NORMAN®

Norman Virus Control for Windows NT

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.

March 1999

Conventions

We use the following conventions throughout this manual:

When we give examples of what you should type in order to use a particular program, the examples look like this:

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

We designate certain keys by surrounding the keyname with "[" and "]", as in:

[Ctrl]

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

File|Run

This means that you should click on the "File" menu and from there click on the "Run" menu item.

Hints and important notes appear in boxes like the one below:

Note: Here is a hint about how to use the scanner...

Individual words or phrases that we intend to stress are in bold:

This virus is **very** dangerous and will...

System Requirements

Norman Virus Control for Windows NT can run on any machine that runs Windows NT Workstation 3.51 and above or Windows NT Server 3.5 and above.

The NVC NT Service requires Windows NT 3.51 with service pack 5, or Windows NT 4.0 with service pack 3.

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. 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

Live Update of NVC

Updates to the scanning engine (definition files, DLL/VxD) are still available from our web sites. In addition, we introduce a polling program that automatically will check for updated files on Norman servers. This program requires that you’re connected to the Internet, and it’s available on the Windows 32 platform (Windows 9x and Windows NT).

Please refer to “Updating NVC” on page 114 for more information about this feature.

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

About Norman Virus Control for Windows NT

Microsoft Windows™ is a familiar sight on desktops around the world. Many organizations, however, are taking their Windows implementation to its next level and installing Windows NT™ for workstations and servers. The main differences between Windows NT and Windows are that Windows NT has full 32 bit memory addressing and is a multi-threaded-, preemptive multi-tasking operating system. In addition, NT is a more stable environment.

Although the security feature is one that Microsoft emphasizes in the marketing of NT, there is still a need for an anti-virus solution for NT.

About NT Services

A service in the Microsoft Windows NT environment is a program that can run whenever the computer is running the operating system. It does not require a user to be logged on. Services are needed to perform user-independent tasks such as directory replication, process monitoring, or services to other machines on a network, such as support for the Internet HTTP protocol.

Most System Administrators prefer to log off from the NT console when they leave their NT machine. This means that no unauthorized personnel have access to the NT console, but users may still log onto the machine via the network. At this stage, no applications can be executed from the console. Service processes, however, are performed according to how they were set up unless the machine is shut down.

Virus Protection for Windows NT

This is why NVC for Windows NT includes an NT service module for virus protection. Since the user does not have to be logged on, various kinds of virus protective operations may take place without user interaction or attention.

Functions in NVC for Windows NT

NVC for Windows NT is comprised of several functions:

- Real-time scanner

  Real-time scanning involves constant monitoring of the file systems. Whenever a file is accessed in a read/write operation or a program is executed, the NVC NT Service is notified and scans the file on the fly.

  In real-time scanning, the application is communicating with the operating system at a low level, enabling the NT Service to “see” all activities on the system. A real-time virus control program is therefore allowed to check for viruses whenever files are accessed. See “Configure Real-Time Scanning” on page 86 for more information.

- Windows scanner

  This is a true Windows NT virus scanner that takes advantage of the Windows NT (v3.51 and above) 32 bit environment.

  The scanner detects and removes all viruses contained in the definition files NVCBIN.DEF and NVCMACRO.DEF. The definition files are updated frequently and available for downloading from our Web site:

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

For automated downloads, see “Updating NVC” on page 114.

You can use the Windows scanner to perform on-demand and scheduled scans at specified intervals.

You may create your own icons which run the scanner with a command line parameter in order to scan using a certain "style" just by clicking on one icon.

- Right-click scanner for on-demand scanning.
- Command Line Scanner

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

- Scheduler

  The scheduler is configurable from within the scanner. If you wish to schedule automatic scans for specific dates and times, use the scheduler function. You may configure scans to run once, hourly, daily, weekly, or monthly. You may even configure several "styles" to run day and night.

- Virus definition files
- A configuration file
- A book on viruses in Windows help file format
- Help file for NVC for Windows NT
- Virus library
- Display functions

NVCNT.EXE and the NVC NT Service

You should be aware of the differences between the traditional NVC scanner (NVCNT.EXE) and the NVC NT

Service. The two modules have overlapping functionality for on-demand and scheduled scanning, as well as the possibility of defining different styles. Real-time scanning, however, is unique for the NT service. NVCNT.EXE offers more scanning options than the NT Service.

In this manual, the chapters on scanning options, on-demand, scheduled scans, and styles are based on the traditional NVC for Windows NT (NVCNT.EXE). These common sections are:

“Configuring the Scanner” on page 28, “Saving Your Configurations as Styles” on page 44, and “Scheduling Concepts” on page 51.

Unless otherwise stated, the corresponding functions in the NT Service work in the same way. The NT Service specific considerations are covered in the section “NVC NT Service” on page 64.

Installing NVC

Before Installing

Many anti-virus products are incompatible. Therefore, if you have a version of an anti-virus product other than Norman's installed, you should uninstall this before installing NVC.

Note: As Thunderbyte AntiVirus (TBAV) is now integrated into NVC, an uninstall procedure for TBAV is now available during the installation of NVC. Unless TBAV is found on your machine during installation, the dialog where you can choose uninstalling TBAV will not appear.

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** applications. From Program Manager you choose File|Run. If you are running Windows NT 4.0, choose Start|Run program. On the command line, type:

   ```
   a:setup
   ```

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

4. 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:
   - Norman Virus Control (NVC), which includes
     - Windows scanner
     - 32 bit command line scanner
     - scheduler
   - NVC NT Service, which includes
     - scanner
     - scheduler
     - real-time scanner
   - Help Files for NVC
   - Norman Internet Update (See number 6 below.)

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.

Note: "Modify Settings for the NVC NT Service" on page 7 lists a set of additional options for those who wish to trim the NVC NT Service to their particular environment. This is not necessary in most environments.

Currently installed components of Norman Virus Control will be updated.

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.
6. When you install Norman Internet Update (NIU) you will be presented with the option of adding it to the Startup group. If you choose Yes (default), NIU automatically checks for upgraded definition files on Norman servers 5 minutes after you have started the PC. See "Norman Internet Update" on page 114.

7. When the installation is completed, new icons are added to the program folder you specified.

Note: If you're running Windows NT version 3.51, there will be a separate icon for uninstalling NVC. This icon will not be created if you're running version 4.0.

8. Setup is now complete. From the final display you can browse the Read Me file and launch Norman Virus Control.

Modify Settings for the NVC NT Service

This section is for the experienced user with particular needs to integrate the NVC NT Service in their program environment. A regular install as described on the previous pages is sufficient in most cases.

The additional options are:

Parameter	**Description**
`nvcsrv -install`	Performs normal installation of the service (default).
`nvcsrv -remove`	Performs normal removal of the service and the real-time components from the registry. Note that this does not remove the files physically. If the real-time components was installed, a reboot is necessary to remove the components from memory.
`nvcsrv -reinstall`	Has the same effect as first removing and then installing the service.
`nvcsrv -deldrv`	Removes the old NVC 4.20 driver if present (`tbntdrv.sys`)

Parameter	Description
`nvcsrv -drivers`	Installs real-time components only. This allows to install the real-time components if the service is already installed but not the drivers.
`nvcsrv -install -silent`	No echo to screen during install.
`nvcsrv -install -nodrvchk`	Suppresses the checking of the presence of the NVC 4.20 driver.
`nvcsrv -install -nodrvs`	Installs the service but not the real-time components.

Detection

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. See “Updating NVC” on page 114 for information on how to get hold of updated files, or you can visit our web site **www.norman.no**.

The 32-bit scanner can detect and remove unknown macro viruses using heuristic methods. Unknown boot sector viruses and polymorphic viruses are also disclosed by means of this method. When the scanner detects an unknown Word 6/7 macro virus, the virus name will be reported as WM/GENERIC. If the 'Repair file if possible' option is ON, all macros in the document are removed. Through internal testing it has been established that the detection rate for unknown macro viruses is about 80%.

With NVCNT you can scan from the menu-driven Windows scanner, the Right-click scanner, or from the command prompt.

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

Specific differences include:

- The Windows scanner can display files and boot areas as hexadecimal values. The command line scanner cannot.
- The Windows scanner has extensive on-line help. The command line scanner does not.

- The Windows scanner can operate in the background. The command line scanner cannot.
- The Windows 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 scanner do not.

See also “Real-Time Scanning” on page 85.

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

Note: The NT Service also features the most important scanning options from within the service. You should therefore refer to this section for an explanation of the different options if you’re scanning your machine using the NT Service.

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

Command line parameter:	/[parameter]

In addition, all available command line parameters are presented in a chart in the section “Command Line Scanning” on page 56.

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.

Boot Sector Repair

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 backup diskette. A dialog box complete with on-line help will guide you through the process if a boot sector virus is detected.

Before You Start

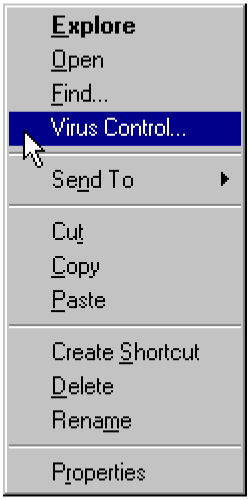
In order to start a scan:

1. Select the target to be scanned - drive(s), directory, or file.
2. Select the options to use during the scan.

The Scanning Process

The Right-click Scanner

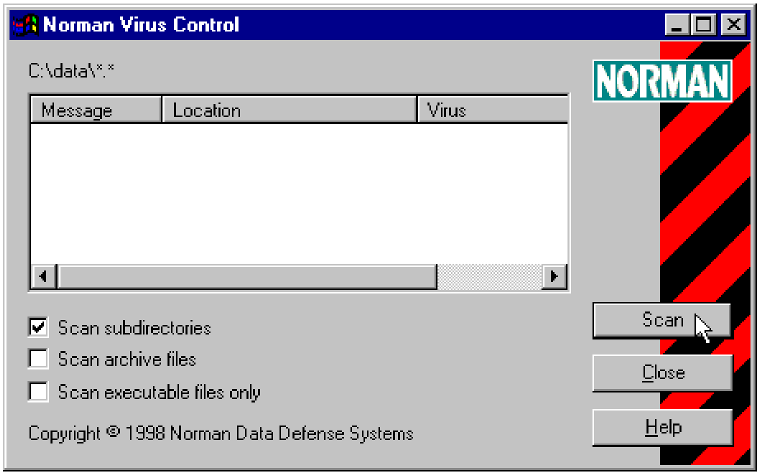
Note: The Right-click scanner is only available for Windows NT with Explorer shell (not Program Manager), version 4.



The purpose of the Right-click scanner is to make scanning easier and more available. You can use it to scan file system objects, like drives, directories, and files. Many users consider virus scanning a necessary evil. Making virus control easier to perform, we believe that the average user will be encouraged to scan more frequently. The Right-click scanner does not require double-clicking an icon or an executable file. Simply select the area you want to scan, for example from Explorer or My Computer, and choose *Virus Control* from the pop-up menu. The Right-click scanner employs the same scanning engine as the other NVC scanners, and therefore provides the same protection as any other Norman scanner.

Using the Right-click Scanner

1. Highlight the object you want to scan, for example a drive, directory, or file. To select more than one object, press the [Ctrl] key and highlight all objects you wish to include in the scan.
2. Click on your right mouse button.
3. Select *Virus Control* from the pop-up menu, and the following screen appears:



C:\data\*.*

Message	Location	Virus

☑ Scan subdirectories

☐ Scan archive files

☐ Scan executable files only

Copyright © 1998 Norman Data Defense Systems

Your options include:

[x] Scan subdirectories

If you have selected a drive or directory, check this option to include subdirectories in the scan.

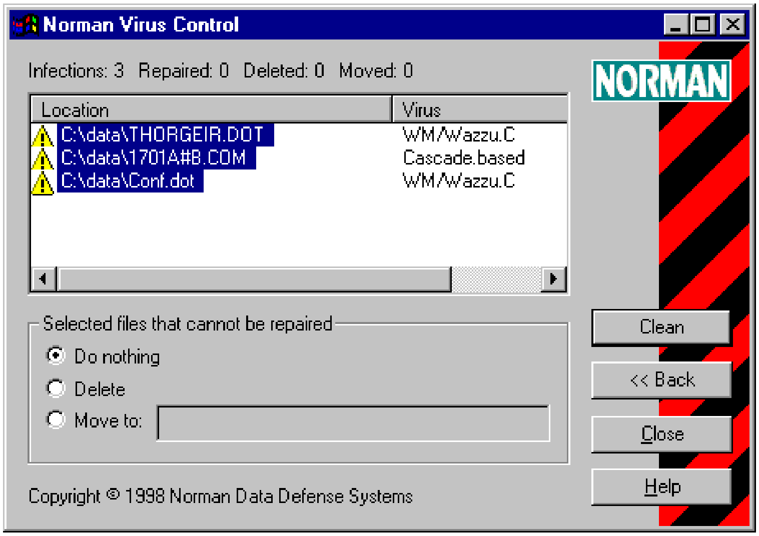
[ ] Scan archive files

Check this option to include archived files in the scan. In this version, only ZIP and ARJ files are supported.

[ ] Scan executable files only

Check this option if you only want to scan executable files.

4. Click on the **Scan** button when you've made your choices.
5. If no viruses are found, the message section of the scanning dialog will inform you about the number of files scanned, files that couldn't be scanned, etc.
6. If viruses are detected, you will see:



Infections: 3 Repaired: 0 Deleted: 0 Moved: 0

Location	Virus
C:\data\THORGEIR.DOT	WM/Wazzu.C
C:\data\1701A#B.COM	Cascade.based
C:\data\Conf.dot	WM/Wazzu.C

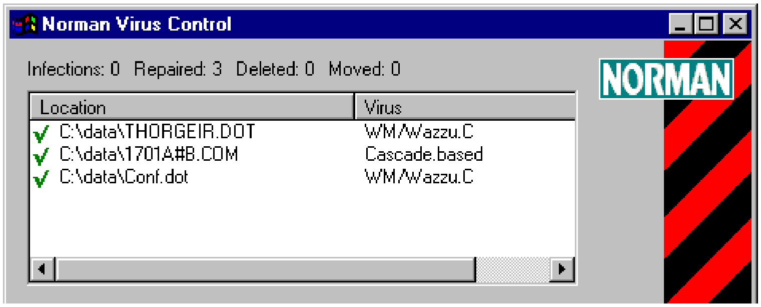
Selected files that cannot be repaired

● Do nothing
○ Delete
○ Move to:

Copyright © 1998 Norman Data Defense Systems

The infected files are highlighted, so you can click on the **Clean** button right away to remove the viruses. When a file has been cleaned, it will appear with a green checkmark in the list box. You will also find information on the number of files which are infected, repaired, deleted, or moved.

Note that the scanner will always try repair first. Then, if repair fails, it will perform your selection in the section "Selected files that cannot be repaired". Infected files that cannot be repaired, will therefore be treated in accordance with your choice among the options **[ ] Do nothing**, **[ ] Delete**, and **[ ] Move to**.



Infections: 0 Repaired: 3 Deleted: 0 Moved: 0

Location	Virus
✓ C:\data\THORGEIR.DOT	WM/Wazzu.C
✓ C:\data\1701A#B.COM	Cascade.based
✓ C:\data\Conf.dot	WM/Wazzu.C

Viruses cannot be removed in the following situations:

1. The file resides on a write-protected floppy 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).

Note: You can treat the files individually by highlighting certain files for cleaning, others for deletion, etc.

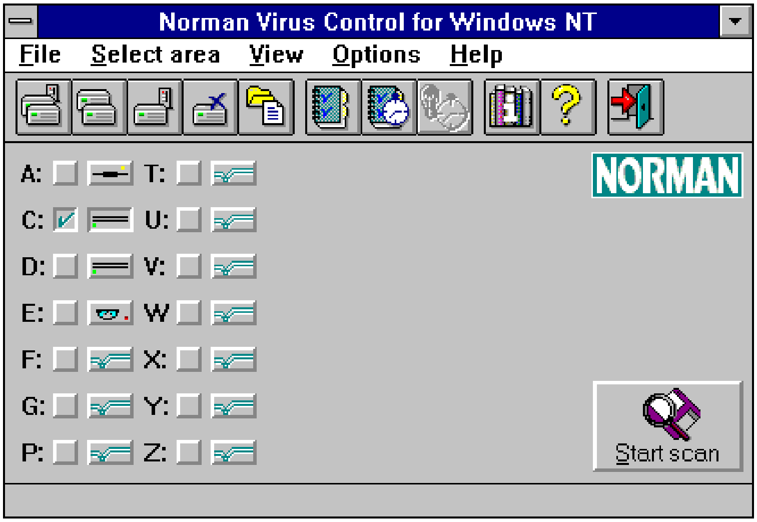
When the **Back** button is activated, you can go back to the scanning dialog to view statistics and possible messages.

