL parameter.

Note: NVC.SYS's removal of boot viruses from diskettes performs a bit differently when Windows is involved.

If the following conditions are met:

- NVC.SYS is active
- Windows is active
- NVCSYS.EXE or NVCW.EXE is active
- a diskette with a boot virus is accessed
- the diskette is write-enabled

In this case, you will see a dialog box like this:

This is a reasonable notice, but the misleading part happens next. Since the diskette is write-enabled, NVC.SYS will automatically remove the boot virus. So subsequent scans of the diskette will show no infection because the virus has already been removed.

If the same conditions as above exist, but **without** NVCSYS.EXE, NVCW.EXE, or NVS.EXE being active, then you will not see the above dialog box. However, NVC.SYS again will remove the boot virus automatically.

Messages from NVC.SYS in Windows

As we mentioned above, since NVC.SYS is a DOS device driver, it does not have the ability to display its messages

through Windows by itself. Instead, you may use one of three Norman Windows programs to serve as message handlers from NVC.SYS to Windows.

In any case, NVC.SYS will always issue its audible alarm, unless you are running NVC.SYS with the /S parameter. See "Configuring NVC.SYS" on page 18.

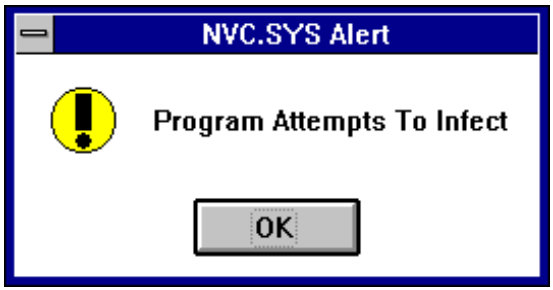
Norman Message Control

Norman Message Control (NVCSYS.EXE) passes messages between NVC.SYS and Windows. Norman Message Control is a one-way message handler which takes information from NVC.SYS and displays it in Windows. Therefore, unlike in DOS, you will not have different choices for next steps when NVC.SYS warns. Instead, NVC.SYS will automatically implement the [B] option for each virus alert incident.

Norman Message Control messages look like this:

Windows Scanner and NVC.SYS Messages

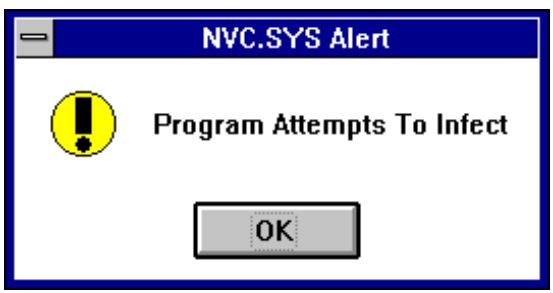
Norman's Windows scanner also accepts messages from NVC.SYS. As with Norman Message Control, this is a one-way message street, in which NVC.SYS passes the message to the Windows scanner, and the message is displayed as follows:



See “Messages from NVC.SYS in Windows” on page 35 for more information.

Windows Scheduler and NVC.SYS Messages

Norman's scheduler for the Windows scanner also accepts messages from NVC.SYS. As with Norman Message Control, this is a one-way message street, in which NVC.SYS passes the message to the scheduler, and the message is displayed as follows:



See “Scheduling” on page 115.

Cat's Claw

Cat's Claw is an on-access (real-time) scanner that detects and repairs binary file viruses and macro viruses, including boot sector infections. This application is based on Norman's established virus protection technology.

Cat's Claw will scan for viruses on boot sectors and in files as they are being opened. Whenever possible, an infected file is repaired before the file is handed over to the application.

If repair is not possible, you will receive a message and the application is not allowed to open the infected file.

The present version of Cat's Claw can detect and remove file and macro viruses known to NVC automatically.

Except for diskettes, Cat's Claw can not remove boot viruses automatically, but will guide you through the established procedure for boot sector virus removal.

Configuration Concepts

Users are not a homogenous group, and we therefore provide you with the option of configuring Cat's Claw to best suit your needs. If you run Cat's Claw with the default settings, the following options apply:

- Cat's Claw will be loaded into memory at startup
- you will be prompted for action when a virus is found
- you will receive a warning if Cat's Claw is unable to scan a file
- uncertified macros will not be removed

The following discussion covers the different dialogs and their options. Cat's Claw is not equipped with default options that necessarily provide the optimal protection for you. One reason is that users have very different needs, another is that regulations in some countries do not allow a program to remove files without the user's explicit consent. This legal restraint is blocking our wish to set automatic removal of viruses as default option.

About Warnings from Cat's Claw

The following discussion will guide you through the configuration option and thus provide you with a better understanding on how the application works. Cat's Claw will always warn you about what's happening by displaying dialog boxes. You will only see a couple of examples of warnings from Cat's Claw. However, all possible warnings are described, and if or when they pop up, click on help for assistance.

Cat's Claw Factory Settings

The factory settings in the Cat's Claw configuration program should not be considered as recommended options.

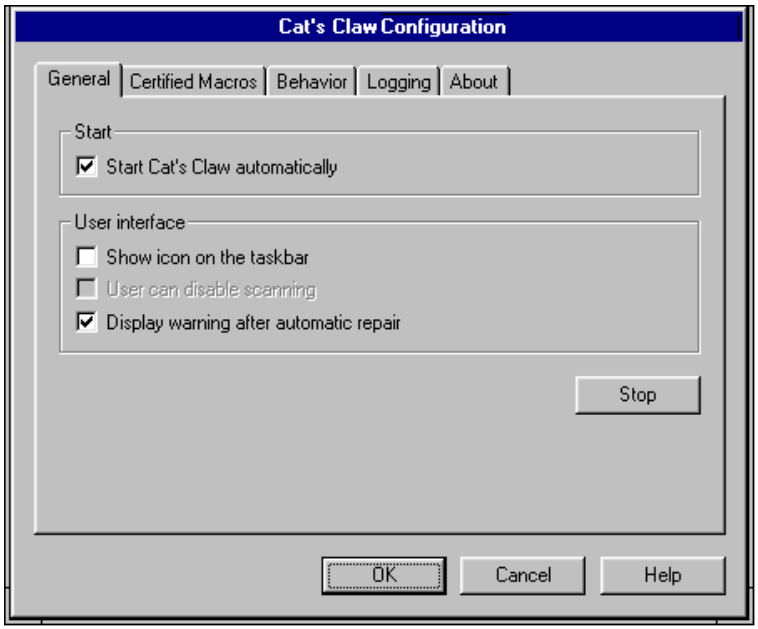
From a security point of view, we strongly recommend that you check the option [ ] **Load Cat's Claw on startup** in the tabbed dialog General.

However, you should use the configuration options to make Cat's Claw work smoothly and efficiently on your PC anyway.

Configuration Dialogs

To access the configuration tabbed dialogs, double-click the Cat's Claw icon in the Norman program group, and you

will see:



General

[ ] Load Cat's Claw on startup

If you want Cat's Claw to be active on your system at all times, then run the application with this default option on to ensure that Cat's Claw is loaded into memory when you start your machine.

[ ] Show icon on desktop

For a visible confirmation that Cat's Claw is active, you can check this option to display an icon like this on your desktop

[ ] User can disable scanning

If you're an administrator and don't want to allow the users to turn off scanning, you should not check this option. The

user will then be prevented from disabling Cat's Claw by clicking on the Cat's Claw icon on the desktop.

[x] Display warning after automatic repair

If you select [ ] **Remove virus from file** (see page 45), you will be informed when Cat's Claw has removed a virus from an infected file.

If Cat's Claw is already loaded, the **Start** button will appear as **Stop**.

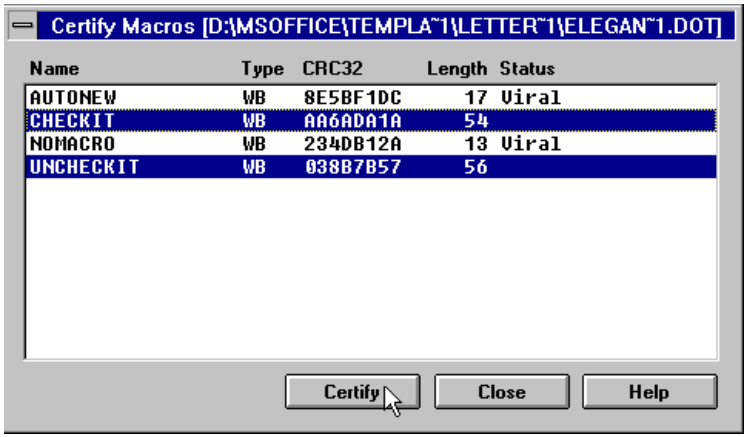
Certified Macros

From this dialog box you can certify the macros that Cat's Claw shall allow in your files. Deciding whether to certify macros or not is a critical decision. Using this function will protect you against new macro viruses not yet identified. We consider this extremely important because new macro viruses pop up every day. On the other hand, 'healthy' but unknown macros can be removed and inflict damage on files. The decision on whether to use the certify macro function is consequently a matter of balancing security versus convenience.

If you certify macros, only these macros will be accepted. See "Handling of Uncertified Macros" on page 46 for more considerations on certified and uncertified macros.

Follow these steps to certify a macro:

1. Click on the **Add** button and choose a file from the Open file dialog.
2. If the selected file doesn't contain any macros, the list box will be empty. Possible macros appear in the Certify Macros list box:



3. Highlight the macros you wish to include and click on **Certify**. You are returned to the Certified Macros dialog.
4. When you highlight a macro in the Certified Macros dialog, the **Delete** and **Comment** buttons become available.
5. Click on **Add** and repeat step 1 through 4 to certify more macros.

Note: If you check the **No action** option in the "Handling of uncertified macros", you will disable the certified macro function.

Fields in the Dialogs for Certifying Macros

There are six fields in the two dialog boxes ("Certified Macros" and "Certify Macros"). Except for the Comments field in the Certify Macros dialog, the information is provided by Cat's Claw:

Status:

There are three types of status that can appear in this field:

1. Empty: if the status field is empty, you can certify the macro.

2. Certified: since this macro is already certified, you cannot certify it again.
3. Viral: macro viruses are made up of multiple macros. This macro is/has been part of a virus and cannot be certified.

Name:

Cat's Claw will use the macro's actual name, or as many characters as possible if it's a long name, to make it possible to recognize for a user.

Cat's Claw will use the following three fields to identify a certified macro. This is internal read-only information.

Type:

Three different types can appear in this field:

1. WB, denoting a Word 6/7 macro
2. VBA3, denoting an Excel 5 macro
3. VBA5, denoting an Office 97 macro

CRC32:

A checksum established as one of the three distinguishing marks for a macro. If the macro is changed after being certified, the changed macro must be certified.

Length:

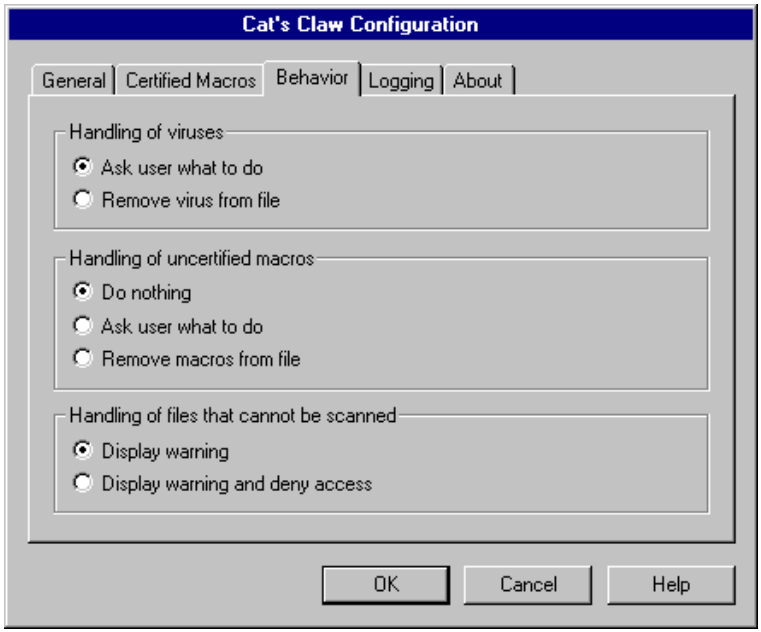
Like any other file, a macro has a certain length. This field displays the macro length used by Cat's Claw to check that a certified macro hasn't been changed after certification.

Comment:

Whatever information you add to a certified macro. This is the only field available for user input.

Behavior

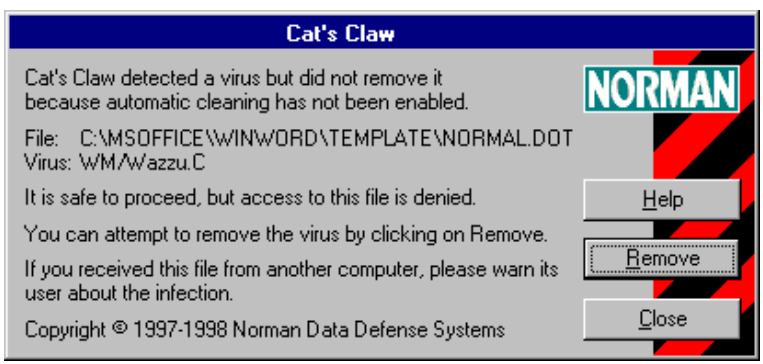
This tabbed dialog box is divided into three sections. This is where you instruct the application how to handle viruses, uncertified macros, and files that cannot be scanned:



Handling of Viruses

[ ] Ask user what to do

If you don't want automatic removal of viruses when you access infected files, you must check this option. When you try to open an infected file, you'll see this dialog:



Manual Virus Removal Warning

You have specified [ ] **Ask user what to do** in the tabbed dialog Behavior, and access to this file is therefore denied. Try to remove the virus manually by clicking on the **Remove** button. Then try to access the file again. For automatic removal of viruses, change your configuration to [ ] **Remove virus from file**.