Click on **Close** to exit the Right-click scanner.

The Windows Scanner

In this section, we give examples of how a normal scan appears. We used all the default options and asked the scanner to scan the entire C: drive.

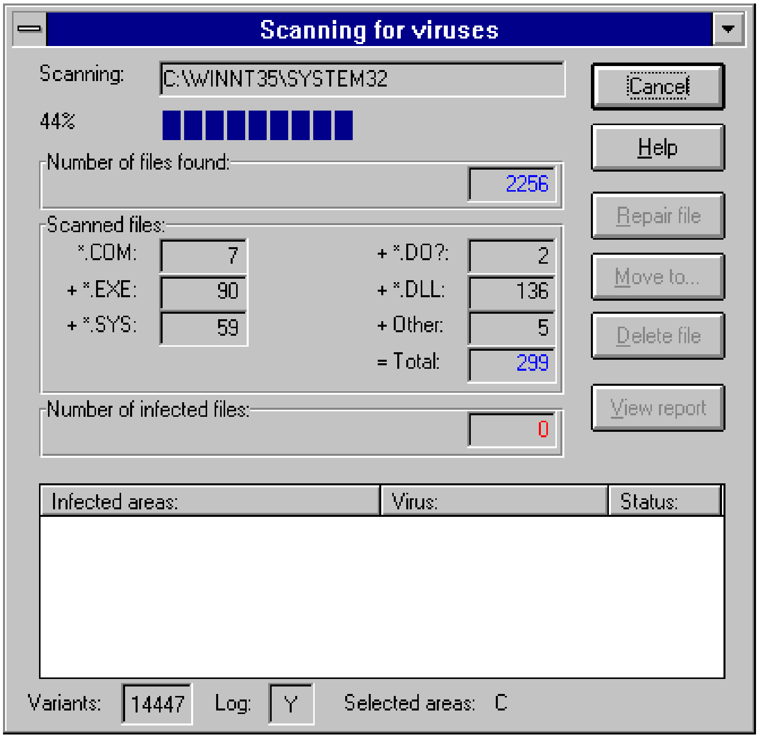
From the main window, check the C: drive and then click the **Start scan** button:



The scanner pops up a dialog box called "Scanning for viruses" which shows the progress as it scans files on the C: drive.

See the Read Me file for a discussion of default file extensions and "Configuration Concepts" on page 24 *for more information on configuring the scanner.*

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



Scanning for viruses

Scanning: C:\WINNT35\SYSTEM32

44%

Number of files found: 2256

Scanned files:

*.COM: 7
+ *.EXE: 90
+ *.SYS: 59
+ *.DO?: 2
+ *.DLL: 136
+ Other: 5
= Total: 299

Number of infected files: 0

Infected areas:	Virus:	Status:

Variants: 14447 Log: Y Selected areas: C

Files: the number of files found in the specified location so far in the process.

Scanned: the number of files that have been scanned so far in the process.

The number of files found in the specified directory will almost always be different than the number of files scanned because the scanner only scans files with certain (default) extensions in addition to the user-specified extensions you specify. Please refer to the Read Me file for more information on which extensions are scanned.

COM:, EXE:, SYS:, OV?:, DLL:, Others: how many files of these different extensions that have been found and scanned for viruses. The total of all these will be equal to the total number of files scanned.

Infected: the total number of infected files that the scanner has found so far in the process.

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

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

The list box at the lower part of the screen displays the path and filename of possibly infected files and/or boot areas along with the name of the virus that has infected these areas. In our example, no infections were found.

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, which summarizes three pieces of information:

Variants: shows the number of viruses and variants this version of the scanner is able to recognize. See “Finding Out More About Viruses” on page 99.

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

Selected areas: displays the areas that you have selected for the scan.

If you are using a style other than the <NORMAL> style for the scan, the name of the style will appear in the title bar of this screen.

Buttons

The following buttons are available in the "Scanning for viruses" display:

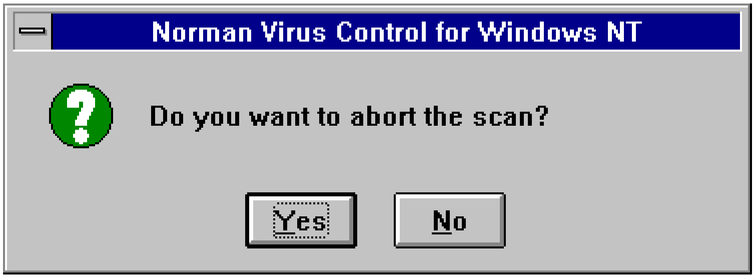
Help

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

Cancel/OK

This button will appear either as **Cancel** or **OK**, depending on the status of the scanning.

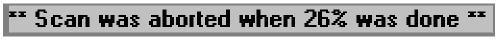
During scanning, the button will appear as **Cancel**. When you click on the **Cancel** button, you instruct the scanner to abort the scan, and the following dialog box will appear:



Norman Virus Control for Windows NT

Do you want to abort the scan?

If you answer **Yes**, the scanner will abort the scanning process, and the "Scanning" area will now appear as follows:



** Scan was aborted when 26% was done **

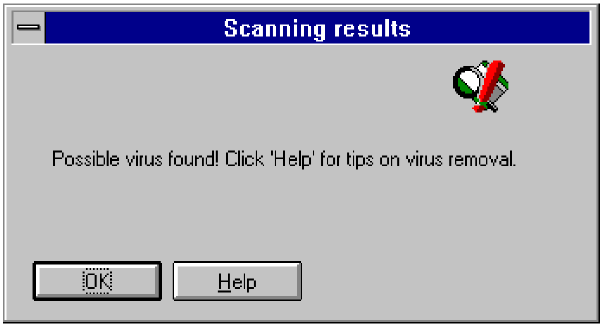
If you answer **No**, the scanner will continue scanning.

When you abort an ongoing scan or when the scan is completed, the button will appear as **OK**. Clicking on the **OK** button closes the dialog box and returns you to the main window.

You may also abort a scan by pressing the [Esc] key.

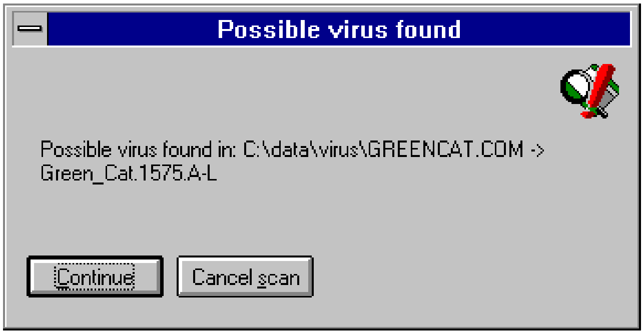
The remaining buttons are to be used after a scan is complete. But before we describe them, there are a few more dialog boxes to review...

If the scanner finds a virus, it pops up one of two dialog boxes:



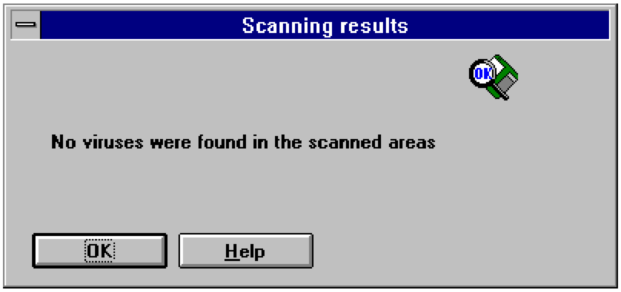
Possible virus found! Click 'Help' for tips on virus removal.

or



Possible virus found in: C:\data\virus\GREENCAT.COM -> Green_Cat.1575.A-L

And if the scanner does not find a virus, it pops up this dialog:



No viruses were found in the scanned areas

If the scanner finds an infected file, the following three buttons will be available on the "Scanning for viruses" dialog box when you highlight the infected file:

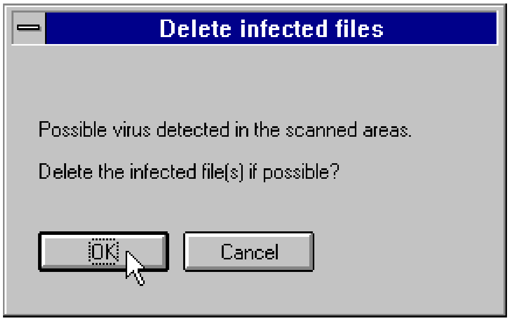
Repair file

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 and click on the Repair file button.

Note: NVC does not allow automatic repair of *boot sector viruses*. See "About Repair" on page 10 for more information.

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:



Delete infected files

Possible virus detected in the scanned areas.

Delete the infected file(s) if possible?

Click on **OK.**

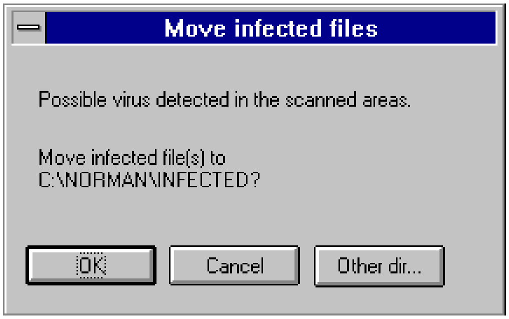
When you delete a file from the "Scanning for viruses" dialog box, the file is **not** overwritten before it is deleted.

Move to...:

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.



Move infected files

Possible virus detected in the scanned areas.

Move infected file(s) to
C:\NORMAN\INFECTED?

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.

Renaming Infected Files

The technique that the scanner uses increments the first eight characters of the file’s name only -- extensions are left untouched. First, if the name is less than eight characters, it is padded with "@" to achieve full length. Then characters are incremented until they reach "Z" -- starting with the last character, going forward.

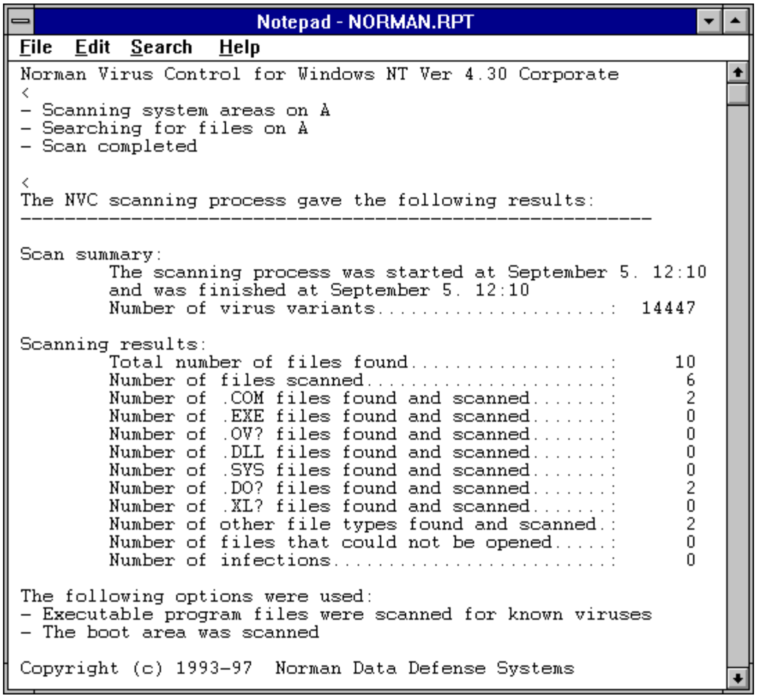
For example, say you have an infected file named `COMMAND.COM`, and the scanner moves it to the `C:\NORMAN\INFECTED` directory. Then the scanner finds another copy of `COMMAND.COM` that is infected and moves it to the `C:\NORMAN\INFECTED` directory. The second instance of `COMMAND.COM` now becomes `COMMAND@.COM`. The third instance would become `COMMANDA.COM`, the fourth would be `COMMANDB.COM` and so on until you reach `CZZZZZZZ.COM`. (But let’s hope that you don’t have this many.)

View report

If you have chosen either of the report options from the "Reporting" tabbed dialog box in the Scanning options dialog (see “Reporting” on page 82), you have the opportunity to view the report on the screen.

This button appears grayed until the job is done or if the report option is not selected.

After the scanner has created the report, you can click on the **View report** button, and Notepad will display the report.



```
Norman Virus Control for Windows NT Ver 4.30 Corporate
<
- Scanning system areas on A
- Searching for files on A
- Scan completed

<
The NVC scanning process gave the following results:
---------------------------------------------------------

Scan summary:
        The scanning process was started at September 5. 12:10
        and was finished at September 5. 12:10
        Number of virus variants.....................:  14447

Scanning results:
        Total number of files found..................:     10
        Number of files scanned......................:      6
        Number of .COM files found and scanned.......:      2
        Number of .EXE files found and scanned.......:      0
        Number of .OV? files found and scanned.......:      0
        Number of .DLL files found and scanned.......:      0
        Number of .SYS files found and scanned.......:      0
        Number of .DO? files found and scanned.......:      2
        Number of .XL? files found and scanned.......:      0
        Number of other file types found and scanned.:      2
        Number of files that could not be opened.....:      0
        Number of infections.........................:      0

The following options were used:
- Executable program files were scanned for known viruses
- The boot area was scanned

Copyright (c) 1993-97  Norman Data Defense Systems
```

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.

Configuration Concepts

To make the most out of the scanner, you should have a strong understanding of how it can be configured. Before you start a scan, you should set configurations from 3 functional areas:

- Where do you want to scan?
- How, specifically, do you want to do the scan?
- What do you want the scanner to do if it finds a virus?

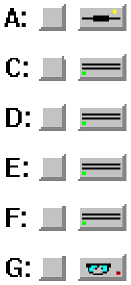
Each section below describes how to select where to scan, what to do during the scan, and what to do if a virus is found.

Choosing Where to Scan

The easiest choice to make is to determine where the scanner should scan. The scanner automatically detects all available physical and logical drives and displays them on the left side of the main window.

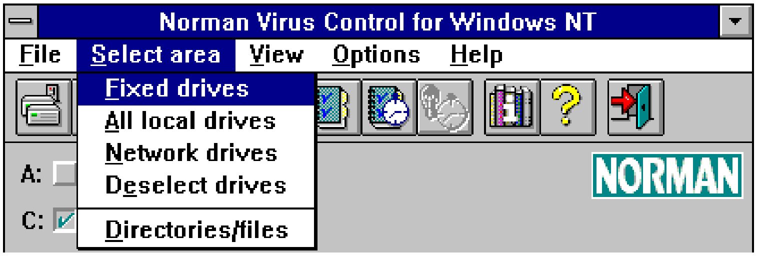
There are several methods for selecting a drive which is to be scanned. Either:

- click on its associated check box

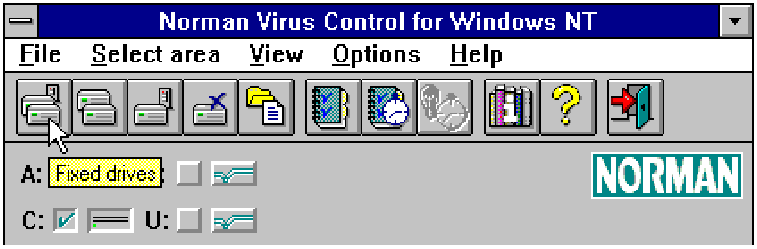


or

- click on Select area and then choose from the list



- or click on a toolbar button.

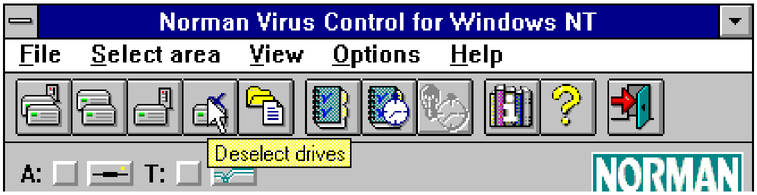


Your choices include:

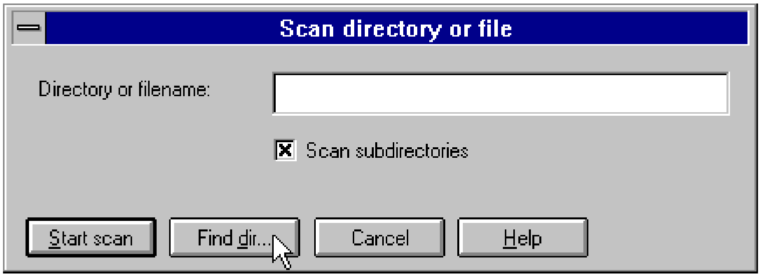
- Local and network hard drives
- Local hard drives
- Network hard drives
- Remove all selections and let you to choose any combination of drives to be specified for scanning.
- Select area|Directories/files (use this when you wish to only scan certain directories or files)

Note: When you select network drives, the boot areas of these drives are not scanned.

To **deselect** a drive, click on the drive's associated check box, and either click on Select area|Deselect drives or click on this toolbar button:



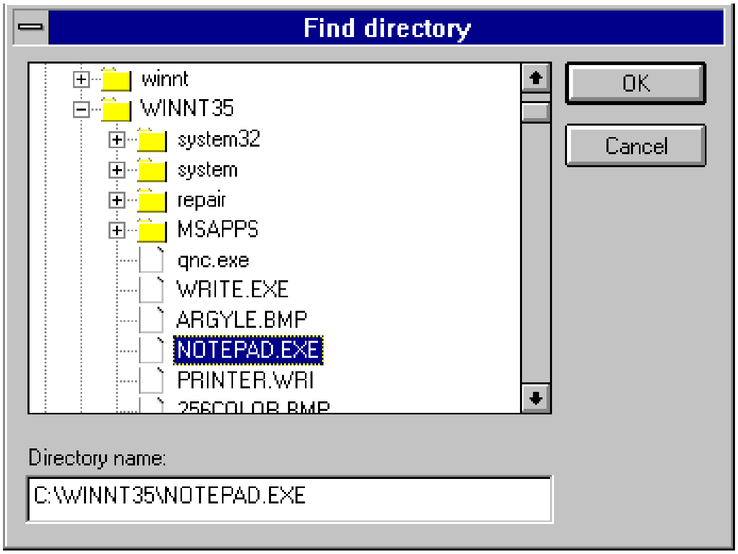
If you choose "Directories/files", then you can:



Directory or filename:

☒ Scan subdirectories

- type in the name of the directory or file that you wish to scan
- clear the [ ] **Scan subdirectories** checkbox if you do **not** wish to scan directories underneath the directory you specify. This option is turned on by default.
- find the file or directory to scan by clicking on the **Find dir** button:



Directory name:
C:\WINNT35\NOTEPAD.EXE

Click on the **OK** button when you have made your choices.

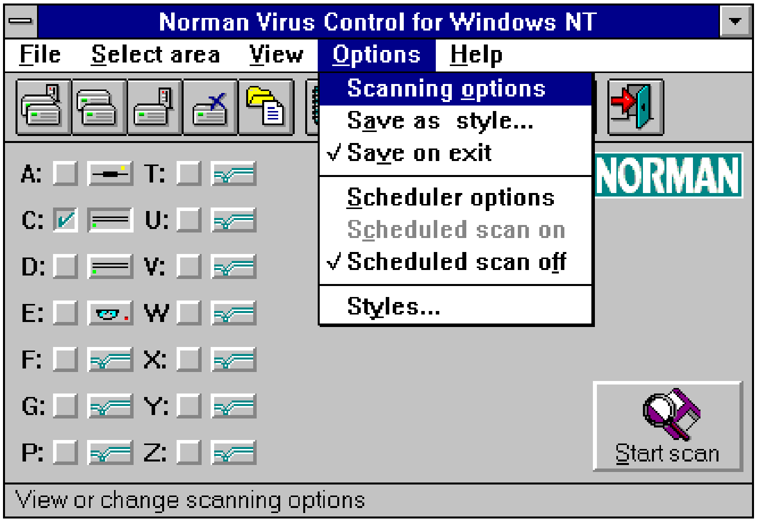
When you click on **Start scan** back in the “Scan directory or file” display, then the scan will start with the current configurations. These may not be the settings that you wished for this scan. Therefore, when you wish to use the "Directories/files" feature, be sure to set all configurations **before** you select "Directories/files"

Configuring the Scanner

Once you have chosen where you wish to scan, you should determine how you want the scan done.

You can configure the scan using one of two methods:

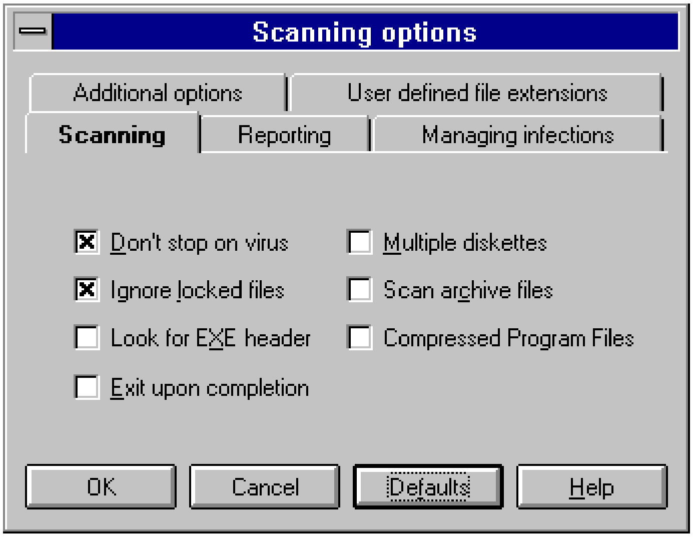
- click on Options|Scanning options to use the Scanning options dialog box:



View or change scanning options

Go to the section "Scanning Options" on page 30 for a more detailed discussion of this dialog box.

Configuring the Scanning Process



☒ Don't stop on virus

☒ Ignore locked files

☐ Look for EXE header

☐ Exit upon completion

☐ Multiple diskettes

☐ Scan archive files

☐ Compressed Program Files

These five dialog boxes contain tabs for configuration screens relating to:

- scanning
- reporting
- managing infections
- additional options
- user defined file extensions

The default settings are:

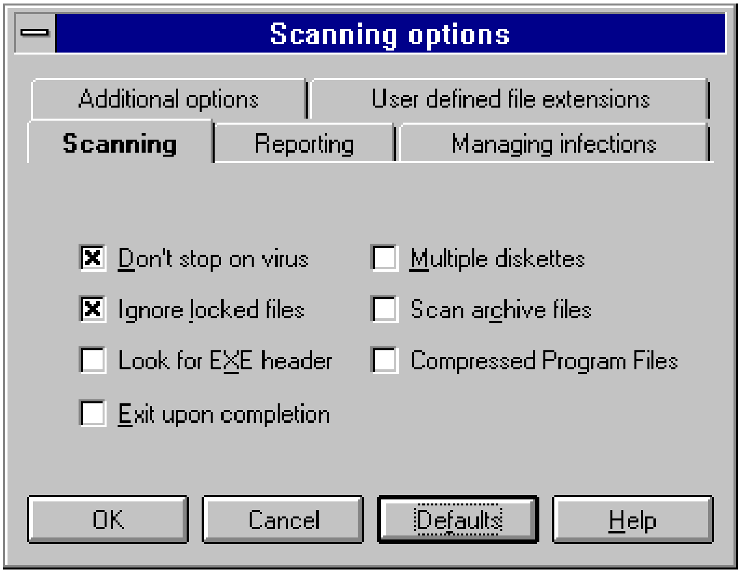
- Don't stop when a virus is found
- Ignore locked files
- Save results to a log file called NORMAN.RPT in the directory in which the scanner resides
- Overwrite previous report(s)
- Log infected files
- Take no action when a virus is found
- Beep when an infection is found

Scanning Options

In the following discussion on scanning options, all default settings are marked like this: **[x] Don't stop on virus**.

When a function has a corresponding command line parameter, it’s referred to like this:

Command line parameter: /[parameter]



☒ Don't stop on virus
☒ Ignore locked files
☐ Look for EXE header
☐ Exit upon completion
☐ Multiple diskettes
☐ Scan archive files
☐ Compressed Program Files

Available options include:

[x] Don't stop on virus

Click on this option when you do not want to sit and watch the scanner working. This is especially useful when scanning a network. Usually, when the scanner detects a virus, it asks for keyboard input, but in this mode, the scanner does not require keyboard input when a virus is found and proceeds until the scan is done.

Command line parameter: /U

[x] Ignore locked files

During normal use, the scanner will stop processing if it cannot open a file. You will see a dialog box showing you which file is locked. At this point, you may press **Cancel** in order to continue the scan but ignore all subsequent locked files.

To avoid error messages when locked files are found, turn this option on.

If you have logging turned on (either report to file or report to printer), then the log will contain the name(s) of the locked file(s).

Command line parameter:	/O

[x] Look for OLE2 header

Files generated in MS Word and Excel can be renamed and thus receive file types other than .doc and .xls, for example, which the scanner is always looking for. However, these files can be identified by their header, which will be OLE2. To detect camouflaged Word and Excel files, which are possible macro virus carriers, this option instructs the scanner to scan files that have OLE2 headers.

[ ] Multiple diskettes

If you have several **diskettes** that you want to check during one scanning session, check this option. You may click on **Cancel** any time you wish to stop.

Any reporting done when this option is checked will result in one report for all diskettes scanned instead of separate reports.

Command line parameter:	/R

[ ] Scan archive files

Archiving files is an efficient way to transfer files as well as freeing up space on your hard drive, a floppy disk, or a server. Since many viruses attach themselves to programs, it is possible to archive an infected file. We provide this option to temporarily uncompress an archived file and scan the files within.

Note: When a file is archived, the scanner can only tell you whether or not it is infected. It cannot take any action on the infected file while it is archived.

The scanner will scan .ZIP and .ARJ files **internally**. This task is performed by the scanner’s internal decompression system. The .ZIP and .ARJ files will therefore not be decompressed into “TMP” or “TEMP”.

If the archived files are other types than .ZIP and .ARJ, then the scanner automatically reverts to **external** decompression, assuming that you have the archive system necessary for decompressing the archive files you want to scan. It also assumes that these programs are available in your path. If they are not in your path, then the scanner cannot decompress the files.

When archived files are being scanned, the **Cancel** button in the ’Scanning for viruses’ display is unavailable.

Command line parameter: /C

[ ] Compressed program files

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

This option makes use of a decompressor emulator to open and scan the file in memory. Scanning compressed program files is more time-consuming than scanning archive files. This is a good reason for not choosing this option unless you have strong reason to believe that a compressed executable is infected.

Command line parameter: /CP

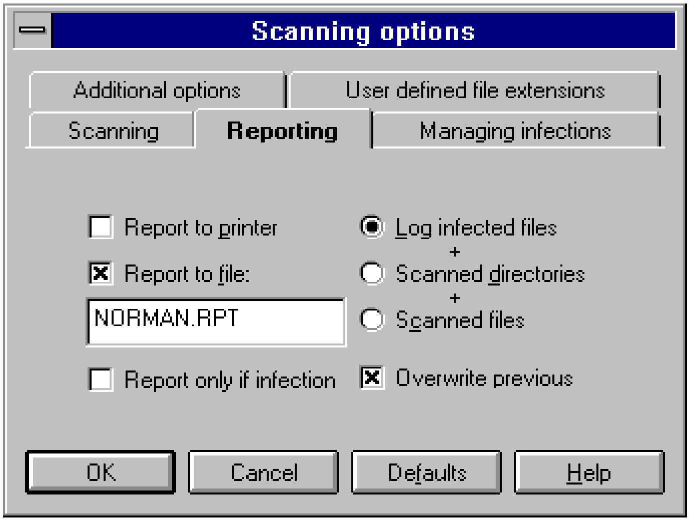
[ ] Exit upon completion

This is a handy when you wish to terminate the scanning session when the scan is complete.

For maximum efficiency, use this option along with the "Minimize while scanning" and "Report only if infection" options. With **all** these options turned on, the scanner will appear as a minimized icon while the scan progresses, a report will be generated only if a virus is found, Notepad will display the report (if it exists), and the scanner will exit when the scan is complete.

> *See the section "Additional Options" for more information.*

Reporting Options



☐ Report to printer

☒ Report to file:

NORMAN.RPT

☐ Report only if infection

● Log infected files
+
○ Scanned directories
+
○ Scanned files

☒ Overwrite previous

If you want the scanner to give you a status report after a scan, you must choose the [ ] **Report to printer** and/or [x] **Report to file** button(s).

[ ] **Report to printer**

The scanner will send its report to the default printer that is set up through NT.

[x] **Report to file**

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

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

[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 be appended to the previous report(s).

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

See also “Scheduling Several Unattended Scans” on page 55.

If reporting to a file is disabled, then the [ ] **Overwrite previous** option will be grayed.

[ ] Report only if infection

The report will only be generated if an infection is found. If this is turned on, then the only reporting level available is [ ] **Log infected files**. See the list below for more details on reporting levels.

Command line parameter: /LQ

You may choose among three reporting levels:

1. **[x] Log infected files**

   This level will only report the infected files that are found. The report is short and concise.

   This level is the default.

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**

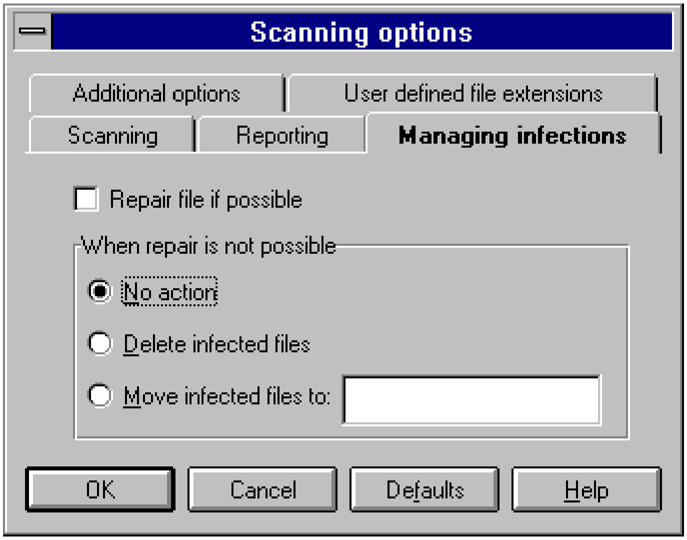
   This level generates a list of all scanned directories and files. Infected files will be specifically marked. Of course, if you scan many files, this report will be quite long.

The "plus" signs between these reporting levels means that when you choose higher levels of reporting, the characteristics of the lower level(s) will be included.

You will see that the reporting level choices on the right side of the dialog box are only available if reporting to file or printer is turned on.

Provided that you selected one of the reporting options, you may at any time view the last report that the scanner generated. Click on View|Report from the main window.

Managing Infections Options



□ Repair file if possible

When repair is not possible

● No action

○ Delete infected files

○ Move infected files to:

There are five options regarding what action the scanner should take when an infected file is found:

The options are:

[ ] Repair file if 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 viruses known to NVC.

The present version of the scanner *detects* and *removes* known viruses. The 32-bit scanner can also detect and remove unknown macro viruses using heuristic methods. When the scanner detects an unknown Word 6/7 macro virus, the virus name will be reported as WM/GENERIC. If the ’Repair file if possible’ option is ON, all macros in the document are removed.

Through internal testing it has been established that the detection rate for unknown macro viruses is about 80%.

Command line parameter: /CL

Viruses cannot be removed in the following situations:

1. The file resides on a write-protected floppy 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).

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

[x] No action (default)

If you wish to leave infected files alone at the time they are detected, then use this option and view the scanning report for details about possible infections.

[ ] Delete infected files

This option is for deleting infected files as they are discovered.

Command line parameter:	/D-

[ ] Move infected files to:

If you want to analyze possible viruses, you can choose this option and enter the path to the directory where you want to quarantine them. The scanner will create the directory if you specify a non-existent directory. Otherwise, the scanner will move infected files into the directory C:\NORMAN\INFECTED.

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.

In a network environment, the area that you specify for storing infected files should be off-limits to everyone but the Supervisor.

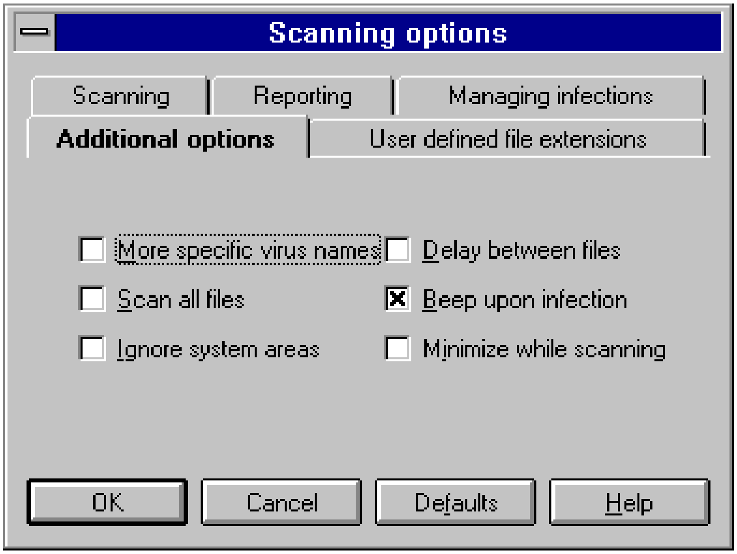
If you have more than one instance of an infected `COMMAND.COM`, for example, and you choose to move each copy into the same directory, then the scanner will rename each instance of the file as described in the section “Renaming Infected Files” on page 22.