[ ] Remove virus from file

Checking this option will automatically remove possible viruses from infected files. You will, however, receive a message about the infection.

Virus Removed Warning

If you check the box [ ] **Don't show this message again today** in this dialog, you will not be informed about other possible cleaning operations until you reboot your machine. However, you can keep track of removed viruses by checking [ ] **Viruses removed** in the tabbed dialog Logging.

Virus Not Removed Warning

In some situations Cat's Claw cannot remove a detected virus. When this happens, you will receive a warning.

Note that your system has not been infected, but the file still is. You will never be granted access to an infected file, and it is therefore safe to proceed.

A virus cannot be removed if the infected file resides on a:

1. Write-protected diskette
2. CD-ROM
3. Network drive and the file is write-protected,

   or if
4. The file is in use (i.e., you do not have write access).

Handling of Uncertified Macros

An uncertified macro does not necessarily contain a virus. However, all unknown macros are possible virus carriers, and you can therefore decide how to handle these. If you have certified certain macros, then these are the only macros that Cat's Claw will accept.

[ ] Do nothing

Cat's Claw will not touch the macro, nor inform you about it. Remember that if the macro contains a known virus, Cat's Claw will take action anyway.

Note: The certify macro function is disabled if you choose this option.

[ ] Ask user what to do

Note: If you run with this option on, ALL macros will be removed except for previously certified macros.

With this options checked, Cat's Claw will warn when an uncertified macro is found.

Uncertified Macro Not Removed Warning

The detected macro is not a virus, but it does not appear on your list of certified macros. Your choices are:

1. Click on **Remove** to clean the file.
2. If you want to access the file without removing the macro, check the option [ ] **Do nothing** and try to open the file again.

[ ] Remove macros from document

Note: If you run with this option on, ALL macros will be removed except for previously certified macros.

When you open a file with an uncertified macro, you will receive the:

Uncertified Macro Removed Warning

Cat's Claw removed macros from this file because:

1. They did not appear on the list of certified macros.
2. You checked the option [ ] **Remove macros from document** in the tabbed dialog Behavior.

With this option checked, Cat's Claw will remove all macros not specified in the tabbed dialog Certified Macros.

Other Messages on Uncertified Macros

Other situations may stop removal of uncertified macros even if you have specified removal:

Cannot Remove Uncertified Macro Warning

The macro(s) cannot be removed if they reside on a:

1. Write-protected diskette
2. CD-ROM
3. Network drive and the file is write-protected,

or if

4. The file is in use (i.e., you do not have write access).

Handling of Files That Cannot Be Scanned

In some situations Cat's Claw is unable to scan a file. Examples are Word 8 files with password protection, damaged files, or when internal system errors occur. The following options decide how Cat's Claw should react under such circumstances.

[ ] Display warning

When you receive a warning when you access a file, you know that this file has not been checked for viruses. You can, however, proceed at your own risk.

The following are possible warnings from Cat's Claw when you have checked the option [ ] **Display warning**:

Password Protected File Warning

Cat's Claw will not deny access to this file because you selected the option [ ] **Display warning**. You can enter the password and open the file at your own risk. Cat's Claw can not guarantee it's free for viruses or uncertified macros.

Damaged File Warning

Cat's Claw will not deny access to this file because you selected the option [ ] **Display warning**. The file is damaged and has not been scanned. You can open the file at your own risk. Cat's Claw can not guarantee it's free for viruses or uncertified macros.

Internal Error Warning

Cat's Claw will not deny access to this file because you selected the option [ ] **Display warning**. Due to an internal error in Cat's Claw or Windows, the file has not been scanned. You can open the file at your own risk. Cat's Claw can not guarantee it's free for viruses or uncertified macros.

[ ] Display warning and deny access

Checking this option involves that you are warned about an unscanned file, and access is denied.

The following are possible warnings from Cat's Claw when you have checked the option [ ] **Display warning and deny access**:

Password Protected File Blocked Warning

You checked the option [ ] **Display warning and deny access**. Password protection stopped Cat's Claw from scanning the file, and you cannot access it. Possible

solution is changing your configuration to [ ] **Display warning** only and access the file at your own risk.

Note: This situation will occur only when a password protected Word 8 file is detected. Cat's Claw can detect and remove macro viruses from password protected files in Word 6 and Word 7.

Damaged File Blocked Warning

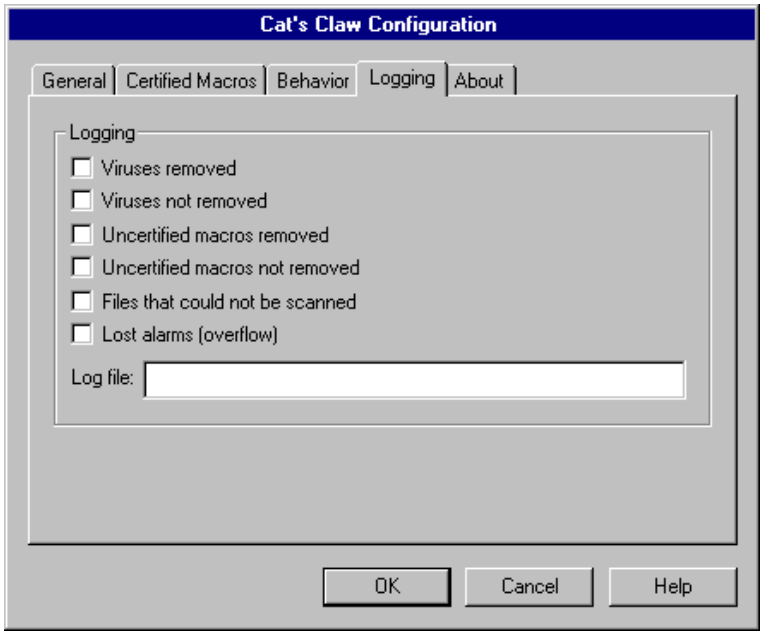
You checked the option [ ] **Display warning and deny access**. Cat's Claw could not scan the file because it's damaged, and you cannot access it. Possible solution is changing your configuration to [ ] **Display warning** only and access the file at your own risk.

Internal Error Denied Access Warning

You checked the option [ ] **Display warning and deny access**. Due to an internal error in Cat's Claw or Windows, the file has not been scanned. Possible solution is changing your configuration to [ ] **Display warning** only and access the file at your own risk, or reboot your machine and try again.

Logging

Cat's Claw will register vital activity in a log file. In this dialog you can decide what kind of information the log file should hold.



As for the other configuration dialogs, you should decide for yourself what kind of information that is important to you.

[ ] Viruses removed

Logs path, file name and name of removed viruses.

[ ] Viruses not removed

Logs path, file name and name of viruses detected but not removed.

[ ] Uncertified macros removed

Logs path and file name of removed uncertified macros.

[ ] Uncertified macros not removed

Logs path and file name of uncertified macros not removed.

[ ] Files that could not be scanned

Logs path and file name of files that Cat's Claw could not scan. Cat's Claw cannot scan files which are:

- password protected, possibly containing macros
- corrupted

[ ] Lost alarms (overflow)

Due to limitations of system's resources assigned to Cat's Claw, a maximum of, for example, 20 alarms can accumulate waiting for user response. If the unlikely situation should occur that you run into e.g. 25 infected files without responding to any of the waiting messages, then you will not be warned from infection number 21 and upwards. This option will give you the *number of infections* that Cat's Claw was unable to handle. If this happens, Cat's Claw will block access to the files rather than ask user what to do.

Loosing alarms does therefore not represent a security risk.

Log file

Enter a valid path and file name for the log file, for example `c:\norman\win16\claw31.log`.

Boot Guard, Generic Boot Area Protection

In addition to the Smart Behavior Blocker, NVC provides one module that uses generic methods to protect the boot area and one module that uses generic methods to protect files.

BootGuard is not dependent on any other module, although it will display information when it detects that the Smart Behavior Blocker is not active. No other module depends on BootGuard's presence.

BootGuard is a **non-resident** universal boot area search/ recognition engine which enables NVC to identify if a master boot sector or system boot sector is infected by known or unknown boot viruses. In addition, if used correctly it can recover the original boot area. Because of BootGuard's recovery abilities, we recommend that at a minimum, you run both NVC.SYS and BootGuard.

The method BootGuard uses is quite simple. An image of the master boot sector and system boot sector is kept inside BootGuard itself, along with specific hard drive information which applies only to the computer in which NVC has been installed. Afterwards, each time BootGuard runs, it checks the information in the image within itself against the information on your hard drive. If there is any discrepancy, BootGuard warns and provides choices for updating the information within BootGuard, restoring the original information, or ignoring the warning altogether. Such checking provides for a fast and easy way to remove boot viruses from the boot area.

Note: During installation, you can choose to let the setup program update `autoexec.bat` with a line which calls BootGuard, allowing BootGuard to run each time you boot the machine. Remember that BootGuard is a non-resident module, guaranteeing accurate information about the state of the boot area only at the time that BootGuard is run.

BootGuard has a remedial amount of enforcement built in. If NVC.SYS is not in memory when BootGuard runs, BootGuard warns that memory is not protected.

If you do run BootGuard without NVC.SYS, and you find that the boot area has been changed, let BootGuard repair the boot sector by pressing [B] and then reboot your machine in order to kill the virus that is in memory.

Since BG.EXE stores information within itself, you should not use Computer A's copy of BG.EXE on Computer B, unless the two computers have exactly the same configuration. Always use the copy of BG.EXE from the distribution disk when you want to install on different machines.

How to Use BootGuard

During installation, BootGuard takes a healthy "picture" of your hard drive's boot area and stores it within BG.EXE. However, if you choose **not** to scan your PC during installation, then you are not allowed to install BootGuard. This is because unless a virus scan has been run, there is no way of telling if the "picture" is healthy at all.

If you make legitimate modifications to your hard drive's boot area, then you should update BG.EXE with the new information by typing:

```
bg /n [Enter]
```

The "/N" parameter saves the boot area's "picture" within BG.EXE. Therefore, it is important to **ensure that your machine is not infected before you use this command**.

See "Scanning" on page 63 for information on scanning your machine.

Note: Because BootGuard stores an image of the boot area within itself, each copy of BG.EXE that is run with the "/N" parameter is machine-specific.

To ensure that BootGuard keeps track of whether or not your boot area has changed, we recommend running BG.EXE from `autoexec.bat`. During installation you can let the setup procedure include BG.EXE in `autoexec.bat` automatically. This way, BootGuard checks the boot area information each time you boot the machine.

To check the status of your hard drive's boot area at any time, simply type:

```
bg [Enter]
```

Under normal circumstances, your boot area will be intact and BootGuard simply displays:

```
Boot Area Is Fine.
```

However, when BootGuard finds something wrong, it issues an audible and visual warning, accompanied by options on what to do next.

Note: If the command BG /N is not run when the hard drive is uninfected, then BootGuard cannot protect your boot area and therefore cannot remove any boot viruses. BootGuard knows when BG /N has not been run and displays a message, telling the user to run BG /N.

The following sections describe BootGuard's warnings.

BootGuard Warning: Changes Detected in Boot Area

This message means that Master Boot Sector or System Boot Sector have been changed. You now have three choices:

Choice	Description	Result
A	Accept changes as valid	BootGuard accepts the changes as valid. It does not check to see if the changes are due to boot viruses, since it is programmed to protect the boot area from all changes. It is possible to corrupt the hard drive by changing the partition data without changing the other code in the Master Boot Sector. In this case, you would have no infection but would have a corrupted hard drive. See “If You Accidentally Press (A), Recover with NVC32X.EXE” on page 56.

B	Discard changes	BootGuard discards the changes by replacing the tampered boot area with the previously stored image. This eliminates the changes effectively, especially if they are due to boot viruses. When you press [B], BootGuard will restore the previously stored image. Therefore, if you accidentally saved an image of an infected boot sector the last time you ran BootGuard, the infected boot sector will now be on your hard drive. This is a good reason for scanning your hard drive before running BootGuard with the "/N" parameter.
C	Ignore	BootGuard ignores the changes temporarily and passes control to the next item in `autoexec.bat`. Since no changes were made to the boot area, this same warning will appear each time you boot or run BG until you either accept or discard the changes.

If You Accidentally Press (A), Recover with NVC32X.EXE

If you accidentally press [A] when you meant to press [B], the Master Boot Sector and System Boot Sector are still recoverable:

1. Boot the computer as usual. If NVC.SYS warns: "Boot Virus Detected in Memory", press [B] to disable it.
2. Change to the NORMAN directory, and at the DOS prompt, type:

nvc32x c: /cl [Enter]

NVC32X.EXE will see the anomaly in the boot area and attempt to repair it. If NVC32X.EXE cannot perfectly remove the boot virus, take note of the virus name.

3. Now run BootGuard again by typing the following at the DOS prompt

   bg [Enter]

4. When BootGuard's warning appears, press [A] to accept it.

Detection

Generic Detection with Canary

Canary is not dependent on any other module and not critical for any other module's functioning. It works well with both the Smart Behavior Blocker and BootGuard. However, if you have problems running a resident module like the Smart Behavior Blocker, we recommend that you use Canary instead.

In the old days of coal mining, miners brought canary birds with them down into the shafts. The canaries served as early warning signals, for they reacted quickly to dangerous gases and lack of oxygen. If a canary died, the miners knew that it was time to get out.

Norman used this idea when designing our Canary programs CANARY.COM and CANARY.EXE). The Canary programs work as **non-resident** "bait" for known and unknown file viruses that infect files with the extensions .EXE and COM. If they become infected, they alert you that a virus is active in your computer. Since the Canary programs do not scan for specific viruses, they detect even unknown viruses. And when they become infected, they display messages on the screen and return errorlevels.

The Canary programs are self aware and know everything about themselves — their own file lengths, the precalculated checksums, and the date and time of their installation.

Most viruses attack a file by inserting their own program codes into the file. When this happens, the file length

increases, and if the file happens to be Canary, Canary detects this immediately and reports "The Canary Bird is Dead!".

Other viruses overwrite parts of the file without altering the file length. As a result, the program will no longer work properly, and the checksums change. Canary will also react to the altered checksums.

If you run Canary, and CANARY.COM and CANARY.EXE have not been infected, you see the following message:

```
EXE:The Canary Bird Lives and all is
well.
COM:The Canary Bird Lives and all is
well.
```

If, for example, a virus has infected the .EXE file, the message will read:

```
EXE:The Canary Bird is Dead!
COM:The Canary Bird Lives and all is
well.
```

You can suppress these messages and report by errorlevel instead. See “Canary's Errorlevels” on page 61.

Note: If Canary detects a virus, you can send a copy of your CANARY.COM and CANARY.EXE files to Norman for further study.
Because Canary uses generic methods, it will not tell you the name of the virus it has detected. To find out, you must use Norman's scanners. See “Scanning” on page 63 for more information on scanners.

Using Canary

The Canary programs are 16 bit DOS programs and therefore must be run from either the command line or from a batch file. In addition, when you run Canary, you

must be in the directory that holds the Canary files; or the directory must be available in the DOS path.

For Canary to be effective, you should run it frequently. Here are three ways to ensure maximum protection:

1. Always activate Canary after you have used a program by inserting instructions for running Canary at the end of each .BAT or .CMD file; or run your applications from a menu system that activates Canary whenever you return to the menu.
2. Implement a resident scheduling function that will start Canary at regular intervals.
3. Develop a good habit of starting Canary manually several times a day.

Frequent use of Canary means swift detection, and swift detection means less damage.

In DOS, if you simply type the name of an executable without the extension, DOS will look for the executable as a COM file first. If a COM is not found, it will then look for an EXE.

The Canary programs take advantage of this fact so that you only need to type `canary`, and CANARY.COM will run. CANARY.COM will then automatically run CANARY.EXE.

The syntax for running Canary is:

```
canary [reporting level] [Enter]
```

The reporting level determines how many messages will be displayed on your screen when you use Canary. Following is a description of reporting levels.

Reporting Level	Function
no entry	All messages from Canary are displayed.

1	Message is displayed only if a virus is detected or an error occurs.
2	No messages are displayed. Reporting occurs only through errorlevels.

Alternate Filenames for Canary

You can rename CANARY.COM and CANARY.EXE using any name you like, as long as you give the two files the same "first name" (e.g., TESTFILE.COM and TESTFILE.EXE). This protects Canary from being attacked by virus-writers.

Canary's Errorlevels

At the end of each run, Canary returns errorlevels which contain the results of the run. You can use these errorlevels in batch files to tailor Canary's use for your needs.

Errorlevel	Meaning
16	Communication between CANARY.COM and CANARY.EXE is invalid. CANARY.EXE has been started by a program other than CANARY.COM. You may have a virus that uses the companion technique. These viruses create a .COM file with the same name as an .EXE file, taking advantage of the fact that DOS will always start the .COM file first. Examples of such viruses are Aids II and Twin351.
9-15	Not used.
8	Cannot open CANARY.COM or CANARY.EXE. Canary cannot open its own .COM or .EXE file for examination.
6-7	Not used.

5	CANARY.COM is infected, and CANARY.EXE is missing.
4	CANARY.COM is normal, but CANARY.EXE is missing. Ensure that both files exist and are available via the path.
3	CANARY.COM and CANARY.EXE have been modified/infected.
2	CANARY.EXE is modified/infected.
1	CANARY.COM is modified/infected.
0	CANARY.COM and CANARY.EXE are normal.

Scanning

About Scanning

Scanning is a way to identify viruses that already exist in memory, files, or boot areas. Identifying these by name requires that the scanner recognizes the virus, which means that scanners must be frequently updated for information about new viruses.

We recommend that you visit Norman's Web site for free downloading of updated versions of the definition file. See "Appendix A" on page 121 for more information.

NVC includes two different virus scanners:

1. Menu-driven for Windows (`NVCW.EXE`)
2. Command line scanner (`NVC32X.EXE`)

The major differences among Norman's scanners are in the interface, so what you see before, during, and after the scan will depend on which interface you are using.

In general, Norman's command line scanners have the same functionality as the menu-driven scanners.

Specific differences include:

- Menu-driven scanners can display files and boot areas as hexadecimal values. Command line scanners cannot.
- Menu-driven scanners can use "styles" to customize scanning configurations. Command line scanners cannot.
- Menu-driven scanners have extensive on-line help. The command line scanner has not.

- The Windows scanner can operate in the background. The command line scanner cannot.
- The Windows menu-driven scanner has drag and drop capability in which you can drag and drop files onto the main window or onto the minimized scanner icon in order to automatically scan the selected file, directory, or drive. The command line scanners do not.

The following section about scanning is based on the functions in the Windows scanner, which is the one most frequently used.

When a function in the Windows scanner has a corresponding function in the command line scanner, it's referred to like this:

Command line parameter: /XX

In addition, all available command line parameters are presented in the section "Command Line Scanning" on page 108.

About Repair

Note: In NVC software and documentation, "repair", "removal", and "cleaning" are comparable terms. They all refer to the process of removing viruses from files or boot sectors, and restore the infected area to its original condition.

The core technology in all NVC components is the scanning engine. The scanning *options* reflect the capability of the engine. In addition to detect viruses, the engine can also *remove* them (*repair* the file or boot sector, and thereby *clean* the machine). This process is technically more complicated than detection.

If anything goes wrong, repairing a file is less hazardous than repairing a boot sector. A corrupted boot sector may render the system useless. To ensure that a failed boot sector repair will not put you in an awkward situation, we do not allow automatic repair of boot sectors.

If a boot sector virus is detected, you will see a dialog box that recommends that you back up the necessary data to a diskette. If the repair fails, you can boot your machine from the restore diskette. A dialog box complete with online help will guide you through the process if a boot sector virus is detected.

In addition to the protection provided for unknown viruses by the Smart Behavior Blocker (see page 14) and the on-access (real-time) scanning by Cat's Claw (see page 38), you can use the Windows scanner and the command line scanner for on-demand and scheduled scans. The following sections will cover the use of these scanners.

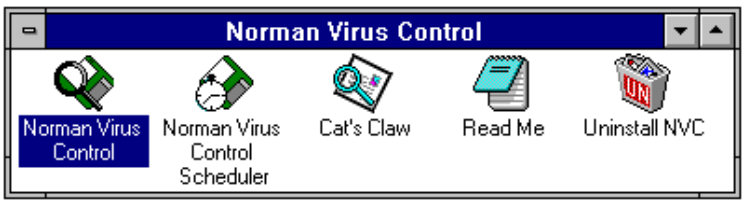
Before You Start

Whether you are using the command line scanner or the menu-driven scanner, there is a common set of procedures to follow in order to start a scan:

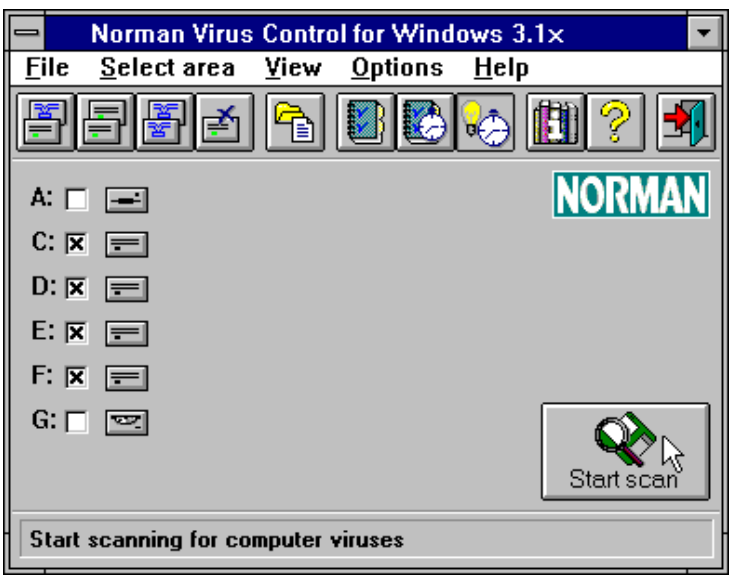
1. Select the target to be scanned — drive(s), directory, or file.
2. Select the options to use during the scan.
3. If you select the Repair option (see "Managing Infections" on page 74), the scanner will remove file and macro viruses known to NVC on-the-fly.

The Windows Scanner

From the program group where the NVC icons were installed, doubleclick on Norman Virus Control:



You'll see the main window called "Norman Virus Control". From here, you can access all the main functions.



Selecting Areas to Scan

Using the Toolbar Buttons

The following toolbar buttons are shortcuts for selecting areas for scanning:

Selects all fixed local and network drives.

Selects all fixed local drives.

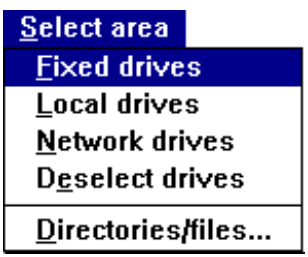
Selects all network drives.

Deselects current selection.

For selecting directories, subdirectories and files.

From the Menu Options

The toolbar button functions are also available from the menu option Select area.



In the Main Window

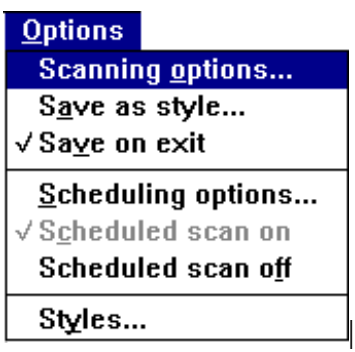
You can also specify any combination of drives you want to scan by checking the relevant drive letters directly in the main window:

Selecting Scanning Options

When you have decided where to scan, you can specify how the scanning should be performed.

You access the scanning options by clicking this toolbar button:

or from the menu option:



In either case, you'll see the tabbed dialog box with all the scanning options grouped on five different pages.

At the bottom of each page you'll see the following buttons:

OK Accept the changes and returns to the main window

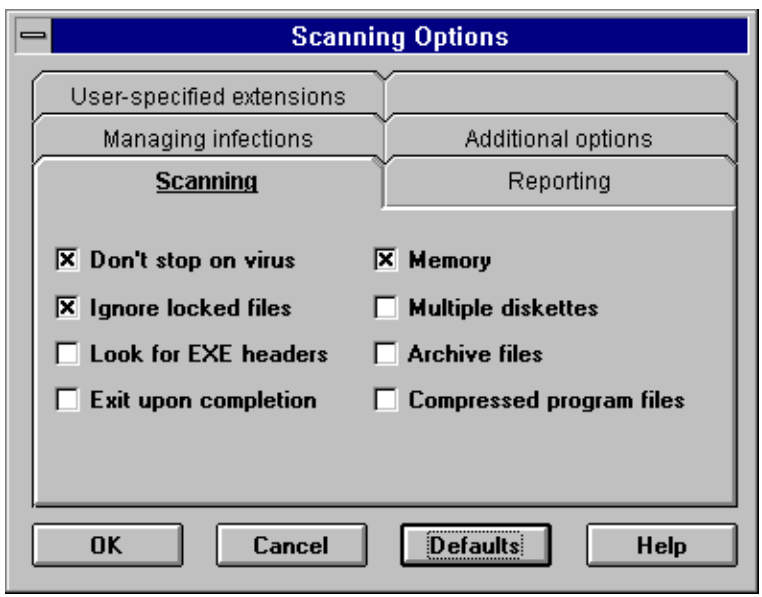
Cancel Cancel all changes

Defaults Display the default settings for all the five dialogs

Help Get online help

Scanning

The first page in the Scanning options tabbed dialog is the Scanning options page:



Note: Options checked like this: [x] are default settings.

[x] **Don't stop on virus**

If you want a scan to complete regardless of virus detection, check this option.

Command line parameter: /U

[x] **Ignore locked files**

Locked files are files presently used by the system. NVCW cannot scan locked files and will inform you of these instances. If you want the scan to run uninterrupted, check this option. The scanning report includes information on the number of files that could not be opened.