Command line parameter:	/MOV

Note: Even if you choose not to repair, delete, or move infected files in this dialog, you can highlight infected files and handle them from the "Scanning for Viruses" display.

Additional Options

There are a handful of options that need not be used by everyone, and so we have placed them here:



□ More specific virus names
□ Scan all files
□ Ignore system areas
□ Delay between files
☒ Beep upon infection
□ Minimize while scanning

[ ] 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.

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 data files and executables. Normally, you do not have to scan files other than the defaults. However, when you use this option, the scanner will scan all files it finds on the specified drive(s).

This is a helpful feature if you suspect you have a virus and want to check all files.

Scanning time increases when you use this option.

Command line parameter: /AF

[ ] Ignore system areas

By default, the scanner scans the system areas (see below for definition) of a floppy disk or a local hard drive. However, in NT, a scan of the system area of the hard drive is normally only allowed by NT when the scan is initiated by a user with administrator permission on the system.

Note: However, any user can scan system areas on **diskettes**.

In cases where system areas have been severely corrupted, scanning them may cause the scanner to fail with an error. This option instructs the scanner to skip these areas and simply scan files.

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

Master Boot Sector (MBS)

The MBS is located on all physical hard drives.

The MBS 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 floppy disks and physical hard drives that are formatted, and it is created with `FORMAT.COM`.

The SBS 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 floppy disk with an operating system on it.

Command line parameter: /BS-

[ ] Look for EXE header

More and more often, we encounter viruses that keep track of all activities in individual files. Many 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 option instructs the scanner to scan 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

[ ] Delay between files

If you instruct the scanner to scan many files, you can use this option to minimize the I/O (read/write from/to disk) load by pausing about half a second between each scanned file.

Command line parameter: /W:

[x] Beep upon infection

By default, the scanner beeps each time it detects an infected file or boot area. Clicking on this check box toggles between turning the beep on and off.

Command line parameter:	/B turns the beep off

[ ] Minimize while scanning

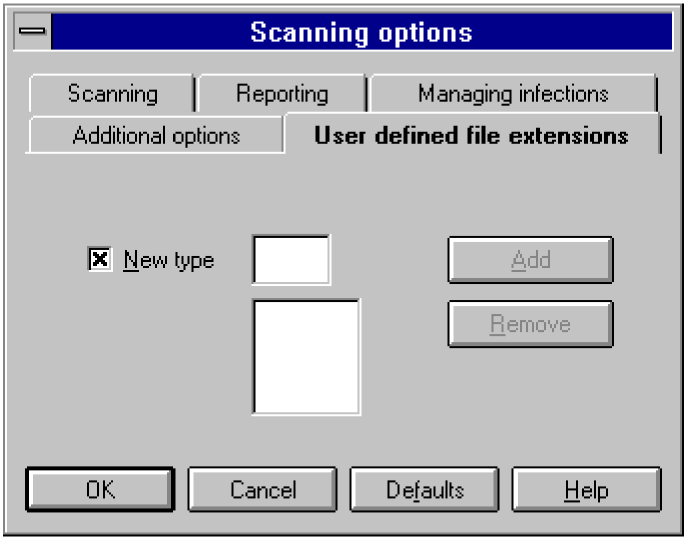
If you wish to have the scanner minimized while it performs a scan, then click on this option. When the scan starts, the scanner will appear as an icon in the lower left corner of your screen.

If the scanner is minimized and you wish to view the results, then you may double click on the icon, and you will see the "Scanning for viruses" dialog box.

User Defined File Extensions

By default, the scanner will scan files with certain extensions. These are file types that we know are exposed to viruses. The scanner checks files with these default extensions in addition to the user-specified extensions you specify. Please refer to the Read Me file for more information on which extensions are scanned.

If you wish to add files with other extensions for scanning, you may use the dialog box shown below to instruct the scanner to look for up to 20 additional extensions.



☒ New type

To add a new user defined file extension:

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

   All file extensions are limited to 3 characters.
3. Click on the **Add** button.

The scanner will save these new extensions in the Registry as a part of the current style.

If you would like to have these extensions included in all of your scans, specify them as a setting within the <NORMAL> style.

If you would like these extensions to be used during only some of your scans, specify them as a setting within a style other than <NORMAL>.

For more information about styles, see “Saving Your Configurations as Styles” on page 44.

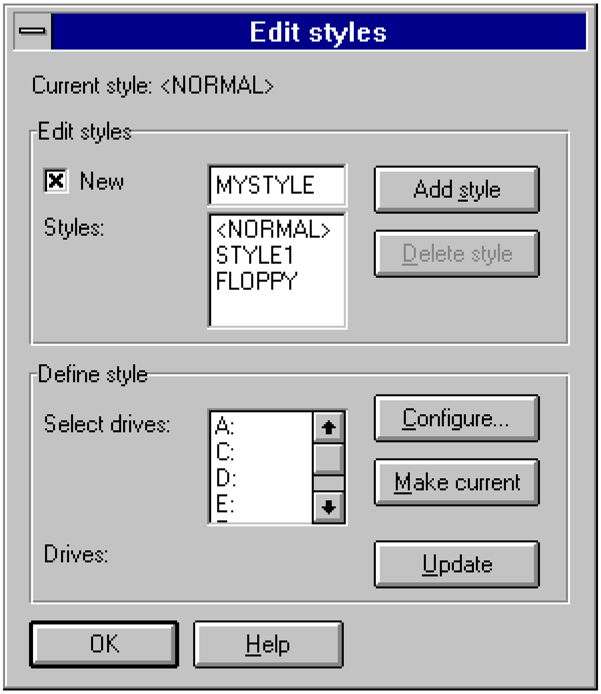
To remove a user defined file extension, click once on the extension you wish to delete and then click on the **Remove** button.

Saving Your Configurations as Styles

You can save yourself time by saving your configurations as styles. For example, if your goal is to run scans in certain combinations (scan floppies and delete infected files; scan local drives and move infected files to a specific location, for example), then you can simply configure both types of scans as different styles and have the scanner use the appropriate style at the appropriate time.

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.

To access the styles function, click on Options|Styles. You will then see a dialog box titled "Edit styles".



Edit styles

Current style: <NORMAL>

Edit styles

☒ New: MYSTYLE

Styles: <NORMAL> STYLE1 FLOPPY

Define style

Select drives: A:, C:, D:, E:

Drives:

The scanner is shipped with one style called the <NORMAL> style. The <NORMAL> style will always be available. You can customize it in any way you wish as well as create up to 20 additional styles, but you cannot delete the <NORMAL> style.

Add a Style

1. Click on the check box marked [ ] **New**.
   A new style is always based on the factory default settings.
2. Give the new style a name.
   Do this by entering the new name in the text box located to the right of the control box. The name can be up to 8 characters long.
3. Click your mouse on the **Add style** button.
   Your style's name is added in the list box “Styles” and is now available as an alternative to the <NORMAL> style.
4. Highlight the new style by clicking it once. Select drive(s) from the “Select drives” list box by highlighting the drive letter(s).
5. Click the **Configure** button.
6. Enter your choices in the tabbed dialog “Scanning options”. When you click on **OK**, a pop up dialog box will inform you that the style has changed.
7. Click on **Update**.
8. If you wish to make this new style current now, then click on the **Make current** button.

When you make a style current, the scanner will be configured with the options that are associated with that style until you choose different options for that style or until you make another style current.

Delete a Style

1. Choose the style you wish to delete from the "Edit styles" dialog by clicking it once.
2. Click on the **Delete style** button. Before the style is deleted, you will be asked to confirm the deletion of the specific style.
3. To complete the operation, click on the **Update** button.

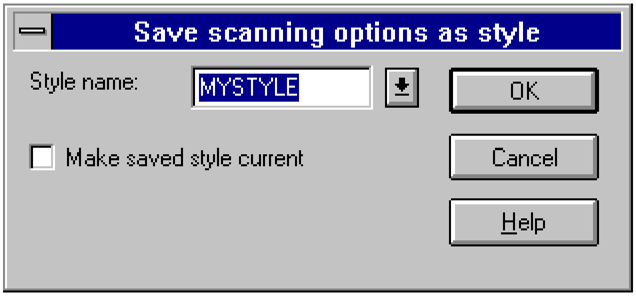
You cannot delete a style if it is current. You must first make another style current, select the desired style name from the list box, and then click on **Delete style**.

If a style is specified for a scheduled scan, you'll receive an error message if you try to delete it.

Save as Style

There will always be a current style. Unless you have specified otherwise, <NORMAL> is current.

When you are working with the scanning options, you are therefore editing the current style. If you want to keep the current style as it is **and** the present changes, you should choose Options|Save as style and save your changes from this dialog box:



Style name: MYSTYLE

□ Make saved style current

See the next section, "Save on Exit", for more information about saving scanning options in styles.

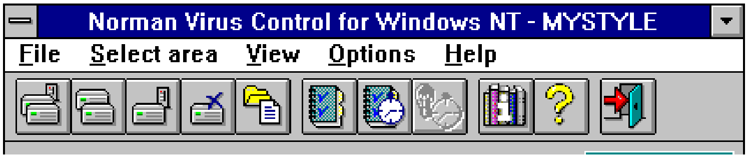
Save on Exit

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 the scanner.

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

Unless you specify otherwise, the <NORMAL> style is the default style. Any configuration changes that you make while the <NORMAL> style is current will become part of the <NORMAL> style, regardless of whether or not you make the configuration changes from the "Edit styles" dialog box.

When a style other than the <NORMAL> style is current, the name of the style will appear in the title bar of the main window, in the title bar of the "Scanning for viruses" dialog box, and right under the title bar in the “Edit styles” dialog box.



Modify the <NORMAL> Style

You cannot change the <NORMAL> style from the “Edit styles” dialog box. To change this style:

1. Make sure that <NORMAL> is the current style.
2. Make sure that Options|Save on exit is on. This is the default setting.
3. Configure your scanning options from the Options|Scanning options tabbed dialog boxes.
4. Click on OK when you’ve made your choices.
5. You have now changed the <NORMAL> style permanently.

   Remember that all new styles are based on the original

<NORMAL> style.

When no other style is specified, the <NORMAL> style will be used. You may specify styles for both on-demand scans and scheduled scans. See “Scheduling Concepts” on page 51 for more information on scheduled scanning.

Specifying Files or Directories As Styles

You can identify drives for scanning by specifying the target areas with scanning options from the “Edit styles” dialog. You cannot specify individual files or directories in the same manner.

You can, however, use the DOS command `subst` to solve this problem.

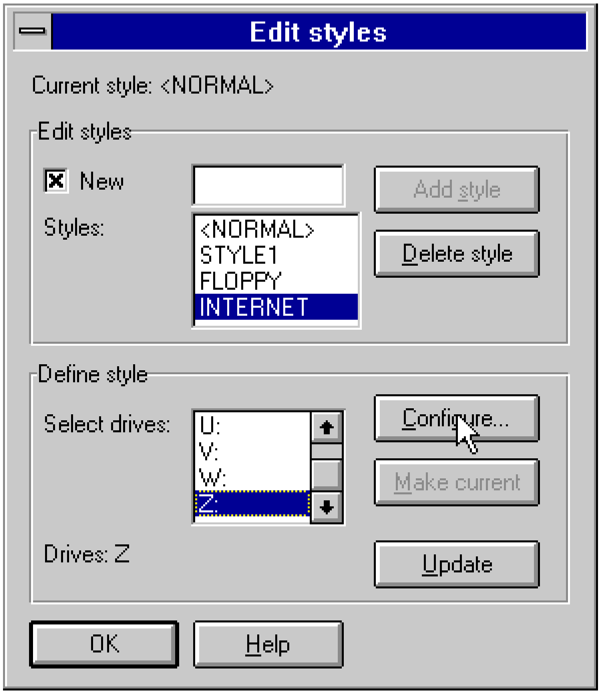
Task: to scan directory `c:\data\internet` only.

1. From the command prompt, type:

```
subst z: c:\data\internet
```

where `z:` is a virtual drive. If a ‘z:’ drive exists on your system, you must select another drive letter.

2. Select Options|Styles and add the new style INTERNET:



Current style: <NORMAL>

Edit styles

☒ New

Styles:
<NORMAL>
STYLE1
FLOPPY
INTERNET

Define style

Select drives:
U:
V:
W:
Z:

Drives: Z

Note that the virtual drive `z:` now appears in the Select drives list box.

3. Highlight the new style.
4. Select the `z:` drive from the box.
5. Click on **Configure** to determine the scanning options.

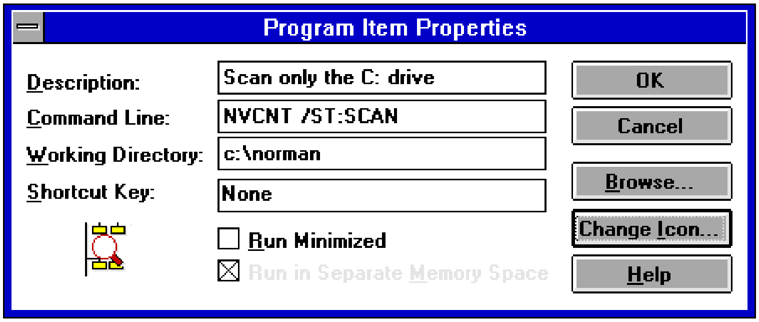
You have now created a style for scanning a specific directory. Like all styles, it is eligible for scheduled scans.

Note: You must run the `subst` command again to create the virtual drive if you have turned off or rebooted your PC.

See also the following section for an alternative way of scanning a specific directory.

Activating Styles From the Command Line

It is possible to create different icons on the NT desktop for different scanning purposes. For example, you might want to have one icon for scanning network drives on demand and another one for scanning particular directories during your lunch hour. To do this, simply create a new Program Item, select the desired icon, and specify the style you wish to use as follows:



Program Item Properties

Description: Scan only the C: drive
Command Line: NVCNT /ST:SCAN
Working Directory: c:\norman
Shortcut Key: None

☐ Run Minimized
☒ Run in Separate Memory Space

In this example, we are loading the SCAN style and asking NVCNT to start scanning immediately after we click on this icon.

The syntax for this feature is as follows:

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

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

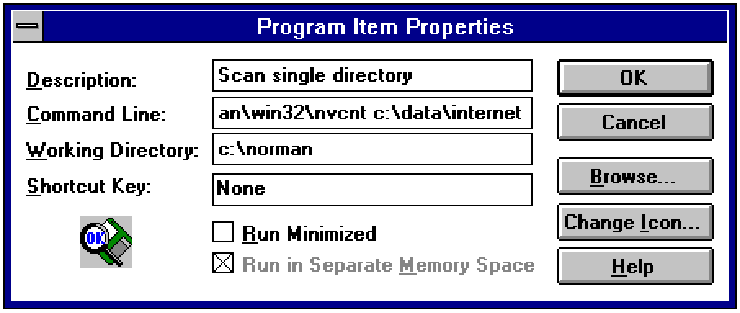
If you run the style SCAN as shown above and add other parameters, like:

```
nvcnt /st:scan a: d:
```

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

When this feature is used, users will not be able to change the configurations within the styles before or after the scan begins. If you wish to change the configuration of a style, do not use these parameters. Rather, load NVCNT as you would normally by clicking on its icon. Then follow the instructions in “Configuring the Scanner” on page 28.

You can specify a directory for scanning and put it on the desktop. This is an example:



Description: Scan single directory

Command Line: an\win32\nvcnt c:\data\internet

Working Directory: c:\norman

Shortcut Key: None

□ Run Minimized

☒ Run in Separate Memory Space

On the command line, you enter:

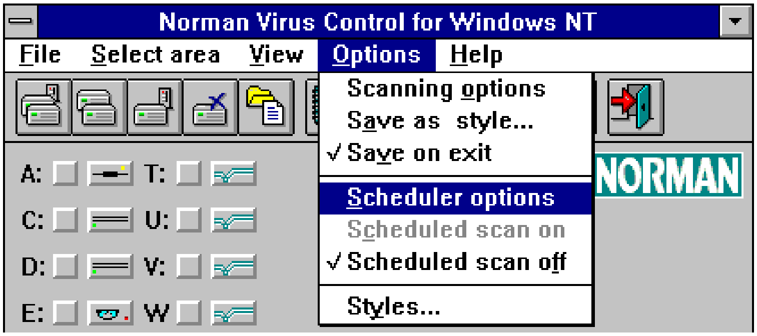
```
c:\norman\win32\nvcnt c:\data\internet
```

Note: Before you doubleclick this icon, make sure that the scanner is not active and that you made the desired style for this scan current before you exited the scanner.

Scheduling Concepts

Not only does the scanner perform on-demand scans, it can also scan at scheduled times. You may configure scheduled scans from several different locations:

- click on the pocketwatch icon on the toolbar
- click on Options|Scheduler options



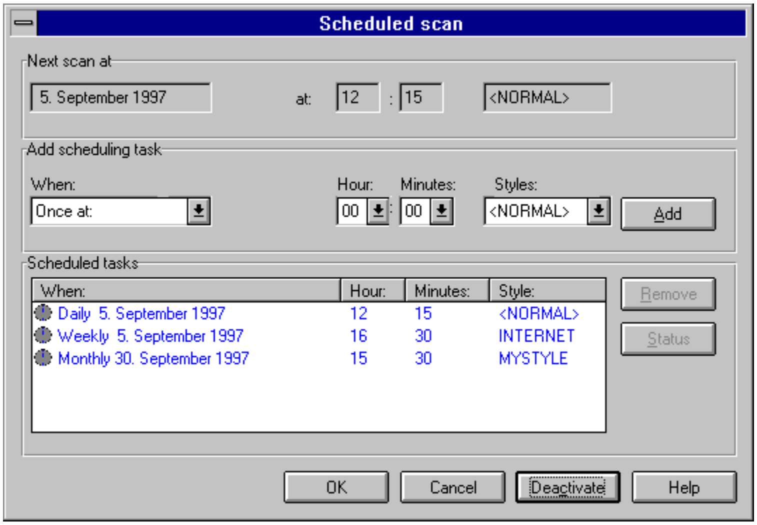
Whether you access the Scheduler from the icon or from the "Options" menu, you can set the following:

- the time a virus scan will begin
- how often the process is to be run
- what type of style to use

You can schedule multiple scans, ranging from once, hourly, daily, weekly or monthly.

Note: If you schedule a combination of hourly, daily, weekly, and monthly scans, make sure that such repetitive scans are set to begin at different intervals within the hour. For example, if you schedule hourly scans to start at (hour):00, ensure that daily scans are scheduled for (hour):15 etc. If two or more scans are scheduled at the same minute interval, only one scan will be performed.

The dialog box from which you configure the scheduled scan looks like this:



Scheduled scan

Next scan at

5. September 1997 at: 12 : 15 <NORMAL>

Add scheduling task

When: Once at:

Hour: 00

Minutes: 00

Styles: <NORMAL>

Scheduled tasks

When:	Hour:	Minutes:	Style:
Daily 5. September 1997	12	15	<NORMAL>
Weekly 5. September 1997	16	30	INTERNET
Monthly 30. September 1997	15	30	MYSTYLE

Schedule a Scan

To schedule a scan, first set the frequency of the scheduled scan from the “Add scheduling task” section of the display. Click the [ ] **When** combo box and choose from:

- **Once**
- **Hourly**
- **Daily**
- **Weekly**
- **Monthly**

When you select **Once**, **Hourly**, or **Daily**, today’s date is automatically selected.

If you select **Weekly**, then you may choose the day of the week on which the scan should occur.

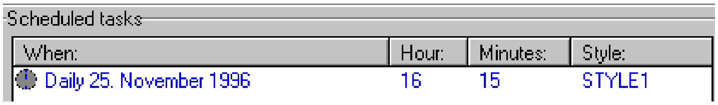
If you click on **Monthly**, the combo box changes to list the numbers 1 through 31. If you choose "5", for instance, then the scheduled scan will occur on the 5th of each month at the time you have specified. If you choose "31", and there are only 30 days in a particular month, then the Scheduler will begin the scan on the 1st of the following month.

Then:

1. Click on the [ ] **Hour** combo and select the hour you wish. Hours are listed in 24 hour format.
2. Click on the [ ] **Minutes** combo and select the minutes you wish. Minutes are given in 15 minute increments.
3. Click on the [ ] **Styles** combo and select the style you wish to use for this particular scheduled scan.
4. Click on the **Add** button, and the scheduled scan appears in "Scheduled tasks" list box.

   Once you have set 20 daily scans, the **Add** *button becomes inaccessible.*

5. When you add a scheduled scan, it pops up in the "Scheduled tasks" list box and activates the scheduler.
6. You cannot change a scan after it's been scheduled. You must highlight the scheduled task by clicking it once, then click the **Remove** button and enter a new scan.
7. The first scheduled scan to be run appears at the top of the list in the "Scheduled tasks" list box, as well as at the top of the display in the list box "Next scan at:".
8. The "Scheduled tasks" list box provides information on future scans. The watch to the left of the scheduled scan tells you that a scan is scheduled:



Scheduled tasks

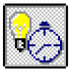
When:	Hour:	Minutes:	Style:
Daily 25. November 1996	16	15	STYLE1

9. Click on the OK button when you have entered all your scheduled scans.

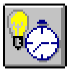
Make sure that the scheduler is active. The scheduled scan is on by default. You can turn the scheduler on and off from the Options menu or from the scheduler status button on the toolbar.

Note: In order for a scheduled scan to occur, scheduled scanning must be ON and the scanner must be active.

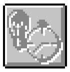
When scheduled scan is **on**, the toolbar button is depressed and looks like this:



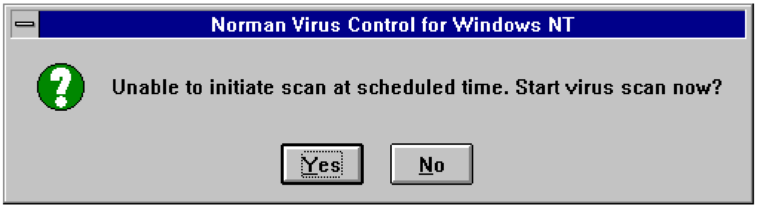
When scheduled scan is **off**, the toolbar button looks like this:



If no scans are scheduled, the toolbar button is all grayed out:



If a scan failed to run at the scheduled time, you'll see this message the next time you access the scheduler:



Norman Virus Control for Windows NT

Unable to initiate scan at scheduled time. Start virus scan now?

Scheduling Several Unattended Scans

Like on-demand scans, scheduled scans require user action when the scan is complete. A scan will either inform you that no infected areas were found, or that a possible infection is detected. In either case, you need to take some action to remove the messages.

However, if a message not responded to is blocking an upcoming scheduled scan, NVC will remove the message some 30 seconds before the scheduled scan is due to run.

There are nevertheless a couple of options you must be aware of when you’re scheduling more than one scan to run unattended at night, for example:

1. Do **not** check the [ ] **Exit upon completion** option in the tabbed dialog “Scanning options”. If you do, the scanner will close and consequently not run the remaining scheduled tasks.
2. You **must** check the [ ] **Ignore locked files** option in the tabbed dialog “Scanning options”. If you don’t, the scan will be blocked by messages about locked files that could not be opened. In Windows NT, this will always be the case with PAGEFILE.SYS.
3. Make sure that you specify different names for the reports for the various styles. Alternatively, uncheck the [ ] **Overwrite previous** option in the Options|Scanning options tabbed dialog Reporting. If you use default option, you’ll only get the report from the last scan.

Command Line Scanning

The scanner also provides the possibility for scanning from the command line. When the scanner is activated this way, it will perform the scanning according to the parameters and is terminated when the scan is done.

However, like the rest of the NVC products, NVC for Windows NT is provided with a separate command line scanner. The command line scanners are not dependent on any other modules. They can send virus alert information to FireBreak through IPX communications, SNMP traps (except for the Windows 3.1x version), 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:

```
nvc32 [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

```
nvc32 /?
```

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 floppies or CD-ROM).
`/AD`	Scan all disks (not floppies). 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 continuously 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.
`/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, except for boot sector viruses.

Param.:	Function:
`/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 specified 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.*
`/MOV`	Move infected files to default INFECTED directory (`c:\norman\infected`).

Param.:	Function:
/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 `nvc32.exe` is installed, type:

```
nvc32 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:

```
nvc32 *.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.

NVC NT Service

Please refer to the sections “About NT Services” on page 1 and “Virus Protection for Windows NT” on page 2 for background information on the NVC NT Service.

NVC NT Service v4.70 features the following functions:

1. On-demand scanning

   You can start the scan, and if you log off, the scanning will not be aborted.

   Due to the nature of the NT Service, non-local drives (like network drives, for example) are not visible to the Service. Please refer to “Configuring the Scanning Process” on page 29 for details on scanning.

2. Scheduled scanning

   You can setup several scheduled scans, which will be executed in the background. Virus alerts from scheduled scans are always logged in the NT Application Event Log, to the report file (if specified), and in pop-up dialogs (if selected).

   Please refer to “Schedule a Scan” on page 53 for details on scheduled scanning.

3. Real-time scanning

   Real-time scanning involves constant monitoring of the file systems. Whenever a file is accessed in a read/write operation or a program is executed, the NT Service is notified and scans the file on the fly.

   In real-time scanning, the application is communicating with the operating system at a low level, enabling the application to “see” all activities on the system. A real-time virus control program is therefore allowed to check for viruses whenever files are accessed. See “Configure Real-Time Scanning” on page 86 for more information.

Modules in the NVC NT Service

The NVC NT Service is currently made up of the following modules:

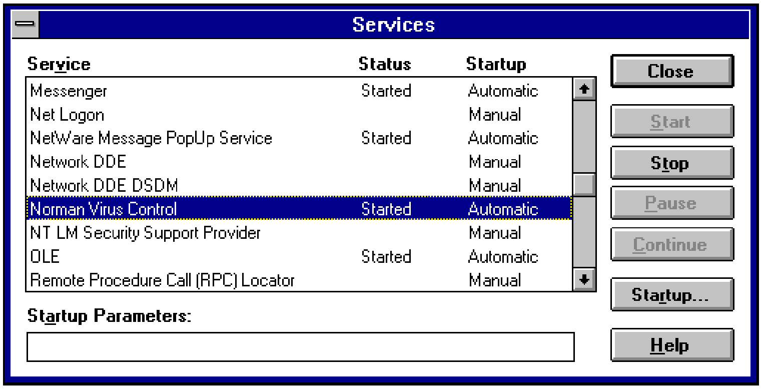
1. NVC NT Service —
   the center of all scanning service-related activities.
2. Command line configuration module —
   if you prefer to work from the command line.
3. GUI-based configuration module —
   the traditional Windows NT interface.
4. Popup message service for notification when a virus is detected.

Note that some options available in the GUI version are not available from the command line. Please refer to “Scanning Options not Available from the Command Line” on page 72 for more details about the differences.

The NVC NT Service Module

To configure the NVC NT Service you must have Administrator’s privileges.

A common place to administer all kinds of NT Services is via the Services applet in the NT Control Panel. When the NVC NT Service has been installed, it will appear like this in the Services applet:



Services

Service	Status	Startup
Messenger	Started	Automatic
Net Logon		Manual
NetWare Message PopUp Service	Started	Automatic
Network DDE		Manual
Network DDE DSDM		Manual
Norman Virus Control	Started	Automatic
NT LM Security Support Provider		Manual
OLE	Started	Automatic
Remote Procedure Call (RPC) Locator		Manual

Startup Parameters:

Basic administrative actions like starting and stopping the NVC NT Service can be done here. The NVC NT Service is started automatically when the system boots.

A service that has been started will survive a logoff. This means that the service will be running even if nobody is logged into the console.

To make it easy to see that the NVCNT service is running, the NVCNT service will identify itself via an icon on the notification area on NT 4 machines. This is done by the nvcpop-up program on behalf of the NVCNT service. On NT 3.51 machines, this feature is not available.

In earlier versions you had to enter the services applet in the control panel, or (if you had administrators rights) enter the ncfgw or ncfg applications to get this information.

Double-clicking the icon will display NVCPOPUP. Tooltip text for the icon is "NVC Service loaded".

Note: You can also start the NVC NT Service from the command prompt in the home directory, which home directory is `c:\norman\win32` by default:

```
ncfg -start
```

The NVC NT Service module is the center for a number of activities:

Controlling On-Demand and Scheduled Scans

The NVC NT Service will feed the scanning engine with filenames and system areas to be scanned. Scanning can be either on-demand or scheduled.

The scheduling function in the NVC NT Service is identical to the corresponding function in NVC v4.70 for Windows NT. However, `NVCNT.EXE` is not required for the service to function properly.

Each scheduled scan is associated with a style, and you can schedule up to 10 different tasks. You cannot transfer a previously defined style from `NVCNT.EXE` to the NVC NT Service or vice versa.

To schedule a scan from the command line:

```
ncfg -at:13:00 -check:c,d:,e:
```

The the specified drives will be scanned daily starting at 13:00 with the settings in the current style. These settings are stored in the automatically created style AT1300. Changing the drive information will not affect the style. This scheduled task is visible from Scheduled scans in NCFGW.

To remove this scheduled scan from the command line:

```
ncfg -remat:13:00
```

The scheduled scan AND the style AT1300 are removed. Note that only styles generated during command line scheduling will be removed. Styles generated from within the GUI are not affected.

See also “Scheduled Scans” on page 93 for more information.

Interface to the NT Registry

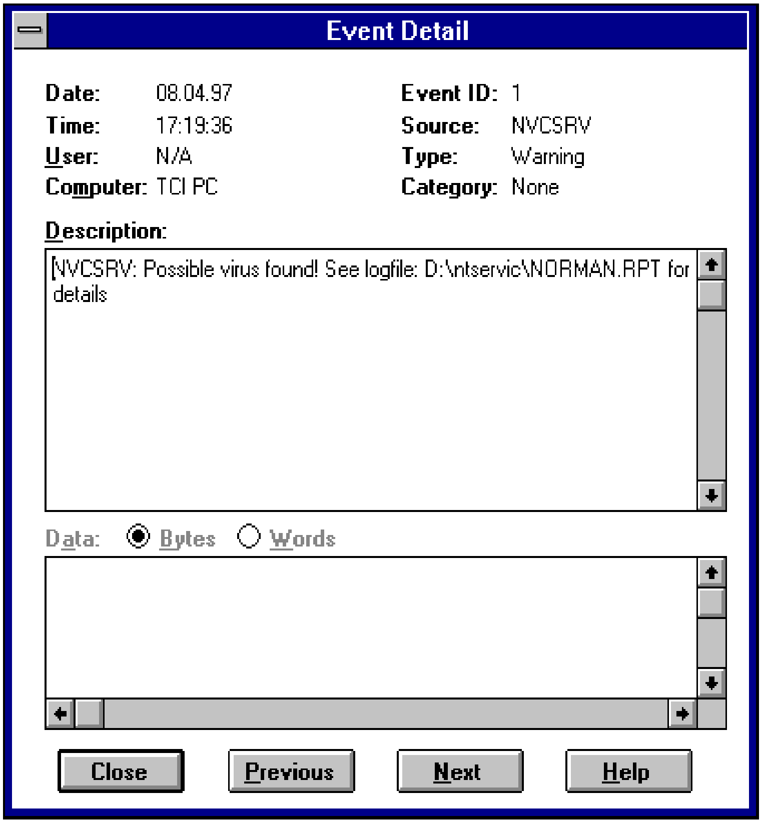
The NVC NT Service module is responsible for various kinds of communication with the NT Registry. When the administrator changes the configuration via the NVC configuration programs (NCFGW and NCFG), the NVC NT Service will update the Registry on behalf of the configuration program. The current configuration data is stored within the NVC NT Service structures.

Neither configuration program will ever manipulate the Registry directly. Instead, the NVC NT Service updates the Registry through the configuration program with the current configuration.

Interface to the NT Event Log

The NT Application Event Log offers a standardized way of presenting various kinds of messages to an Administrator. The NVC NT Service will store alert messages in the Event Log whenever viruses are found. This function is configurable from the real-time scanning options. Please refer to “Configure Real-Time Scanning” on page 86 for more details.

If a virus is found, you will see this message in the Event Viewer:



Event Detail

Date: 08.04.97 Event ID: 1
Time: 17:19:36 Source: NVCSRV
User: N/A Type: Warning
Computer: TCI PC Category: None

Description:

NVCSRV: Possible virus found! See logfile: D:\ntservic\NORMAN.RPT for details

Data: ● Bytes ○ Words

Produce Standard NVC Report File

When you run on-demand or scheduled scans, the NVC NT Service will produce a report file consistent with the standards used in the NVC version 4.x modules.

Please refer to the *Administrator's Guide* for more details about the report file structure, and to “Reporting” on page 89.

Configuration Module – Command Line Version

The command line configuration program provides an easy and flexible way of configuring the NVC NT Service. From the command prompt, it is possible to perform various tasks by using the following syntax:

```
ncfg <-parameter> [<-parameter>]
```

The following command starts the NVC NT Service:

```
ncfg -start
```

You only have to start the NVC NT Service using this command *the first time* you start the service after it's been installed.

These parameters are currently available The first five parameters must be executed *prior to starting* the NVC NT service:

Parameter:	**Explanation:**
-delayrtstart:x	Delay startup of the drivers, where 'x' denotes number of minutes.
-rtdisable	Disable real-time components when the service starts.
-rtenable	Re-enable real-time components when the service starts.
-manualstart	Change startup mode to manual.
-autostart	Reset startup mode to automatic.
-abort	Abort an ongoing scan.
-arc	Scan inside .ZIP and .ARJ archive files.
-at:<hour>:<min>[,...]	Scan drive(s) at scheduled time(s). Only daily scans can be specified.
-check:<drive>:[<drive>...]	Start scanning drive(s).
-defaults	Reset all options to defaults.
-hipri	Run scanning thread at high priority.

Parameter:	**Explanation:**
-log:<filename>	Override default log filename (NORMAN.RPT). Must be an existing filename.
-logdirs	Include scanned directories in log.
-logfiles	Include scanned files in log.
-machine:<name>	Send commands to any machine in the network.
-mov:<directory>	Move all infected files to <directory>. Must be an existing directory.
-nolog	Do not produce log file while scanning.
-query	Query NVC NT Service status.
-remat:<hour>:<min>	Remove a scheduled scan.
-rtonreadonly	Real-time components scan on read operations only.
-rtonwriteonly	Real-time components scan on write operations only.
-rtscanon	Start the real-time scanner.
-rtscanoff	Stop the real-time scanner.
-start	Start the NVC NT Service.
-stop	Stop the NVC NT Service.
-ver	Display NVC NT Service version information.

:Default Options

Scanning: Files with certain extensions will always be scanned. Please refer to the readme file for a complete list.

Reporting: Report to file `c:\norman\win32\norman.rpt` (if you chose the default option during installation), log infected files only and append report to any previous instance of the file.

Managing infections: No action when a virus is found.

Examples:

To start a virus scan on drives c:, d: and e:, type in the following command:

```
NCFG -check:c:,d:,e:
```

Note that the scanning options in the current style will be used. Use the `-query` parameter to check which style is current.

To start virus scan at 02:30, type in the following command:

```
NCFG -at:02:30
```

Note: Command line parameters will always override corresponding settings in a style, including drive selection.

Please refer to “Save as Style” on page 46 for more information on styles.

Scanning Options not Available from the Command Line

The command line version is designed to handle basic tasks related to virus control and does therefore not contain some of the more sophisticated functions available from the GUI-based version. This includes most of the options found in the four tabbed dialog boxes in the GUI-based version’s menu option Options|Scanning options. See “Scanning Options - On-Demand And Scheduled Scanning” on page 77.

However, if options are defined in a style from the GUI configuration program, they will be executed when that particular style is applied in a scan from the command line version.

Distribution with N_DIST

A major advantage of the command line configuration program is to use it with N_DIST, the Norman distribution program. Combining these two programs makes it possible for an administrator to configure a large number of NVC NT Service installations from one single point.

Since an NT Service requires Administrator’s privileges to install and configure, the NVC NT Service, when distributed via N_DIST, will skip all workstations with restricted user access. You should therefore make sure that you log in as an Administrator on the workstations where you want to install the NVC NT Service.

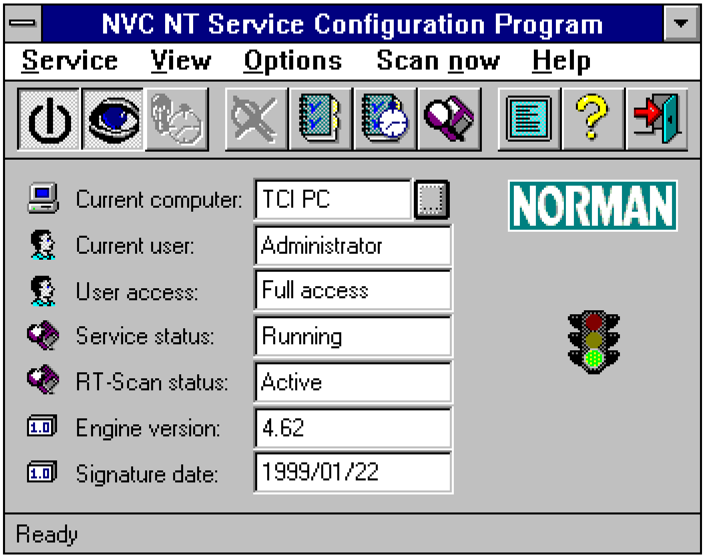
The N_DIST script created during an Administrator’s install, will include the copy functions for the various modules of the service.

Please refer to the *Administrator’s Guide* for more information about N_DIST.

Configuration Module - GUI Version

The preferred way of configuring the NVC NT Service is probably from NCFGW.EXE, the GUI based configuration program. You need Administrator’s privileges to configure the service.

This is the main window:



Current computer: TCI PC

Current user: Administrator

User access: Full access

Service status: Running

RT-Scan status: Active

Engine version: 4.62

Signature date: 1999/01/22

Ready

Main Window Information

The boxes in the main window display useful information:

Current computer

The name of the computer currently selected. Click on the browse button to the right of the computer name. The Select computer dialog appears. You can administer several instances of NVC NT Service on different machines from one machine. From any workstation in the network, you can administer a Windows NT server.

Current user / User access

The type of access this user has to the resources within the NVC NT Service. User access is either “Full access” for the Administrator or “RESTRICTED!” for the non-Administrator. When “RESTRICTED!” is displayed, the fields Service status and RT-Scan service will display status "Unknown". The traffic light will not appear.

Without full rights on the system, the front-end configuration program is not allowed make any inquiry to the service (for security reasons).

Service status

The possible status of the NVC NT Service is:

- Unknown
- Not installed
- Installed
- Starting
- Running
- Scanned xx%
- Stopping
- Stopped
- Pausing
- Paused
- Continuing

RT-Scan service

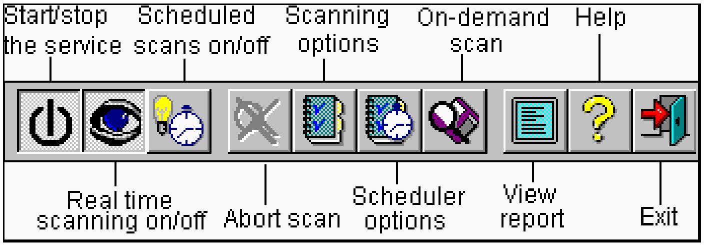
The possible status of the real-time scanning is:

- Active
- Passive
- Empty
- Incompatible
- Not installed

Engine version / Signature date

Which NVC version you are running, and the date of the current virus definition files (`nvcbin.def` and `nvcmacro.def`). The date format is yyyy/mm/dd.

The Button Bar



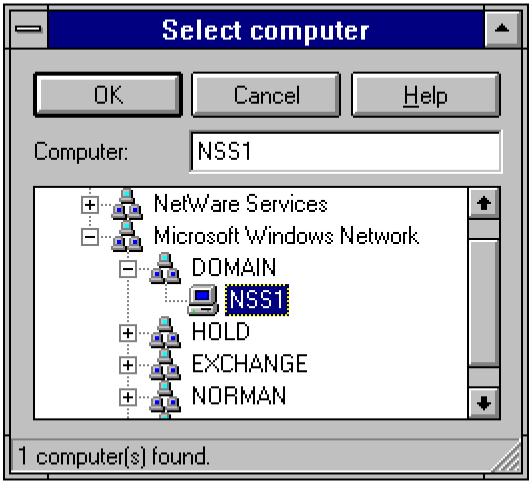
These options are also available from the pull-down menus.

From the menu or the toolbar buttons, it is possible to change to different administrative screens:

- Configure scanning options, including styles
- Configure scheduled scans
- Configure real time scanning
- Select areas for on-demand scanning
- Various pieces of status information (report file, scanning history, configuration)

Select Computer

Before you start configuring the scanner, make sure that you are logged in on the desired server. In the main window you can see the name of the currently selected computer. To change computer, click on the browse button to the right of the Current computer field, or choose the menu option Service|Select computer. The following dialog appears:



Computer: NSS1

1 computer(s) found.

Ncfgw will always display the local computer first. Click on **OK** or choose another computer from the Explorer-like interface in the lower part of the display.

When you have selected a computer and clicked on **OK**, you will see the main window with the information described above.

Note: When you have selected a remote computer all configuration settings, available drive letters, etc. apply to the specified computer. You are in fact working "locally" on the remote computer. Networked drives are therefore not visible.

Scanning Options - On-Demand And Scheduled Scanning

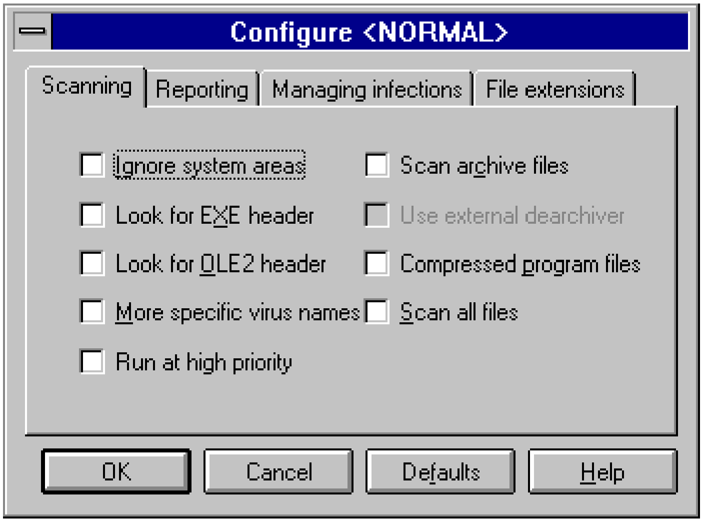
See “Configuring the Scanner” on page 28 for configuration hints.

Note: These scanning options only work with on-demand and scheduled scans. See “Configure Real-Time Scanning” on page 86 for real-time scanner options.

When you choose Options|Scanning options from the main window, you’ll see a dialog prompting you to choose between real-time and on-demand scanning options. This has been done to ensure that real-time scanning is not confused with on-demand scanning and vice versa.

You can choose from a number of different scanning options. Use these options for optimizing the scanning process. Click on **OK** when you have made your choices in all the tabbed dialog boxes. The settings are stored in the current style.

Click on **Defaults** to reset the options to factory settings. You can access the scanning options from the toolbar or from Options|Scanning options:



□ Ignore system areas
□ Look for EXE header
□ Look for OLE2 header
□ More specific virus names
□ Run at high priority
□ Scan archive files
□ Use external dearchiver
□ Compressed program files
□ Scan all files

[ ] Ignore system areas

By default, the scanner scans the system areas of a floppy disk or a local hard drive. However, in NT, a scan of the system area of the hard drive is normally only allowed by NT when the scan is initiated by a user with administrator permission on the system.

Note: However, any user can scan system areas on **diskettes**.

In cases where system areas have been severely corrupted, scanning them may cause the scanner to fail with an error. This option instructs the scanner to skip these areas and simply scan files.

[ ] 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 option instructs the scanner to scan 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.

[ ] Look for OLE2 header

Files generated in MS Word and Excel can be renamed and thus receive file types other than .doc and .xls, for example, which the scanner is always looking for. However, these files can be identified by their header, which will be OLE2. To detect camouflaged Word and Excel files, which are possible macro virus carriers, this option instructs the scanner to scan files that have OLE2 headers.

Note: If you check this option, the scanner will look for OLE2 header in **all** files and therefore increase scanning time considerably.

[ ] 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.

[ ] Run at high priority

The operating system will grant the scanner more system resources — sometimes at the expense of other tasks. Not recommended for ordinary scans.

[ ] Scan archive files / [ ] Use external dearchiver

It is possible to archive an infected file. We provide this option to temporarily decompress an archived file and scan the files within.

Scanning archive files involves unarchiving the file to a subdirectory of the temporary directory and then performing the scan. The subdirectory will be named with the first 8 characters of the archive file, and its extension will be .NVC. If you turn off the machine or if you run out of disk space during the scanning of an archive file, the subdirectory will not be deleted as it normally would, even though it may be empty. Next time you scan this particular archive file, it will not be scanned because a subdirectory exists with an identical name. Therefore, if an NVC subdirectory exists, you must delete it manually.

Note: When a file is archived, the scanner can only tell you whether or not it is infected. It cannot take any action on the infected file while it is archived.

The scanner will by default scan .ZIP and .ARJ files **internally**. This task is performed by the scanner’s internal decompression system. The .ZIP and .ARJ files will therefore not be decompressed into the “TMP” or “TEMP” directory.

If the archived files are other types than .ZIP and .ARJ, then the scanner automatically reverts to **external** decompression, assuming that you have the archive system necessary for decompressing the archive files you want to scan. It also assumes that these programs are available in your path. If they are not in your path, then the scanner cannot decompress the files.

If you check both these options, the scanner will **only** decompress using external decompression.

[ ] Compressed program files

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

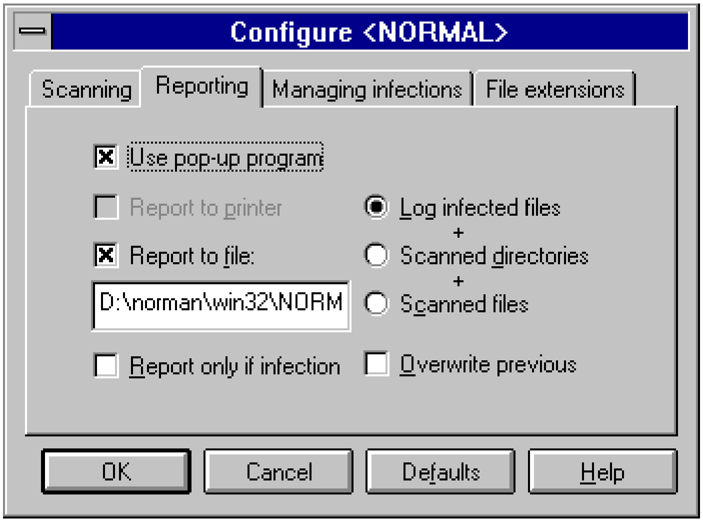
This option makes use of a decompressor emulator to open and scan the file in memory. Scanning compressed program files is more time-consuming than scanning archive files. This is a good reason for not choosing this option unless you have strong reason to believe that a compressed executable is infected.

[ ] 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 data files and executables. Normally, you do not have to scan files other than the defaults. However, when you use this option, the scanner will scan all files it finds on the specified drive(s). This is a helpful feature if you suspect you have a virus and want to check all files.

Scanning time increases when you use this option.

Reporting



☒ Use pop-up program

□ Report to printer

☒ Report to file:

D:\norman\win32\NORM

□ Report only if infection

● Log infected files
+
○ Scanned directories
+
○ Scanned files

□ Overwrite previous

When you are performing scans running in the background or at scheduled times, you probably want to know what happened during the scanning process.

The report option offers the opportunity to see if viruses were found, and if so provide the name and location of the virus. You can also see how many files and which file types were included.

From the tabbed dialog "Reporting" under the menu option Options|Scanning options you can define:

- use pop-up program (to display virus warnings)
- report to printer
- report to file (and enter the path and report name)

- report only if infected
- log infected files/directories/scanned files
- overwrite the previous report

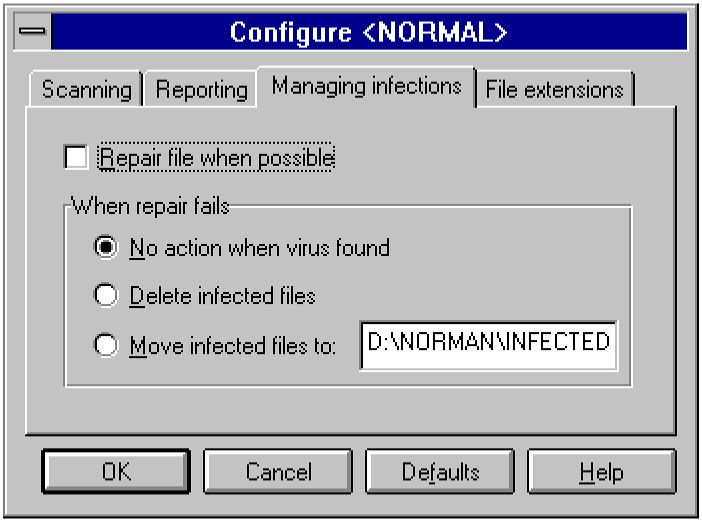
You can, of course, setup different reporting options for the different styles. We recommend that you assign different report names for the various styles in order to make it easier to tell one from the other. For example, specify a report name identical to the style name.

Regardless of what you choose for a report name, the scanning report includes the name of the style used in a scan.

Make sure that you don't check the [ ] **Overwrite previous** option if you use the default directory and report name (`c:\norman\win32\norman.rpt`). If you do, only the latest report will be available.

Managing Infections

Use the tabbed dialog Managing infections (Options|Scanning options) to decide how the NT Service should handle virus infections:



□ Repair file when possible

When repair fails

● No action when virus found

○ Delete infected files

○ Move infected files to: D:\NORMAN\INFECTED

The options are:

[ ] Repair file 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.

Viruses cannot be removed in the following situations:

1. The file resides on a write-protected floppy 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).
4. It’s a boot virus. To remove boot viruses, you must run the Windows or command line scanner against the infected area.

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

---

[x] No action (default)

If you wish to leave infected files alone at the time they are detected, then use this option and view the scanning report for details about possible infections.

[ ] Delete infected files

This option is for deleting infected files as they are discovered.

[ ] Move infected files

If you want to analyze possible viruses, you can choose this option and enter the path to the directory where you want to quarantine them. The service will create the directory if you specify a non-existent directory.

File Extensions

By default, the scanner will scan files with certain extensions. These are file types that we know are exposed to viruses. The scanner checks files with these default extensions in addition to the user-specified extensions you specify.

See the readme text file for more information on default file extensions.

If you wish to add files with other extensions for scanning, you may use the dialog box to instruct the scanner to look for up to 20 additional extensions. Note that you cannot change the default file extensions for the real-time scanner.

To add a new user-defined file extension:

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

   All file extensions are limited to 3 characters.
3. Click on the **Add** button.

The scanner will save these new extensions in the Registry as a part of the current style.

If you would like these extensions to be used during only some of your scans, specify them as a setting within a style other than <NORMAL>.

To remove a user-defined file extension, click once on the extension you wish to delete and then click on the **Remove** button.

Real-Time Scanning

While on-demand and scheduled scans are performed upon specific user request, real-time scanning is activated whenever a file is *accessed*. Therefore it is important to be aware of what the real-time scanner is doing. The following sections cover configuration of the real-time scanner, and what happens when a virus is found.

The real-time scanner is ON by default and activated with the default options. The toolbar button appears depressed and in color. If you remove the all options for real-time scanning without turning it OFF, the button will still be depressed and grayed out and the RT-Scan status field will be “Empty”. You can turn real-time scanning off in three different ways:

1. From the main window, click on the real-time scan on/off button:
2. From the main window, chose the menu option Service|Stop real time scanner.
3. From the command line: `ncfg -rtscanoff`

We recommend that you run real-time scanning at all times to ensure constant monitoring of all system activity.

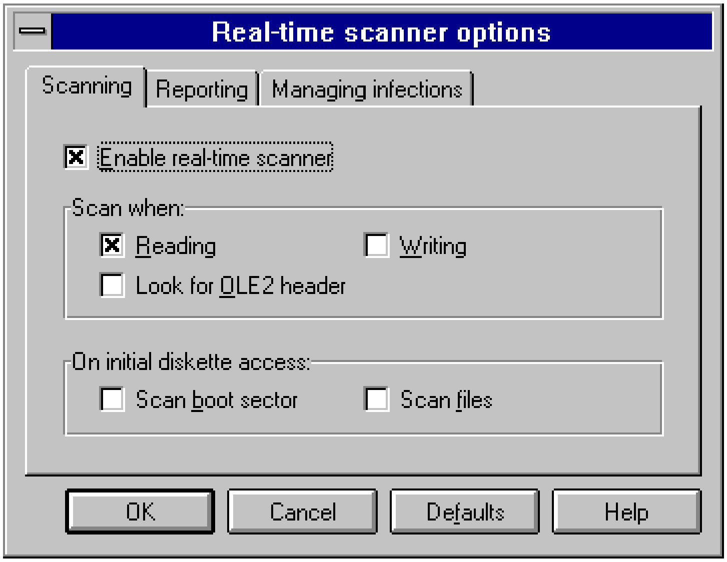
When the real-time scanner is active, you will see a little green light in the information area on your desktop (lower right corner). This feature is only available for NT version 4 or later.

Configure Real-Time Scanning

You can configure the real-time scanner from Options|Scanning options. This dialog is made up of three tabbed dialog boxes:

- Scanning
- Reporting
- Managing infections

Scanning



☒ Enable real-time scanner

Scan when:

☒ Reading ☐ Writing

☐ Look for OLE2 header

On initial diskette access:

☐ Scan boot sector ☐ Scan files

[x] Enable real-time scanner

Check this option to ensure that real-time scanning always is active.

Scan when:

[x] Reading / [x] Writing:

Note: The default settings are different for workstations and servers: [x] **Writing** for servers and [x] **Reading** for workstations. This is done to avoid that a high I/O activity affects your system performance. If you check both options, they will be reset to their original value after a reboot.

Scanning files on read/write operations involves checking a file on *access.* The following are examples of situations when files are being accessed:

- Copy or move files from one drive to another. In this case it’s a read operation on the source drive and a write operation on the target drive.
- Copy or move files between directories on the same drive.
- Start a program. In this case, files are accessed in a read operation.
- Copy or move file to or from a floppy. This is a read and write operation.
- Save files to a server drive. This is a write operation.
- Open document.
- Save document.

To complicate matters, there are different tools available for copy, move, and rename of files. The technical implementation of the individual tools decides if a move file command, for example, involves *accessing* the file.

Note that a file is *not* accessed during renaming or moving within the same drive.

Write/read operations on a HPFS file system will not be recognized by the real-time scanner.

[x] Look for OLE2 header

Files generated in MS Word and Excel can be renamed and thus receive file types other than .doc and .xls, for example, which the scanner is always looking for. However, these files can be identified by their header, which will be OLE2. To detect camouflaged Word and Excel files, which are possible macro virus carriers, this option instructs the scanner to scan files that have OLE2 headers.

On initial diskette access:

Note: A new diskette will *not* be checked before you *access* the diskette drive by clicking on the drive letter from Explorer/File Manager, or by entering the command `dir a:`. Subsequent accesses on the SAME diskette will not be notified an thus not checked. To check the same diskette again you must either do an on-demand scan on the diskette or remove it, insert another one which is accessed, and then re-insert the original diskette.

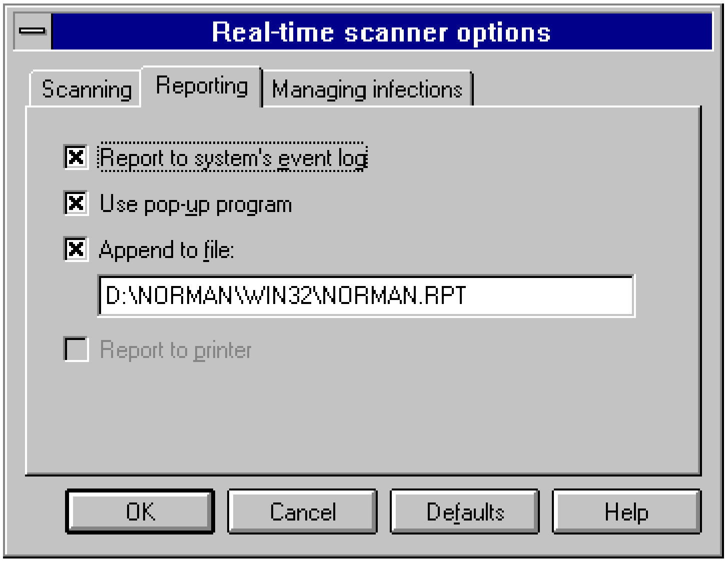
[ ] Scan boot sector

If you check this option, the real-time scanner will check the boot sector on a diskette inserted into the diskette drive.

[ ] Scan files

If you check this option, the real-time scanner will check all files on the diskette you are inserting.

Reporting



☒ Report to system's event log

☒ Use pop-up program

☒ Append to file: D:\NORMAN\WIN32\NORMAN.RPT

☐ Report to printer

[x] Report to system’s event log

The NT Application Event Log offers a standardized way of presenting various kinds of messages to an

Administrator. The NVC NT Service will store alert messages in the Event Log whenever a virus is found.

[x] Use pop-up program

If you want to be notified as soon as an infected file is detected, choose this option.

[x] Append to file

You can specify a separate report for the real-time scanner. This option is useful if you want to keep the information from the real-time scanner in a file different from the on-demand and scheduled scanning report.

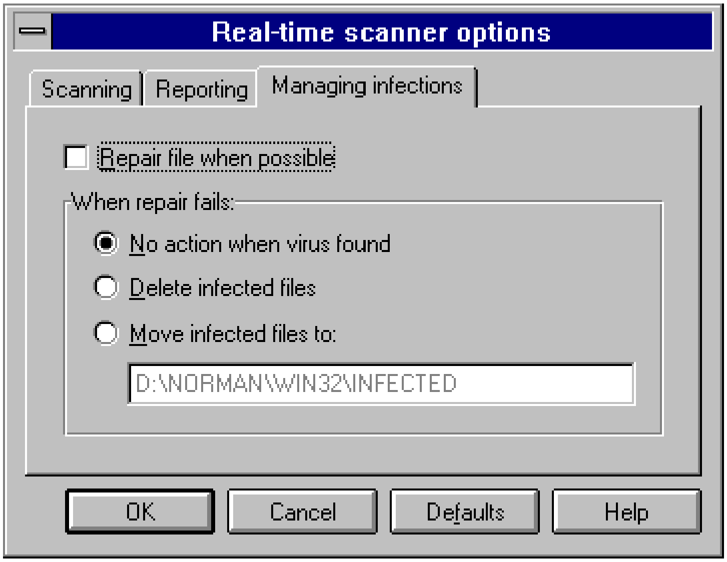
[ ] Report to printer

The real-time scanner sends the report file to the default printer that is set up through NT.

See the section “When A Virus Is Found” on page 94 for information on how to handle infected files.

Managing Infections

Use these options to decide how the real-time scanner should handle virus infections:



Real-time scanner options

□ Repair file when possible

When repair fails:

● No action when virus found

○ Delete infected files

○ Move infected files to:

D:\NORMAN\WIN32\INFECTED

There are four options regarding what action the scanner should take when an infected file is found:

The options are:

[ ] <u>R</u>epair file when possible

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

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

---

[x] <u>N</u>o action

If you wish to leave infected files alone at the time they are detected, then use this option and view the scanning report for details about possible infections.

[ ] <u>D</u>elete infected files

This option is for deleting infected files as they are being discovered.

[ ] Move infected files to:

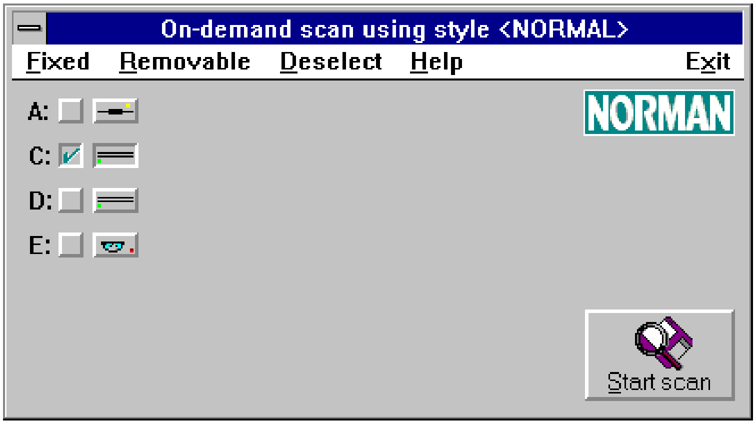
If you want to analyze possible viruses, you can choose this option and enter the path to the directory where you want to quarantine them. The scanner will create the directory if you specify a non-existent directory. Otherwise, the scanner will move infected files into the directory C:\NORMAN\INFECTED.

In a network environment, the area that you specify for storing infected files should be off-limits to everyone but the Supervisor.

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 as described in the section "Renaming Infected Files" on page 22.

On-Demand Scans

You can start on-demand scans by clicking the toolbar button or choosing the menu option Scan now. In either case, the following dialog appears:



A: □
C: ☑
D: □
E: □

The drives specified in the current style are checked. Note that the current style is specified in the title bar. You can group drives in fixed or removable drives, or choose Deselect to clear all drives and specify any combination you wish.

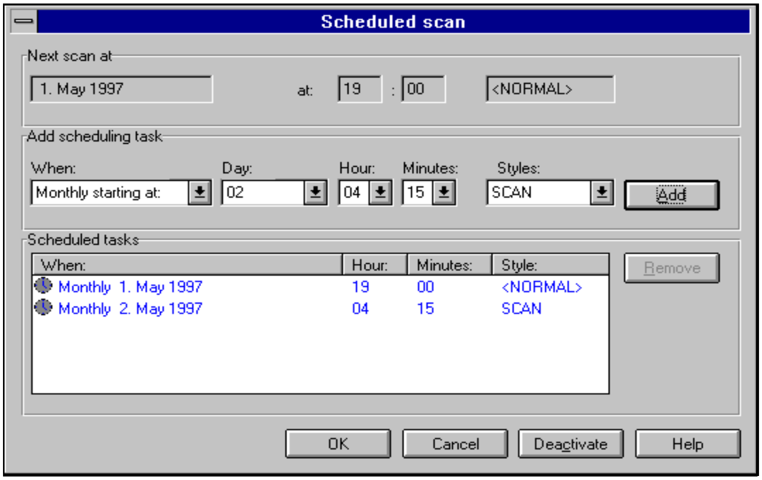
Remember that no remote drives are available, even though you may be running ‘locally’ on a remote machine.

Click on **Start scan**.

Note: If you change the drive information in this dialog, these changes will be reflected in the current style.

Scheduled Scans

Scheduled scanning is an ideal NT service function. Simply specify when and how the scan shall be performed. Click on the toolbar button or choose the menu option Options|Scheduler options and enter the requested information in this dialog box:



Scheduled scan

Next scan at

1. May 1997 at: 19 : 00 <NORMAL>

Add scheduling task

When:	Day:	Hour:	Minutes:	Styles:
Monthly starting at:	02	04	15	SCAN

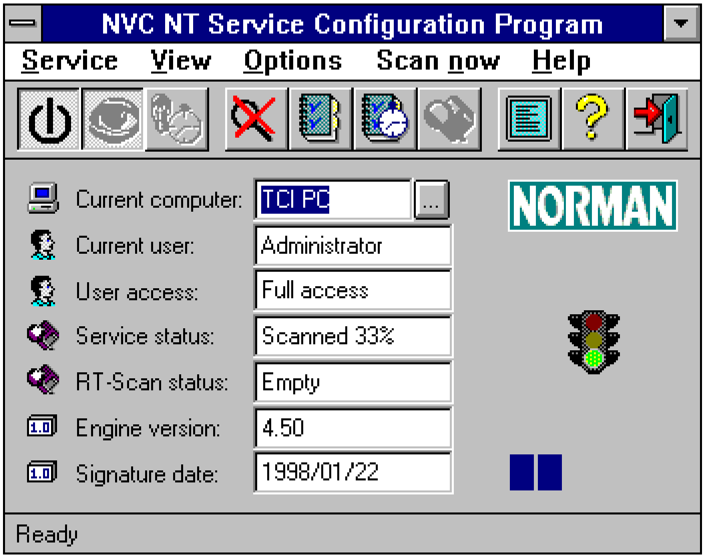
Scheduled tasks

When:	Hour:	Minutes:	Style:
Monthly 1. May 1997	19	00	<NORMAL>
Monthly 2. May 1997	04	15	SCAN

Please refer to the section “Scheduling Concepts” on page 51 for more information on this functionality.

The Scanning Process

When you're performing an on-demand or scheduled scan, the *Service status* field will display the status of the current scan as a percentage. A progress bar to the lower right provides the same information:



Current computer: TCI PC

Current user: Administrator

User access: Full access

Service status: Scanned 33%

RT-Scan status: Empty

Engine version: 4.50

Signature date: 1998/01/22

Ready

Note: Real-time scanning is temporarily disabled during on-demand and scheduled scanning.

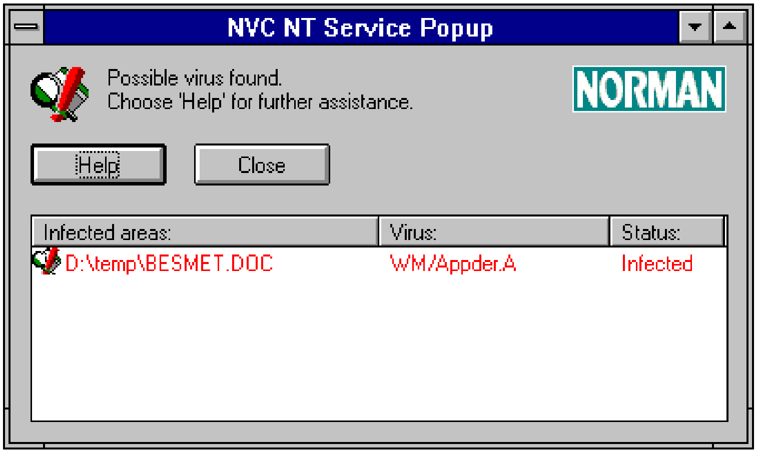
When A Virus Is Found

When a virus is found, you can be notified about the incident in three different ways, depending on your configuration options:

- Pop-up program
- NT Event Log
- Report file

All alert types are available for on-demand, scheduled and real-time scanning.

The most visible notification is a pop-up program that appears when the real-time scanner detects a virus:



Possible virus found.
Choose 'Help' for further assistance.

Infected areas:	Virus:	Status:
D:\temp\BESMET.DOC	WM/Appder.A	Infected

This is a dialog box with the necessary information on the infected file. You can grab the dialog with your pointing device and minimize, maximize, or move it around on the screen. You can also resize the columns inside the dialog.

If you want to remove the dialog after you recorded the information on infections, then click on **Close**.

To view the real-time scanning report, you must go back to the configuration program and view the report from there. A report is generated if you checked the report to file option and specified a file name in the dialog “Real-time scanner options”. If you do not close the dialog, possible new virus detections will be added to the list.

You cannot manage infected files from this dialog — it is displayed for informational purposes only:

Infected areas: the path and the name of the infected file.

Virus: the name of the virus.

Status: how the infected file(s) was handled.

First of all you should check the *status* of the infected file. The alternatives are:

Status:	**Reason:**
Repaired	Under Options|Real-time scanning options you checked the [ ] **Repair file when possible** option for automatic removal of viruses.
Deleted	You did not check the repair option, and/or the infected file could not be repaired. You also specified that infected files should be deleted.
Moved to...	You did not check the repair option, and/or the infected file could not be repaired. You also specified that infected files should be moved.
Infected	You did not check the repair option, and/or the infected file could not be repaired, and/or you specified [ ] **No action when virus found**.

If the status is “Repaired” or “Deleted”, the virus is already taken care of. Note that the file name and location is displayed. This information is also available in the NT Event Log and in the report file.

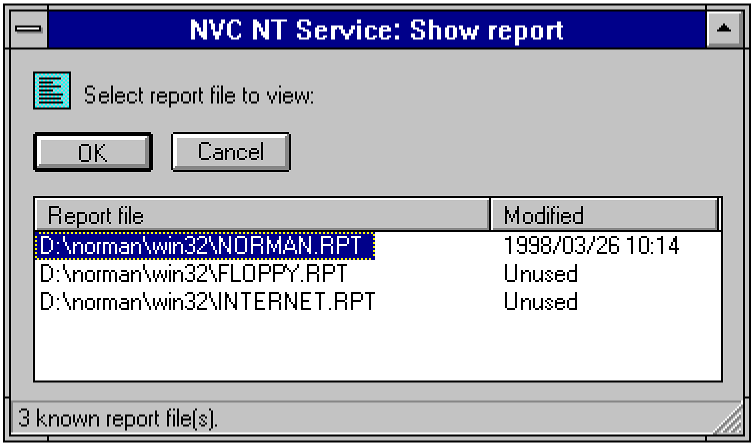
If the status is “Moved to...” or “Infected”, you still have one or more infected files on your machine. Remove the virus(es) by running the scanner with the option **[ ] Repair file when possible** ON, or highlight the virus in the list box and click the **Repair** button.

If NVC cannot remove the virus(es), you should delete the file(s) altogether.

Note: If an infected file resides on a write-protected floppy or a protected area on a server, the NVC NT Service cannot repair, move, or delete the file. When this is the case, the status for the file will always be listed as “Infected”.

View Report

When you select View|Report from the NT Service’s main window, you will see a list of all report file names. If you specified separate report files for the different styles (see “Saving Your Configurations as Styles” on page 44), you can access any of these from this dialog:



NVC NT Service: Show report

Select report file to view:

Report file	Modified
D:\norman\win32\NORMAN.RPT	1998/03/26 10:14
D:\norman\win32\FLOPPY.RPT	Unused
D:\norman\win32\INTERNET.RPT	Unused

3 known report file(s).

The path and names of the report files are displayed together with the date and time when the report was last updated.

Highlight the report file you want to see and click on **OK**.

The report is displayed as plain text in a separate window.

If you have specified a specific report file for a certain style that hasn’t been applied yet, the report file will appear in the list with status ’Unused’ in the column Modified.

If a report file cannot be displayed because an on-demand or scheduled scan is writing to the file, the Modified column will signify ’In use’.

Styles in NVC NT Service

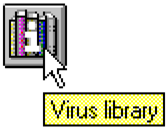
You cannot use styles from NVCNT with the NVC NT Service or vice versa, because the configuration options are different for the two modules. Therefore, you must define separate styles for NVC NT Service. However, the procedures for setting up and editing styles are identical. Please refer to “Saving Your Configurations as Styles” on page 44 for details.

Other Functions

Finding Out More About Viruses

There are several functions within the scanner which allow you to learn more about viruses.

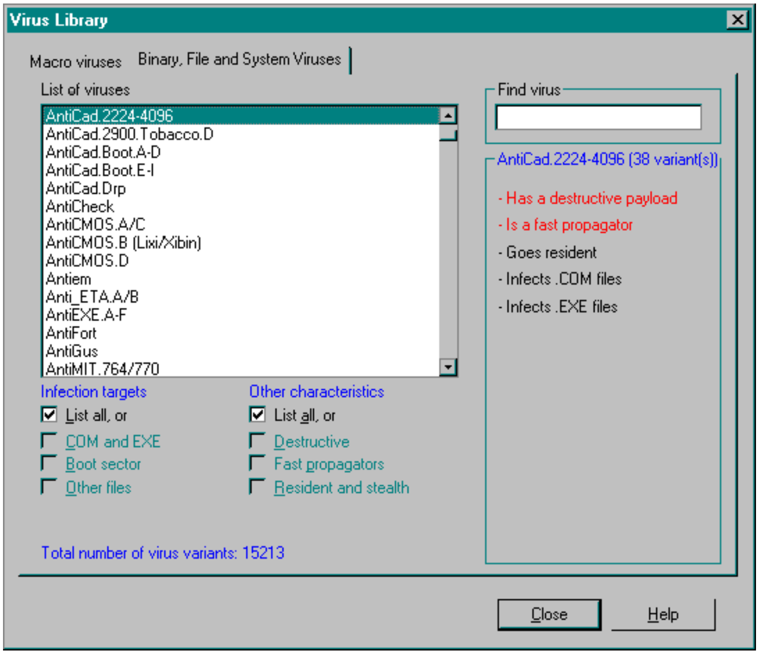
Virus Library gives an overview of names and characteristics of the viruses that the scanner can recognize. You can access Virus Library through View|Virus Library or by clicking on this toolbar button:



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.



AntiCad.2224-4096
AntiCad.2900.Tobacco.D
AntiCad.Boot.A-D
AntiCad.Boot.E-I
AntiCad.Drp
AntiCheck
AntiCMOS.A/C
AntiCMOS.B (Lixi/Xibin)
AntiCMOS.D
Antiem
Anti_ETA.A/B
AntiEXE.A-F
AntiFort
AntiGus
AntiMIT.764/770

AntiCad.2224-4096 (38 variant(s))

- Has a destructive payload
- Is a fast propagator
- Goes resident
- Infects .COM files
- Infects .EXE files

Infection targets

☑ List all, or
☐ COM and EXE
☐ Boot sector
☐ Other files

Other characteristics

☑ List all, or
☐ Destructive
☐ Fast propagators
☐ Resident and stealth

Total number of virus variants: 15213

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 floppy 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.

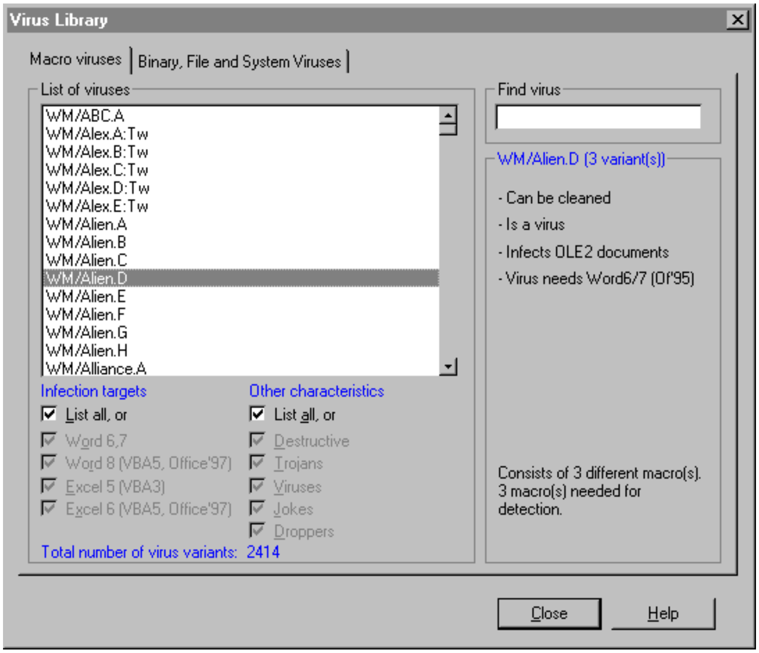
Other files

Infects other files.

Goes resident in Low, High, UMB, Video RAM

The virus stays in memory when first activated.

Macro Virus Attributes



Virus Library

Macro viruses | Binary, File and System Viruses

List of viruses

WM/ABC.A
WM/Alex.A:Tw
WM/Alex.B:Tw
WM/Alex.C:Tw
WM/Alex.D:Tw
WM/Alex.E:Tw
WM/Alien.A
WM/Alien.B
WM/Alien.C
WM/Alien.D
WM/Alien.E
WM/Alien.F
WM/Alien.G
WM/Alien.H
WM/Alliance.A

Infection targets

☑ List all, or
☑ Word 6,7
☑ Word 8 (VBA5, Office'97)
☑ Excel 5 (VBA3)
☑ Excel 6 (VBA5, Office'97)

Other characteristics

☑ List all, or
☑ Destructive
☑ Trojans
☑ Viruses
☑ Jokes
☑ Droppers

Total number of virus variants: 2414

Find virus

WM/Alien.D (3 variant(s))

- Can be cleaned
- Is a virus
- Infects OLE2 documents
- Virus needs Word6/7 (Of'95)

Consists of 3 different macro(s).
3 macro(s) needed for detection.

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. See Binary viruses on page 99.

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.

Book on Viruses

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

Topics include: evolution, virus theory, and more!

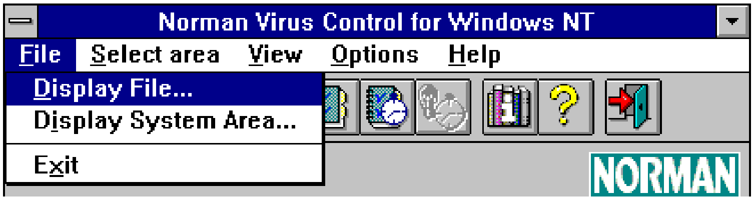
Navigate through all this information by clicking on the **green** entries.

The Display Feature

The **Display** feature displays data from files and system areas as hexadecimal values and printable characters.

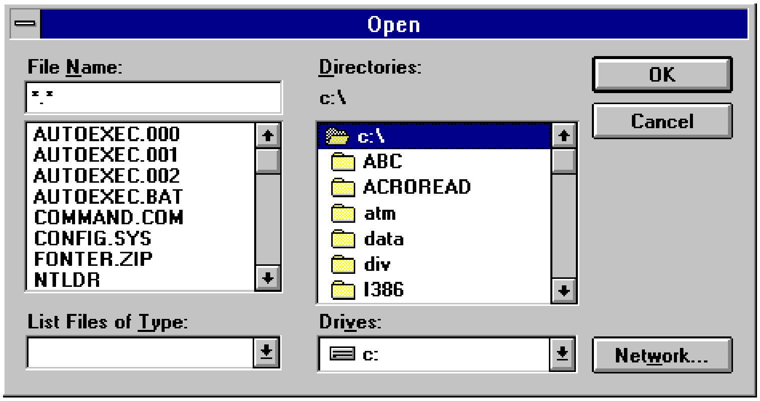
You can access this function from the File menu.

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" menu option.



Display File

If you choose **Display file**, you will be prompted to choose a file from within a file window.



File Name: *.*

AUTOEXEC.000
AUTOEXEC.001
AUTOEXEC.002
AUTOEXEC.BAT
COMMAND.COM
CONFIG.SYS
FONTER.ZIP
NTLDR

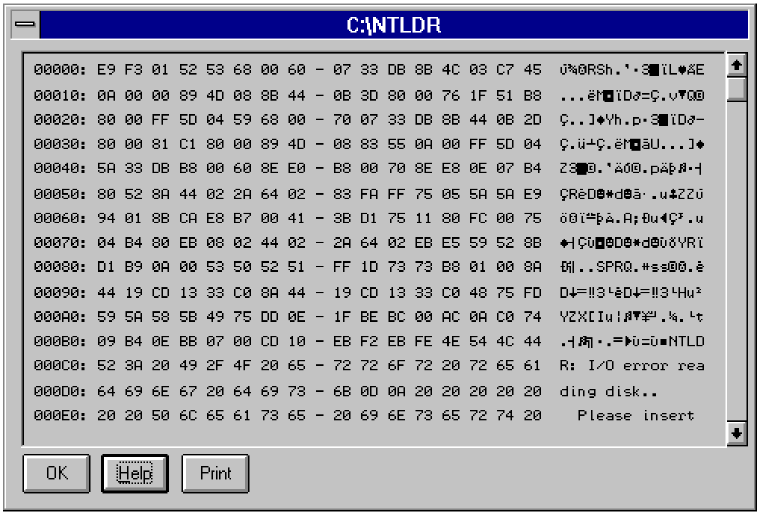
Directories: c:\

c:\
ABC
ACROREAD
atm
data
div
I386

List Files of Type:

Drives: c:

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