Command line parameter: /O

[ ] **Look for EXE header**

Many viruses look for signatures in .EXE files and make their decision on whether or not to infect based upon what they find (instead of simply looking for a file extension). To detect such viruses, this parameter scans files that have EXE headers.

Note: If you check this option, the scanner will look for the EXE header in **all** files and therefore increase scanning time considerably.

Command line parameter: /X

[ ] **Exit upon completion**

Check this option if you want to close NVCW altogether after running a scan.

[x] **Memory**

When you scan the memory area, NVCW looks for resident viruses. You should always make sure that no viruses exist in memory, and this option is therefore the default.

Memory will not be scanned when you scan Directories/ files only.

[ ] **Multiple diskettes**

If you are scanning more than one diskette, then check this option to save time. NVCW will scan memory only once, rather than scan memory every time you insert a diskette. The scanning results for all the scanned diskettes are included in one single report.

Command line parameter: /R

[ ] **Archive files**

Many users compress large files to free space on hard drives or diskettes. Infected files can be found within such archive files, and you can instruct Norman's scanners to look inside the archive file. Norman's scanners can use an internal decompression method which allows us to look inside the archive file without decompressing the files onto a local or remote drive. This saves the extra step of deleting the decompressed files from the local/remote drive.

If our scanner could not use its internal decompression method, it automatically reverts to external scanning. External scanning requires that the relevant archiving system is present on your system and available in the path.

Command line parameter: /C

[ ] **Compressed program files**

Many users apply PKLITE, DIET, LZEXE or ICE, for example, to compress program files. A compressed program file is better protected against viruses because the compression works almost like encryption. Still, if the compressed program file contains a virus, then the virus is activated whenever you run the executable. Even though you can scan for the virus externally, the virus is still there and will be activated the next time you run the program.

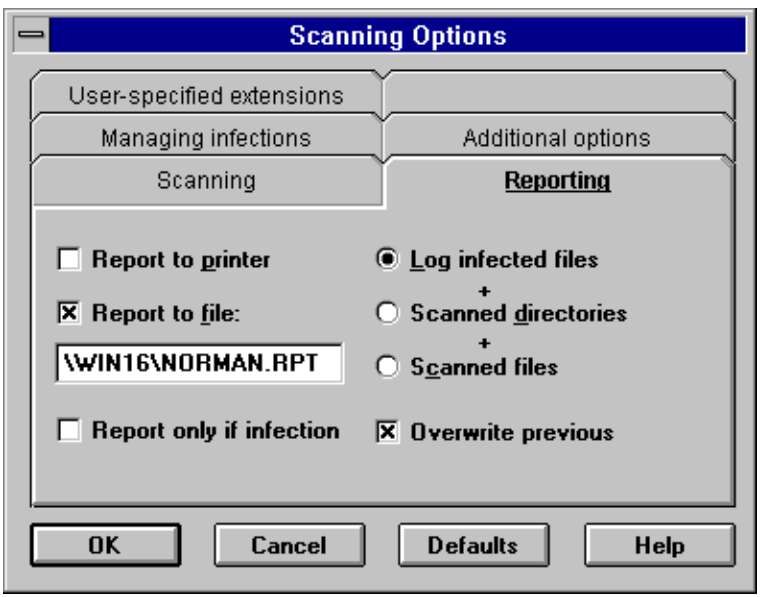
This option make use of a decompressor emulator which opens and scans the file in memory.

Command line parameter: /CP

Note: NVCW can only tell you whether or not a compressed file is infected. It cannot take any action on the infected file while it is compressed.

Reporting

In this dialog you can specify if you want a report after a virus scan, what should be included in the scanning report, and if the report should be printed or saved as a file. The dialog box looks like this:



[ ] Report to printer

If you choose Report to printer, the scanner will send its report straight to the printer that is set up through Windows.

[x] **Report to file**

This is the default option that will create the report NORMAN.RPT in the directory where NVCW resides. You may, however, specify another report name and directory.

No report will be generated when you scan Directories/files only.

Note: NVC now allows the use of UNC (Universal Naming Convention) names and environment variables wherever file and directory names can be entered. Please refer to the *Administrator's Guide* for details.

Command line parameter: /LF

[ ] **Report only if infection**

You should select this option if you don't want a report unless infected files are detected.

You can also choose among three reporting levels:

1. Log infected files.

   This level is default and will only report the infected files that are found.

2. Scanned directories.

   This level will make a list of all the directories that were scanned in addition to all the files that were found to be infected.

3. Scanned files.

   This level generates a list of **all scanned directories and files**. And infected files will be specifically marked.

If you choose item #2, the log will be a superset of information from items 1 and 2. Similarly, if you choose

item #3, the log will be a superset of information from items 1, 2, and 3.

Command line parameter: /LQ

[x] **Overwrite previous**

By default, the previous report is overwritten. If you want to keep track of previous scans on your PC, you should uncheck this option. The report will then append to the previous report(s).

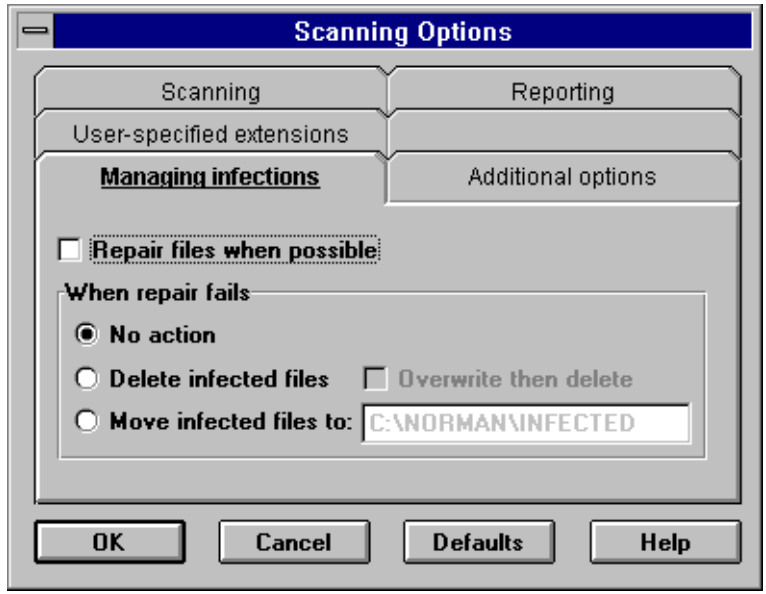
If you are running several unattended scheduled scans, you must specify different report names for the different styles or uncheck this option.

Command line parameter: /LG

See also "Scheduling Scans" on page 116.

Managing Infections

When infected files are found during a scan, you can decide how these should be treated by entering your options here:



[ ] Repair files when possible

This option ensures that viruses detected during on-demand or scheduled scans are removed on-the-fly, if possible. If this option is checked, you are well protected against all viruses known to NVC.

Command line parameter: /CL

Note: If you choose this option, the remaining options in this dialog box are valid only when repair is not possible.

[x] No action

The default option leaves you the choice to consider the intruder before you decide how it should be dealt with.

Note: Even if you choose not to delete or move infected files in this dialog, you can highlight infected files and

delete or move them from the "Scanning for viruses" display. See "When a Virus Is Found" on page 90.

[ ] **Delete infected files**

Check this option to delete infected files. Before an infected file is deleted, you will be presented to a dialog where you're asked to confirm the deletion. In other words, even though you check this option, you are allowed to change your mind later on.

See "When a Virus Is Found" on page 90 for more information on handling infected files.

Command line parameter: /D-

[ ] **Move infected files to:**

This option instructs the scanners to move infected files to a specified directory. The default directory is C:\NORMAN\INFECTED. Like the delete option, this function is not automatic, because you'll have to confirm removal of infected files.

NVC cannot move files from write-protected areas, such as a write-protected diskette.

Note: NVC now allows the use of UNC (Universal Naming Convention) names and environment variables wherever file and directory names can be entered. Please refer to the *Administrator's Guide* for details.

Command line parameter: /MOV:

If you have more than one instance of an infected `COMMAND.COM`, for example, and you choose to move each copy into the same directory, then the scanner will rename each instance of the file.

[ ] **Overwrite then delete**

This instructs the scanner to overwrite and then delete infected files. If you subsequently run a utility such as UNDELETE, you can recover the file, but it will be full of random 1s and 0s, making it unusable.

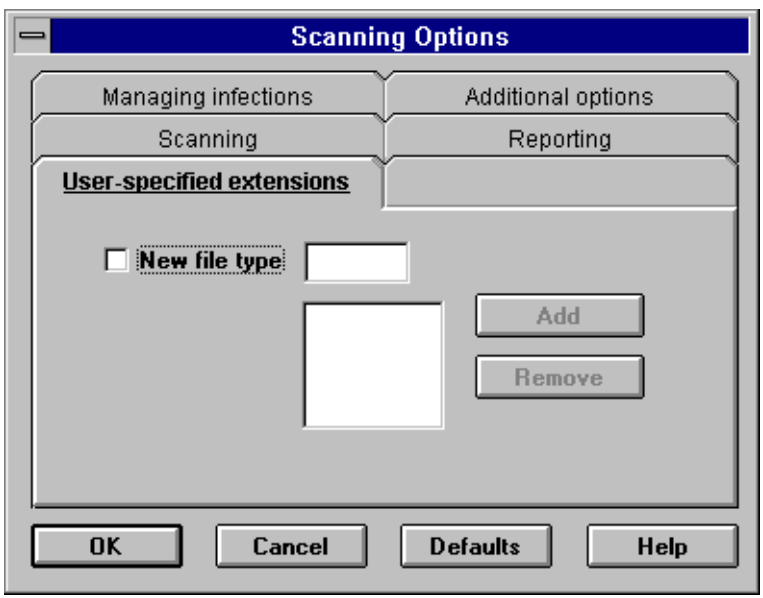
Command line parameter:	/D

User-Specified Extensions

Normally, only files with pre-defined extensions are scanned.

Please refer to the Read Me file for more details about pre-defined extensions.

In the Windows scanner, you can define up to **20** new file types from this dialog box:



To add a new file type:

1. Click on the [ ] **New file type** check box.
2. Type the file extension in the accompanying text box.

3. Click on the **Add** button.

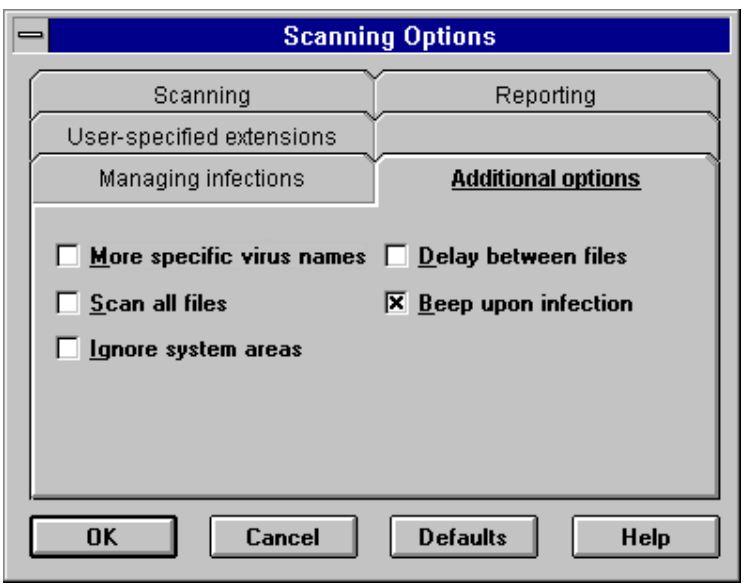
New file types will be saved in the NVC.INI file and will be used every time you run the program until you delete them.

To remove a user-specified file type, highlight the extension you wish to remove and then click on the **Remove** button.

Command line parameter: /E[extension]

Additional Options

To further optimize the scanning, choose additional options from this dialog box:



[ ] More specific virus names

This option allows the scanner to use secondary virus signatures when it finds a virus, resulting in a more specific name for the virus.

Note that this option does **not** increase the number of viruses detected but does increase scanning time.

Command line parameter: /Y

[ ] **Scan all files**

One of the goals a virus has is to infect other files. The most efficient way of doing this is to infect executables. Normally, you do not have to scan files other than NVCW's defaults. However, NVCW will scan all files it finds on a drive when you use this parameter. This is a helpful feature if you suspect you have a virus and want to check all files.

Note that if you choose this option, scanning time increases.

Command line parameter: /AF

[ ] **Ignore system areas**

By default, NVC always scans the system areas of a diskette or a local hard drive.

On repeated scanning on the same drive(s), you can check this option. NVCW will only scan the system areas of the same drive once and concentrate on the files.

Command line parameter: /BS-

[ ] **Delay between files**

If you are about to scan many files, you can use this option to minimize the workload on your PC by instructing the scanners to pause between each scanned file.

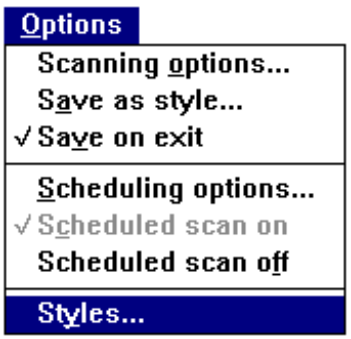
This feature has been designed specifically for networks. It also works well in multi-tasking environments such as Windows. The duration of the pause is 30 milliseconds by default. This default cannot be changed in the Windows scanner.

Command line parameter: /W:

[x] **Beep upon infection**

Usually during a run, NVCW beeps at the first instance of an infected file or boot area. Uncheck this option to turn off the beep.

Styles



Now that you've been through the scanning options, you may have got some ideas on how to configure your scans. Different tasks may call for different configurations.

If you have preferences for how the scanner is to be run, you may set those preferences, save your settings as **styles**, and then use the styles whenever you wish. Think of styles as templates for scanning.

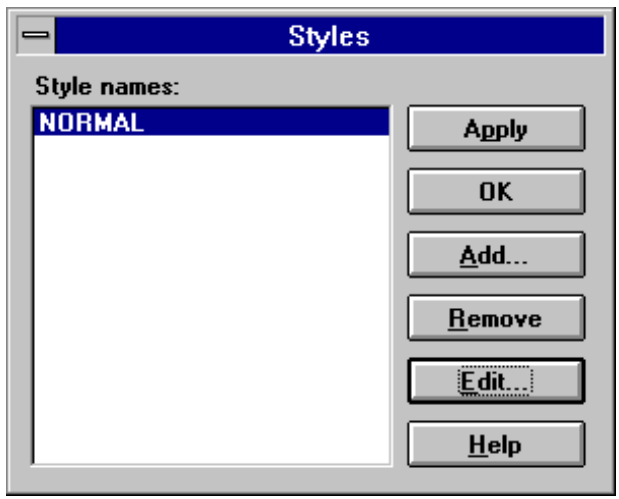
The scanner is shipped with the style <NORMAL> as default. This style can be modified but not deleted. All new styles are based on the factory default settings. These are the checked options in the "Scanning options" dialogs in the previous section.

See also"Scheduling" on page 115.

In addition to customizing <NORMAL>, you may create up to 20 additional styles.

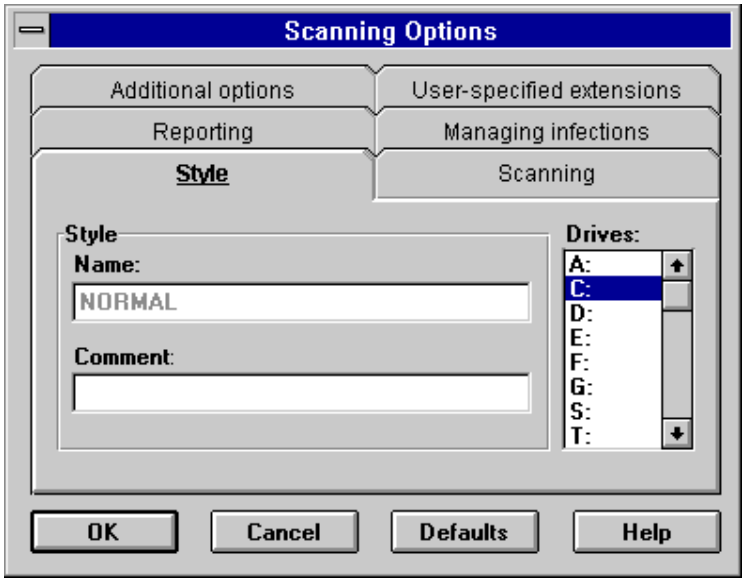
To customize or add styles, click on the Styles menu item from the Options menu.

This menu option provides this dialog box:



Modify the <NORMAL> Style

1. Click on the <NORMAL> style entry so that it is highlighted and click on **Edit**.
2. In the "Style" dialog, select the drive(s) that you wish to be scanned with this style.



3. Click on the relevant tabbed dialog boxes to set your options for this style.
4. Click on **OK** when you have entered your choices.
5. You are now back in the "Styles" dialog. If you wish subsequent scans to be based on the <NORMAL> style, then click on the **Apply** and **OK** buttons. This makes the <NORMAL> style current for all subsequent scans. Styles other than <NORMAL> can be used as current styles, if you wish. Click on the **Apply** button and then **OK** to make a style current.

Note: If any other style than <NORMAL> is current, the name of the current style appears on the title bar in the main window.

If you wish to have a scheduled scan occur later on based on a specific style, then you must choose Options|Scheduler options from the menu bar in order to set the time for the scheduled scan. Alternatively, click on the scheduler icon from the toolbar.

See “Scheduling” on page 115 for more details about scheduling scans.

Add a Style

1. Click on the **Add** button.
2. Type in a name for your style — up to 8 characters.
3. Follow the steps 2 - 4 above.
4. The new style name appears in the list box of styles.
5. Highlight the new style name and click on the **Apply** and **OK** buttons if you want to make the new style current.

You can enter up to 20 new styles. To check which style is current, open the “Styles” dialog box. The highlighted style is the current style.

The current style will also appear on the title bar in the main window.

Delete a Style

Note: You cannot delete the current style, so we have to sneak up on the style that you want to delete.

1. Choose any style from the combo box **except** the one that you wish to delete.
2. Click on **Apply**.
3. Now highlight the style you want to delete, but do **not** activate it — click only once.
4. Click on **Remove**.

The default style is <NORMAL> and cannot be deleted.

Start Virus Scanning Based on a Certain Style

1. Choose the style you want to use from the combo box.
2. Click on **Apply**. This makes the style current.
3. Click on **OK** to return to the main window.

4. Start the scanning process by clicking on **Start scan**.

Activating Styles from the Command Line

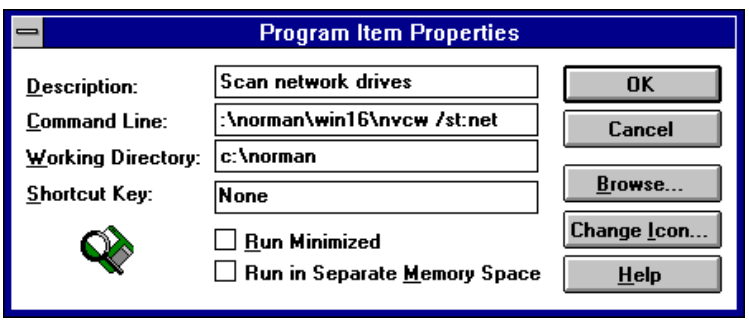
With the Windows scanner you can activate styles from the command line. In other words, you can force NVCW to use a certain style when it begins scanning. This is useful for creating customized icons which result in scanning using a particular configuration.

For example, if you wanted to have one icon for scanning networked drives and another one for scanning local drives during your lunch hour, you could use the following syntax for NVCW:

```
NVCW /ST:[name of style]
```

There must be **no** spaces between the parameter and the name of the style.

For example, to create a customized icon in Windows, choose File|New|Program Item from Program Manager and fill in the appropriate text boxes:



If you run the style NET as shown above and add other parameters, as in:

```
nvcw /st:net a: d:
```

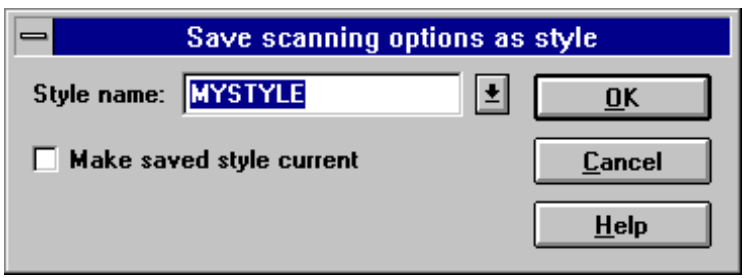
the added parameters override the style. In this example, only `a:` and `d:` are scanned.

Note: When this feature is used, you will not be able to change the configurations within the styles before the scan begins. If you wish to change the configuration of a style, do not use these parameters. Rather, load NVCW as you would normally by clicking on its icon.

Save as Style after Configuring

When you are changing the scanning options, the new settings will affect the current style. If you want to keep the original style the way it was, then you can save your changes as a new style.

From the main window, choose Options|Save as style, and you will see this dialog:



Type in the name of the new style.

If you intend to apply the new style now, check [ ] **Make saved style current** before you click on the **OK** button.

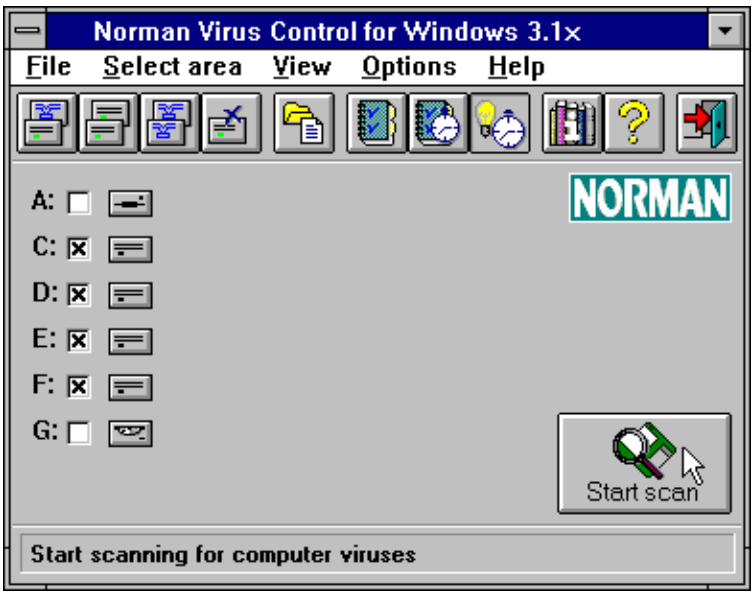
Save on Exit

The menu option Options|Save on exit is on by default. If you change the settings for a style, they are permanently saved when you exit NVCW.

If Options|Save on exit is OFF, changes to a style are only valid for the present NVCW session.

Starting the Windows Scanner

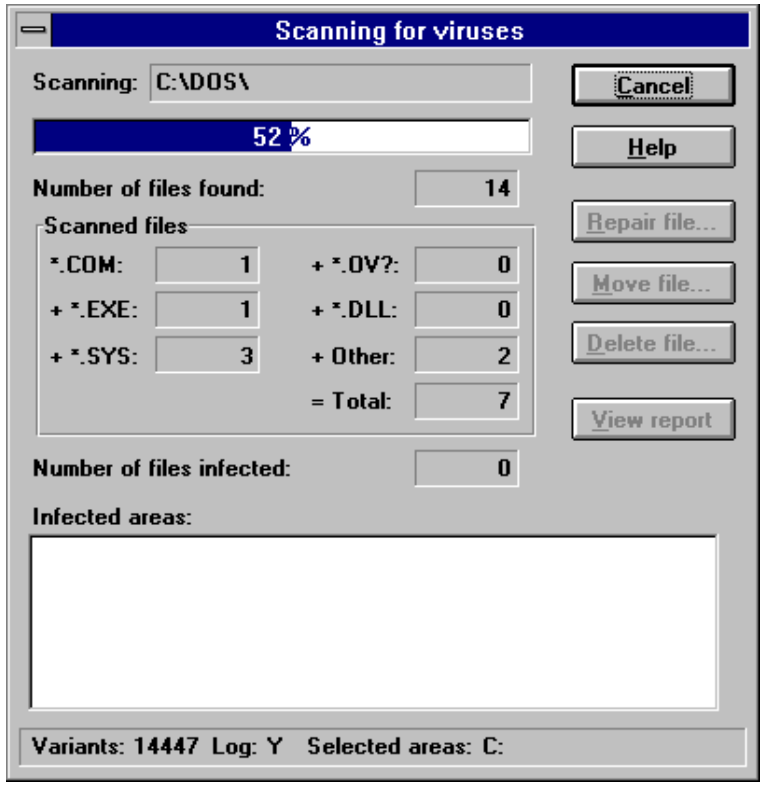
When you have decided where and how to scan, click on the **Start scan** button in the main window:



Unless you have specified otherwise, NVCW scans the system's memory first.

After the memory scan is completed, NVCW pops up the "Scanning for viruses" dialog box which shows its progress as it scans the system areas followed by files with certain pre-defined extensions.

The dialog contains status information, an overview of infected files, and six buttons.



In the uppermost part of the dialog box, NVCW.EXE displays the following information, updating it as the scan progresses:

Scanning: this shows the area that is currently being scanned.

The dialog box also contains a horizontal progress bar which shows the percentage of the scan that has been completed.

Number of files found: the number of files that have been found in the specified scanning area so far in the process.

Scanned files: the number of files with certain extensions which have been scanned so far in the process.

Note: The number of files found in the specified directory will almost always be different than the number of files scanned because NVCW only scans files with the default extensions in addition to the user-defined file types you specify.

See the Read Me file for more information on pre-defined file extensions.

Number of files infected: the total number of infected files that NVCW has found so far in the process.

Below the progress bar is a list box that contains the path and filename of all infected files along with the name of the virus that has infected these files.

If the list of infected files is long, you can scroll through the list box by using the scrollbar or the [PgUp] and [PgDn] keys.

At the bottom of the dialog box is a status line. This line summarizes three pieces of information:

Variants:
Shows the number of viruses and variants this version of the scanner is able to recognize.

Log:
Shows you whether or not the report function is activated. This field can have the values Y or N.

Selected areas:
Shows what area(s) is included in the scan.

In the right hand side of the window you will find a column of buttons:

Cancel/OK:
This button will contain one of two different messages, depending on the status of the scanning.

When the program is in process, the button will appear as **Cancel**. When you click on the **Cancel** button, you instruct

NVCW to abort the scan. You will get a status message about the scanned area before the scanner stopped.

Note: To abort a command line scan, press [Esc]. Remember, however, by using the /SN parameter you can force the scanner not to abort when a user presses [Esc].

Help
Gives direct access to the NVCW help system, which is context sensitive. That is, when you click the help button, NVCW brings you directly to the help screen which explains the use of the function you are currently using.

Repair file
If you did not check the **[ ] Repair file if possible** option in the Managing Infections tabbed dialog, this button becomes available if a virus is detected. Highlight the infected file/ area and click on the **Repair file** button.

Delete file
If you did not check the **[ ] Delete infected files** in the Managing Infections tabbed dialog, then highlight the infected file in the list box and click on the Delete file button

*When you delete a file from the "Scanning for viruses" dialog box, the file is **not** overwritten before it is deleted.*

Move file
This button permits you to move selected infected file(s) -- even if you did not set the scanner to move infected files to a specified directory.

To move an infected file, click once on the file (in the "Infected areas" list box), and then click on **Move to...**

The scanner will ask you to confirm that you want to move the infected file to the directory specified in the “Managing infections” tabbed dialog.

The default directory is `C:\NORMAN\INFECTED`. If you specify a different directory and the directory does not

exist, the scanner will create it. Click on the **Other dir** button to select a different directory.

You might have several infected files which happen to have the same name. If the scanner tries to move a file to a certain directory and finds that the filename already exists in that directory, it will change the name of the newest file until it is unique.

When a Virus Is Found

The option of automatic removal of known viruses is implemented in the scanning function. During on-demand and scheduled scans, the scanner will check for known viruses. If a virus is found, the scanner will try to remove it on-the-fly.

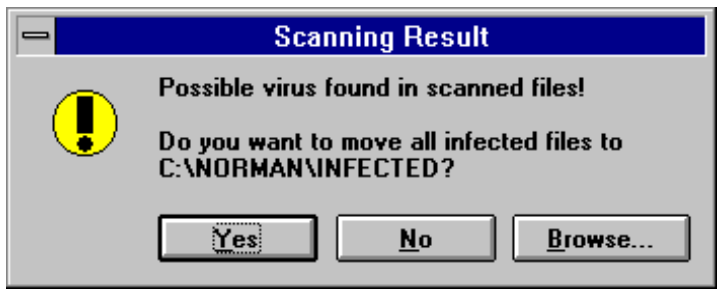
Viruses cannot be removed in the following situations:

1. The file resides on a write-protected diskette or CD-ROM
2. The file resides on a network drive and is write-protected,
3. The file is in use (i.e., you do not have write access).

If a virus is detected during the scan, you'll be notified about the infection. The messages you get depends on what you specified in the "Managing infections" dialog (see page 74).

If you specified "Delete infected files", you'll see this dialog:

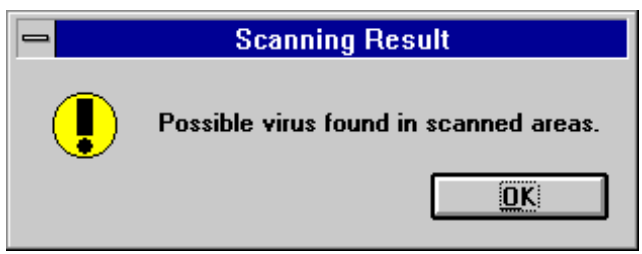
If you specified “Move infected files to”, a dialog will ask you to confirm moving to the directory you specified:



In the future if you want NVCW to move **all** infected files to a specific directory, go back to the “Managing infections” dialog box, click on [ ] **Move infected files to**, and type in the name of the directory to which the infected files should be moved. When infections are found, you will be prompted to move the infected files to the directory you entered, or even select a new directory by clicking the **Browse** button.

You might have several infected files which happen to have the same name. If NVCW tries to move a file to a certain directory and finds that the filename already exists in that directory, it will change the name of the newest file until it is unique.

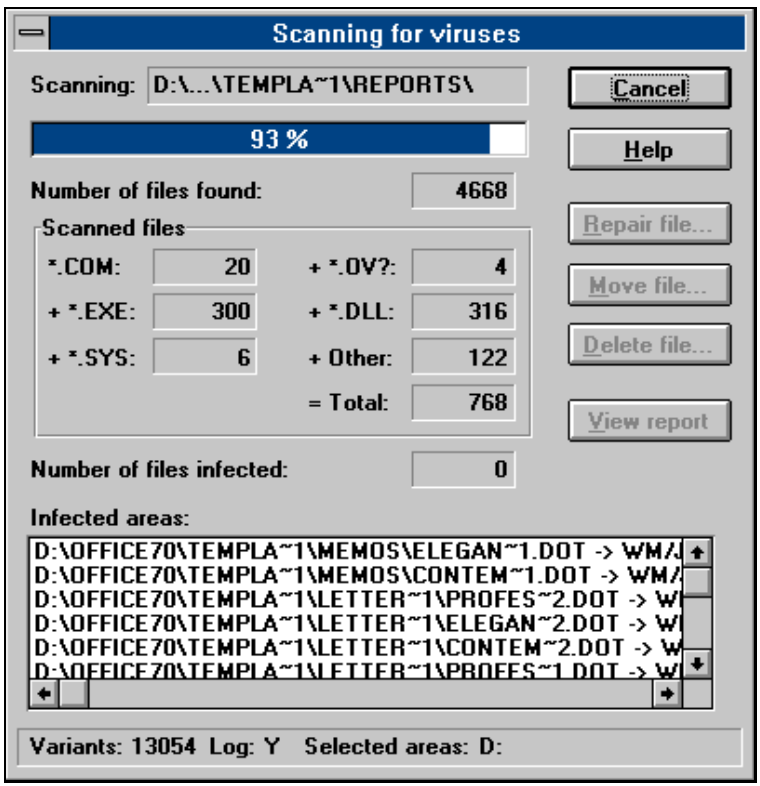
If you specified [ ] **No action**, you will see this dialog:



When you click on **OK**, you’ll return to the “Scanning for viruses” display. Note that the infected file(s) appears in the

"Infected areas" list box with details about the virus and where it's located.

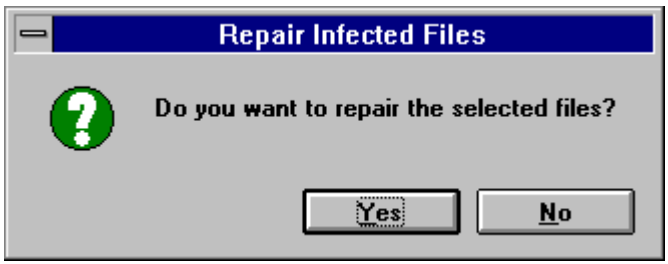
In the "Infected areas" list box at the bottom of the "Scanning for viruses" display, you will receive information on infected files when you run an on-demand scan. The scanner reports the path and name of the infected file and the virus name.



Files infected by viruses that could not be removed are listed. Highlight the infected area by clicking on it **once**. The buttons **Move file** and **Delete file** are now activated, and you are allowed to delete or move the infected files.

The **Repair file** button is activated when you highlight a file with a virus that can be removed by the scanner.

First, try to remove the virus by highlighting the infected file in the list box and then click on the **Repair file** button. You will see this message:

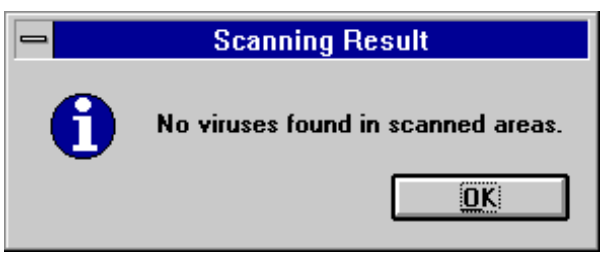


Click **Yes**. If the file can be repaired, it will no longer appear in the Infected areas listbox.

Note: If an infected file resides on a write-protected diskette, on a CD-ROM, or on a protected area on a server, the scanner cannot repair, move, or delete the file.

When No Viruses Are Found

And if no virus is detected, this dialog box appears:



Hopefully, this is the message you'll get most of the time!

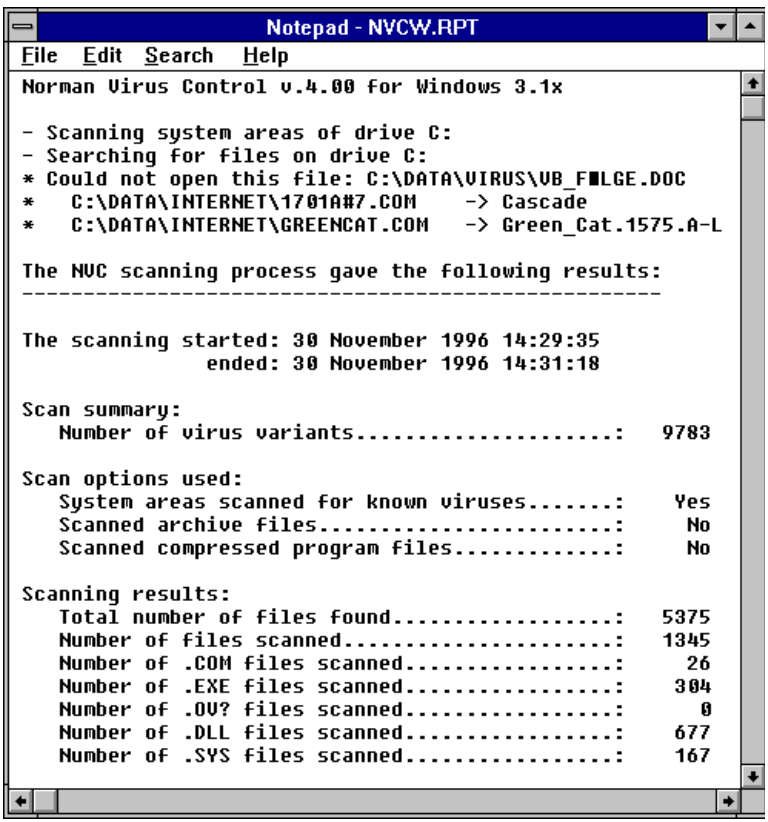
View the Scanning Report

View report: If you have chosen either of the report options from the tabbed dialog "Reporting"

(Options|Scanning options), you have the opportunity to view the report on the screen.

The **View report** button appears grayed until the scan is completed and remains gray if no report option is selected.

After NVCW has created the report, you can click on **View report**, and it displays the contents of the report, either through Windows Notepad or Windows Write, depending upon the size of the report file (Notepad cannot handle a file larger than 32 KB).



You can scroll through the report by using either the scroll bar or the [PgUp] and [PgDn] keys. You can also save it as a different filename, print it, and so on.

Report File Structure

The report file consists of:

- A file header, stating the program name and version.
- A scan report section, containing information about directories and files scanned, and possible virus infections.
- A summary section.

Please refer to the *Administrator's Guide* for more details about the report file structure.

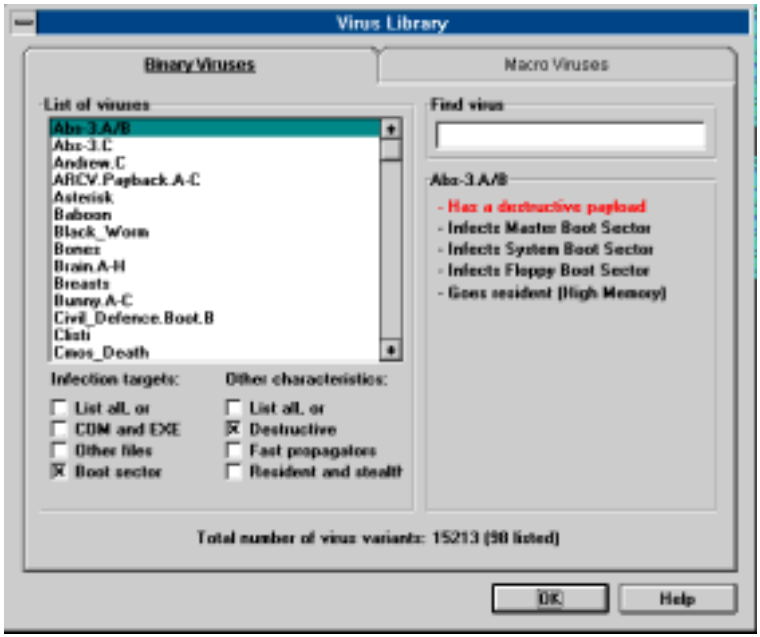
Virus Library

In the Windows menu-driven scanner, this function is available from View|Virus library in the main window or by clicking on the toolbar button:

Computer viruses can be categorized in two distinctly different classes: binary and macro viruses.

1. *Binary, file and system viruses* contain executable code, i.e. program instructions. Binary viruses can infect program files (frequently referred to as executables), boot sectors, or other executable code on your PC.
2. *Macro viruses* do not contain executable code. They employ the macro programming language used in most word processors and spreadsheets. Macro viruses will infect Word or Excel files, for example, and replicate when infected files are accessed. Macro viruses do not depend on specific microprocessors or operating systems.

The virus library contains two tabbed dialogs, one for binary viruses and one for macro viruses. Here you will find key information for every virus in this list.



The total number of viruses identified is virtually increasing by the hour, and the list is consequently quite extensive. Because viruses are treated differently depending on type and property, it is useful to gather as much information as possible about the virus.

The list box on the left of the dialog box contains the names of the viruses that the scanner can recognize. The area on the right describes the most important characteristics of the virus that you have chosen from the list. The complete list is sorted alphabetically. Because of its comprehensive nature, it may be time-consuming to use the arrow keys to navigate through the list. Therefore, you can search for viruses using other methods.

- Use the scrollbar to the right of the list box to move quickly through the list. Then highlight a list item for more information on this virus.
- If you know the first letter of the virus you are looking for, you can simply type its first letter from the keyboard. The first virus whose name starts with

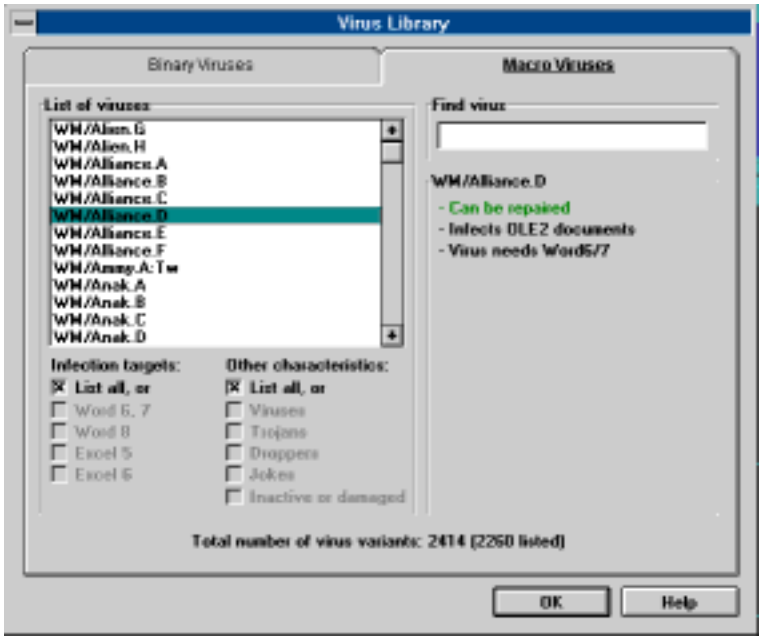
this letter will appear as the first item in the box. Continue pressing the same key until the desired virus appears highlighted.

- If you know the full name of the virus you are searching for, you can use the [Tab] key to set the focus on the text box to the right of the list box. Then type the name of the virus and press [Enter].
- You can narrow your search by clicking the check boxes in the two columns under the list box. The left hand column displays viruses by what they infect, while the right hand column allows you to sort viruses by how they perform.

If you check the [ ] **List all, or** check boxes, the other options in that column are grayed out.

There are many viruses that are known by several names. Hence, a virus you are looking for under one name may be in this list under another name. Call us if you can't find the virus for which you are searching...

Binary Virus Attributes



These are the possible attributes for binary viruses:

It has a destructive payload

While most viruses are relatively harmless, this virus will perform destructive acts such as delete critical files, format your hard drive, or destroy other data.

It is a fast propagator

The virus stays in memory (goes resident) and hooks the services used by other programs to open, read, write and/or close files. Whenever any program opens a file, this will start the virus code, infecting the opened file, or look for another file to infect.

Uses encryption

The virus code itself is encrypted to avoid detection. It can be detected anyway.

Uses stealth techniques

The virus tries to hide itself to avoid detection. It is normally detected anyway.

Overwrites original file

The virus code overwrites parts of the infected file. Files infected this way cannot be cleaned, but must be replaced from backups in order to get rid of the virus.

Boot Sector

Infects boot sectors on diskettes and/or hard drives. Will in most cases infect the hard drive if left in the diskette drive when the PC is booted.

EXE, COM files

Infects mainly EXE or COM files or both.

COMMAND.COM

Infects COMMAND.COM.

OV? files

Infects overlay files. An overlay file is a part of a program split in separate, overlayed, files.

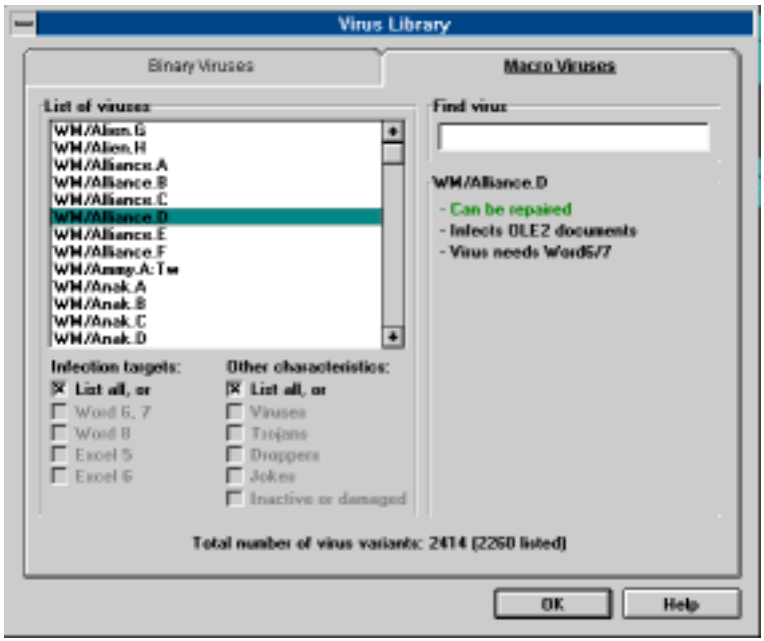
Other files

Infects other files.

Goes resident in Low, High, UMB, Video RAM

The virus stays in memory when first activated.

Macro Virus Attributes



These are the possible attributes for macro viruses:

Can be repaired

Documents or template files infected by macro viruses can in most cases be repaired. Technically, this involves removal of the viral macros, while legal, user defined macros are left intact.

However, some macro viruses "snatch" user defined macros while replicating, making each infection unique. The user defined macros will in most cases be changed to call the main macro in the virus. The WM/CAP family of macro viruses is an example of viruses with this capability. Files infected by this kind of virus are repaired by removing **all** macros.

It has a destructive payload

While most viruses are relatively harmless, this virus will perform destructive acts such as delete critical files, format your hard drive, or destroy other data.

Is polymorphic

The virus changes itself from infection to infection.

Is a Virus

This is a true virus, able to replicate itself. Opening this document will trigger the macros, probably infecting other document files.

Is a Trojan

This is not a virus, meaning that it doesn't replicate. Contains other forms of malicious code.

Drops binary virus

This macro virus contains a binary virus.

Is a joke, non-infectious

This document file contains macro code that performs harmless, sometimes visible, actions. Opening this document will trigger the macros, but no other document files will be infected.

Contains garbage
Is inactive or damaged.

This document file contains remnants of macro viruses, or other macros that don't work as intended.

Infects Word2 documents

This document file contains a macro virus that requires Microsoft Word version 2 to replicate.

Infects OLE2 documents
Virus needs Word6/7 (Office '95)
Virus needs Excel6 (Office '95)
Virus needs Word8 (Office '97)
Virus needs Excel6 (Office '97)

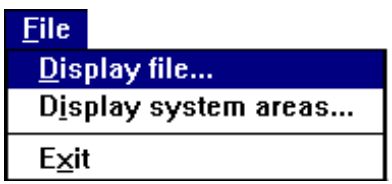
This document file contains a macro virus that needs one of the specified Microsoft applications to replicate.

Functions Specific to the Windows Menu-Driven Scanner

There are a few features available in the Windows menu-driven scanner that are not available in other Norman scanners.

- Display file/system area
- Styles
- Fast scan
- Drag and drop
- Running in the background
- Book on viruses

Display function

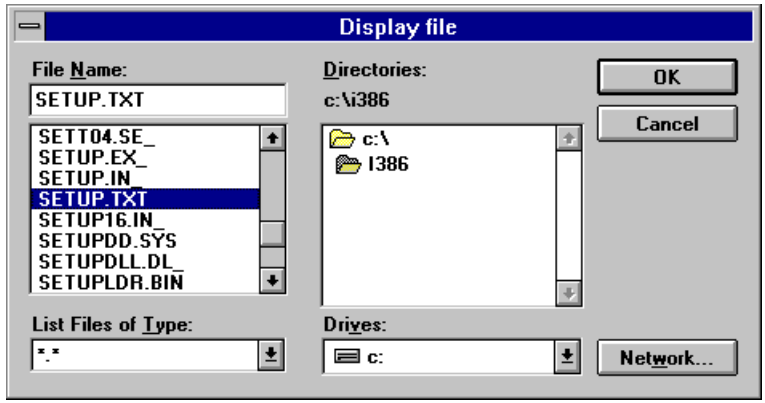


This function is available from the main window option File.

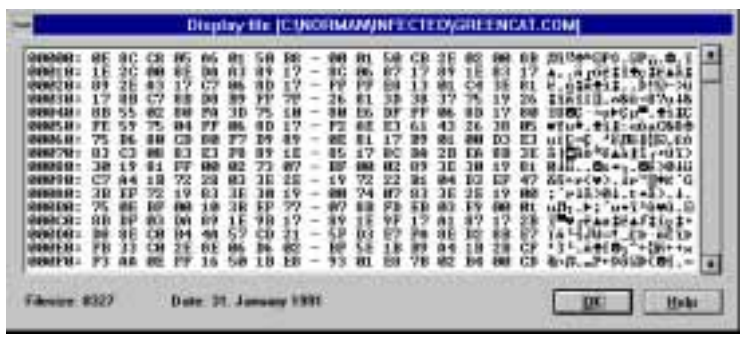
If you want to take a look at the contents of a file (presented as hexadecimal values and printable characters), or if you wish to look at the contents of the system areas on your boot drive, you may choose the display options.

Display Files

If you choose File|Display file, you can pick a file from within a window, like this:



When you have chosen a file to display, the following dialog box appears:



The dialog box shows you the file contents as hexadecimal values (left) and text (right). To maneuver up and down within the file, use the scrollbar along the right edge of the dialog box.

This function is especially useful when technical personnel want to look inside a file or sector for signs of a virus infection.

There are two buttons at the bottom of the dialog box:

OK quits from the function and returns you to the main window.

Help gives you help on the display function.

Display System Areas

If you choose File|Display system areas from the main window, this screen will appear:

The System area includes the Master Boot Sector (MBS) and System Boot Sector (SBS).

You have a choice of viewing the MBS area of the first physical hard drive as well as the SBS on drive C:.

Master Boot Sector (MBS)

The MBS is located on all physical hard drives. It contains, among other data, information about the partition table (information about how a physical disk is divided into logical disks), and a short program that can interpret the partition information to find out where the System Boot Sector is located. MBS is independent of type of operating system.

System Boot Sector (SBS)

The SBS is located on all diskettes and physical hard drives that are formatted, and it is created with FORMAT.COM. It contains, among other data, a program whose purpose is to find and run an operating system (DOS, UNIX, or OS/2, for example).

If the program does not find an operating system to run, the user will be prompted for a diskette with an operating system on it.

Scanning Diskettes

You should be aware of the following situation when you are scanning diskettes:

If a boot virus is found on the diskette by the **Windows** menu-driven scanner **and** the Smart Behavior Blocker is active **and** the diskette is write-enabled, NVC.SYS will automatically remove the boot virus. Subsequent scans will report that the diskette is not infected with a boot virus.

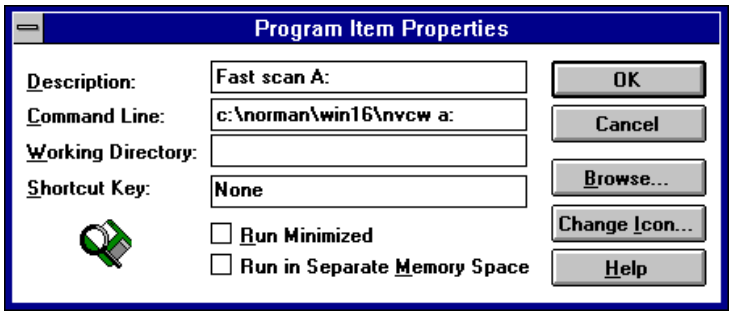
Fast Scans

You can set up icons in Program Manager to scan a specific **drive** using the **scanning options** from the current style.

Note: Remember that the current style stores drive information. By using this method, however, you can override the drive information in the current style, but you use the scanning configuration information from the current style.

Simply create a new icon. (In Windows, click on File|New|Program Item.) And on the command line, specify the drive and path for NVCW.EXE. Follow it with a space and the letter of the drive that you wish to scan. Don't forget the ":".

For example, here is what your Program Item Properties would look like:



Clicking on the resulting icon will do the following:

The Windows scanner will automatically start scanning A:. The scanning options will be determined by the options defined in the **current** style.

Drag and Drop

Note: This is available only when you use it with another application that supports drag and drop.

You can automatically scan a drive, directory, or file by:

Ensuring that the scanner is active — either maximized or minimized

Starting an application that supports drag and drop (i.e., File Manager in Windows)

Selecting the target drive, directory, or file and dragging it to the Norman scanner icon (if it is minimized) or to the Norman scanner main window (if it is maximized).

The scanner will automatically scan the selected target, using the scanning options in the current style.

Running in the Background

If you are scanning a large hard drive, you can minimize the scanner after it has started. This will allow it to work in the background while you move on to other tasks. When

the scan is complete, you will be informed if viruses are found.

Book on Viruses

As an extra feature, the Norman Book on Viruses is available in the Windows help file format.

Topics include: international trends and evolution, removing a virus, virus theory, and more. Navigate through all this information by clicking on the green entries.

Command Line Scanning

The command line scanners are not dependent on any other modules. They can send virus alert information to FireBreak through IPX communications, and they can be run from batch files. For more details, see "Norman programs and IPX communications" in the *Administrator's Guide*.

The 32 bit command line scanner is available on the following platforms:

Platform:	Exe file:	Default location:
Windows 3.1x	`NVC32X`	`c:\norman\dos`
Windows 95	`NVC32`	`c:\norman\win32`
Windows NT	`NVC32`	`c:\norman\win32`
OS/2	`NVC32`	`c:\norman\os2`

Using the Command Line Scanner

The syntax is:

```
nvc32x [drive]:[path] [/parameters]
[Enter]
```

Note: A space must precede each parameter that you use.

Simply select the combination of parameters that you wish to use and specify them on the command line.

Scanning Options

From the directory where the Norman programs reside, run the command

`nvc32x /?`

from the command line to display a list of available options. The following tables chart out the available parameters and their functions. The first table presents parameters that are relevant for the ordinary user. The second table explains parameters that may be useful for system administrators

Param.:	Function:
/?	Show help.
/ALD	Scan all local disks (not diskettes or CD-ROM).
/AD	Scan all disks (not diskettes). Possible network drives are scanned in addition to local fixed drives.
/AF	Scan all files. The default is files with extensions like .exe, .com, .doc etc. The list is continously reviewed and therefore presented in the readme file.
/B	No alarm when infections are found.
/BS-	Ignore system areas from scanning. The system areas of the same drive will only be scanned once if several file specifications for the same logical drive are specified.
/BS+	Scan system areas only.
/C	Scan archive files. Infected files can be found within archive files, and you can instruct NVC to look inside the archive file.
/CP	Scan compressed program files. A decompressor emulator will open and scan the file in memory.
	The scanner can only tell you whether or not an archive file or a compressed program file is infected. It cannot take any action on the infected file while it is archived/compressed.

Param.:	Function:
/CL	Repair files when possible. With this parameter, NVC will prompt you to confirm prior to cleaning infected boot sectors and files. When /CL is used concurrently with /U or /Q, however, NVC will not prompt you before cleaning.
/D	Overwrite and delete infected files. Recovery of an overwritten file is not possible.
/D-	Delete infected files. Infected files are automatically deleted. Since we are not overwriting the file before we delete, recovery of the infected file is possible with tools such as the Norton Utilities.
	If the /D or /D- parameters above are used together with /CL, /CL will take precedence. If the file cannot be repaired, it will be overwritten and/or deleted.
/H	Show help.
/LA	Log all scanned files. By default, the command line scanner will only log names of scanned directories and infected files. This parameter forces the scanner to log the names of all files that were scanned. If you wish to specify the name of the log file, then pair this parameter with /LF.
/LF:	Log to specifed report file. Type in the name immediately after the parameter (no spaces).
/LF	Log to standard report file NORMAN.RPT.
/LG	Append log to existing report file. Default is overwrite.
/LQ	Create report file only when infections found.
/LS	Log all scanned directories.
	Note that in order to produce a report, you must specify one of the L options above.*

Param.:	Function:
/MOV	Move infected files to default INFECTED directory (c:\norman\infected).
/MOV:	Move infected files to specified directory. Type in the name immediately after the parameter (no spaces). If you don't type in a directory, NVC will create it for you relative to where the NSE directory is located. If it is installed in c:\norman\nse, the infected directory will be c:\norman\infected.
/N	Suppress the default memory scan.
/NW	Don't display messages regarding the status of your licence (for example, licence expiration).
/O	Ignore files that cannot be opened. If you have specified a log file, locked files are listed there.
/Q	Quiet mode, i.e. no screen output at all. Overrules the /O and /U parameters.
/R	Repeat the scan. Useful for checking several diskettes.
/S	Scan subdirectories. Use this option if you have specified a directory and want to include subdirectories in the scan. If you have specified a drive letter, subdirectories are automatically included in the scan.
/V	Verbose mode. Display all details during scan.
/W:	Wait specified number of milliseconds between each file.
/X	Look for EXE header in all files. Like /AF, this parameter will increase the scanning time because all files are checked.
/Y	Display detailed virus name.
/YH	Abort the scan when a virus is found and display the path and virus name.

The following command line parameters are useful for system administrators:

Parameter:	Function:
/NVCADMCFG:	Override environment NVCADMCFG, where the program looks for nvcadm32.cfg (if nvc32.cfg is not found). If no such environment is defined, the program will search for the file one level up from where it is executing.
/NVCCFG:	Override environment NVCCFG, where the program looks for nvc32.cfg. If no such environment is defined, the program will search for the file one level up from where it is executing.
/SN	Do not allow user aborts.
/TEMP:	Override environments TEMP/TMP. If no such environment is defined, the program will create it one level up from where the directory NSE is located.
/U	Do not stop when infections are found. Overrules the /O parameter.
/WORK:	Specify where NORMAN.RPT and INFECTED directory is created. If nothing is specified, the program will place the report file one level up from where it is executing.

Combining Different Parameters

The command line scanner is flexible in the sense that you can combine parameters to carry out multiple tasks in one command.

Here are a couple of examples on how you can combine parameters. From the directory where `nvc32x.exe` is installed, type:

```
nvc32x a:\*.txt /n /bs- /lf
```

This will scan all files on the diskette with the extension `.txt`, the boot sector will not be scanned, and the `norman.rpt` will be created in the directory where `nvc32x.exe` is installed.

Then type:

```
nvc32x *.txt a: c:
```

to scan `txt` files in the current directory and then the boot areas and default file extensions on `a:` and `c:`.

Note: Specifying `c:\` (with a slash) will scan files only in the root drive, but `c:` (without a slash) will both scan files and the disk's system areas.

Command Line Scanner Errorlevels

You can automate the command line scanners by using errorlevels in batch files. The errorlevels for the command line scanners are::

Errorlevel:	Meaning:
13	Licence does not allow the program to start.
12	The file `NVC32.CFG` was not found.
10	Files skipped (could not be accessed).
9	The scanner was interrupted and did not complete its scan.
8	The scanner stopped due to an error in logic.
6	Disk input/output error.
5	You did not enter valid scanning criteria.

Errorlevel:	Meaning:
4	The hardware configuration has changed since you installed the scanner.
3	The scan began without having any scanning criteria.
2	Detected an active virus in memory.
1	Detected one or more viruses in one or more files.
0	Scanned for viruses and did not find any.

Scheduling

Overview

Many users like to have the flexibility to schedule virus scans periodically.

From the scheduler you can define:

- which area to scan
- when scanning should start
- where to scan

This is what you do:

1. Save the scanning configuration that you wish to use during a scheduled scan and save as a separate style. See “Save as Style after Configuring” on page 85.
2. Determine when you wish to start the scheduled scan. Choose between once, hourly, daily, weekly, or monthly. You can schedule up to 8 scans to run at different times.

Although scheduler options can be accessed through the scanner, scheduled scans cannot commence if the scheduler is disabled.

Make sure that the scheduler is always enabled. However, either of the following situations will prevent a scheduled scan from running:

1. NVCW is active. You must exit the main window altogether in order for a scheduled scan to run.
2. Your PC in switched off.
3. The “Scheduled scan on” option is unchecked. In this case, the scheduler button appears grayed on the toolbar.

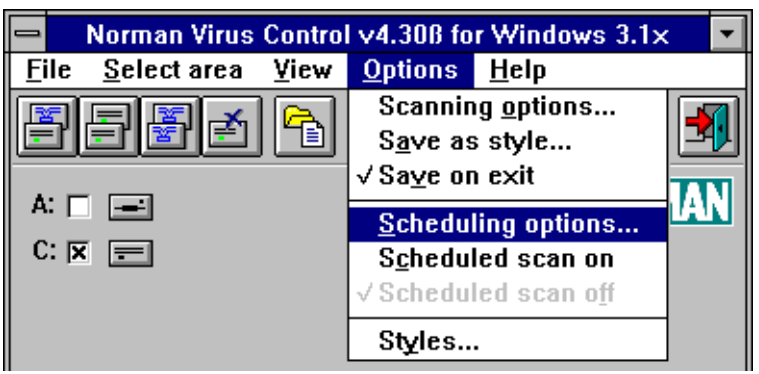
4. The style for a scheduled scan does not exist (i.e., it was deleted after the scan was scheduled).

Note: If you enter a date and/or time **before** the current day and time, the scheduler will start the scan 15 seconds after it's been enabled.

Scheduling Scans

You can access the scheduling options by clicking the scheduler button on the toolbar

or from the Options pull-down menu:



About the scheduling menu options:

- Scheduling options brings you to the scheduler, where you enter all the details about when and where scanning shall take place.
- Scheduled scan on activates the scheduler.
- Scheduled scan off deactivates the scheduler.

Enter a Scheduled Scan

When you enter Scheduling options for the first time, this is what you see:

A sample weekly scan based on the <NORMAL> style appears in gray under “Scheduled events”.

The row at the top of the screen shows details about the next scheduled scan. You can see what time it starts (time is displayed in 24 hour format), weekday, date, month, year, and what style will be used for the scan.

See also “Save as Style after Configuring” on page 85.

Common to all fields

The scheduler consists of a number of fields with different options that you can view by pressing the arrow up/down keys on your keyboard. You can also click on the arrows to the far right to display the alternatives for the current field.

Use the [Tab] key or mouse pointer to move from one field to another.

The intercorrelation between the Weekday, Day, Month, and Year fields ensures consistency for the values you enter.

You can define a maximum of 8 scheduled scans.

To enter a scheduled scan:

1. Click on the [ ]**Schedule** check box to enter a scheduling task. If unchecked, all fields are grayed out.
2. In the next field you specify the frequency of the scan. You can choose from:
   - Hourly from
   - Once at
   - Today at
   - Daily from
   - Weekly from
   - Monthly from
3. Enter the hour and minute that the scan should start. The hours are presented in the 24 hour format, and the minutes are given in 5 minute increments.
4. Select a weekday. If you entered "Today at" in #2 above, then weekday, date and year is grayed out and the present day and date appears.
5. When you specify the frequency of a scan, the weekday, date and year appear in their respective fields with the current date as the default. Changing the "Weekday" automatically updates the date field. Also, if you change the "Day" field, the weekday changes accordingly.
6. If you change the month, the numeric value in the "Day" field remains the same, while the "Weekday" field is corrected.
7. If you change the year, the month and the numeric value in the "Day" field remains the same, while the "Weekday" is corrected.

8. Finally you must specify which style to run. The <NORMAL> style is the default. Use the arrow keys to scroll through the available styles.

Note: Remember to click the [ ]**Enable scheduling** check box and **OK** to enable the scheduled task(s).

Also remember to exit NVCW altogether when you're done. A scheduled scan is not allowed to start when NVCW is active. The logic is that if you're performing a task in NVCW, a scheduled scan would interrupt your work and inflict loss of data.

Buttons

Click on **OK** to return to the main window when you have entered your choices.

Click on **Cancel** to return to the main window without saving your work.

Click on **Undo** to remove all entries for the current input.

Click on **Clear all** to clear all entries from the screen. If you then click on **Undo**, all previously saved entries are retrieved.

Scheduled Scan On/Off

The menu item Options|Scheduled scan will be turned ON automatically if you have entered and enabled scheduled scans. If you deactivate this option or if one of the situations listed above is true, the scheduler will run overdue scans next time it's activated.

In other words, scheduled scans not yet run are queued up for scanning like future scans are.

If several scheduled scans failed to run, the scheduler will run one scan per specified style from the queue.

The same principle applies if your machine is running, but you are using the scanner for other tasks at the time a scheduled scan is due. The scheduler waits until you exit NVCW and then activates the scanner to perform the scheduled task.

You can tell if the scheduler is activated by looking at the toolbar. If the scheduler is active, this button will appear with an illuminated light bulb, like this:

If the scheduler is not active, or if no scans have been scheduled, it looks like this:

Clicking on this button will toggle between activating and deactivating the scheduler.

Appendix A

General information on installation/updates

Any virus scanner is only as effective as its most recent update, so obtaining frequent virus signature updates is critical to maintaining a secure computing environment

---

There are two different kinds of updates for NVC:

Version update: actual program changes for one or more of the modules in the package. To install a version update, run a regular install as described in the setup procedure.

Definition file update: changes to the files `nvcbin.def` and `nvcmacro.def` (in c:\norman\nse). These files hold the virus signatures (fingerprints of known viruses) and are used by the scanning engine. To install a definition file update, doubleclick on the file name and follow the instructions on the screen.

Definition file updates are available from our Web site on a regular basis. We recommend that you pay us a visit at:

http://www.norman.no/update.htm

Index

—N—

—O—

—P—

—Q—

—R—

—S—

—T—

—U—

—V—

—W—