```
00000: E9 F3 01 52 53 68 00 60 - 07 33 DB 8B 4C 03 C7 45  ú%☺RSh.'·3█ïL♦ÄE
00010: 0A 00 00 89 4D 08 8B 44 - 0B 3D 80 00 76 1F 51 B8  ...ëM◘ïD♂=Ç.v▼Q©
00020: 80 00 FF 5D 04 59 68 00 - 70 07 33 DB 8B 44 0B 2D  Ç..]♦Yh.p·3█ïD♂-
00030: 80 00 81 C1 80 00 89 4D - 08 83 55 0A 00 FF 5D 04  Ç.ü┴Ç.ëM◘âU...]♦
00040: 5A 33 DB B8 00 60 8E E0 - B8 00 70 8E E8 0E 07 B4  Z3█©.'Äó©.pÄÞ♫·┤
00050: 80 52 8A 44 02 2A 64 02 - 83 FA FF 75 05 5A 5A E9  ÇRèD☻*d☻â·.u♣ZZú
00060: 94 01 8B CA E8 B7 00 41 - 3B D1 75 11 80 FC 00 75  ö☺ï╩ÞÀ.A;Ðu◄Çⁿ.u
00070: 04 B4 80 EB 08 02 44 02 - 2A 64 02 EB E5 59 52 8B  ♦┤Çö◘☻D☻*d☻öõYRï
00080: D1 B9 0A 00 53 50 52 51 - FF 1D 73 73 B8 01 00 8A  Ð╣..SPRQ.↔ss©☺.è
00090: 44 19 CD 13 33 C0 8A 44 - 19 CD 13 33 C0 48 75 FD  D↓═‼3└èD↓═‼3└Hu²
000A0: 59 5A 58 5B 49 75 DD 0E - 1F BE BC 00 AC 0A C0 74  YZX[Iu¦♫▼¥╝.¼.└t
000B0: 09 B4 0E BB 07 00 CD 10 - EB F2 EB FE 4E 54 4C 44  .┤♫╗·.═►ö=ö■NTLD
000C0: 52 3A 20 49 2F 4F 20 65 - 72 72 6F 72 20 72 65 61  R: I/O error rea
000D0: 64 69 6E 67 20 64 69 73 - 6B 0D 0A 20 20 20 20 20  ding disk..
000E0: 20 20 50 6C 65 61 73 65 - 20 69 6E 73 65 72 74 20    Please insert
```

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.

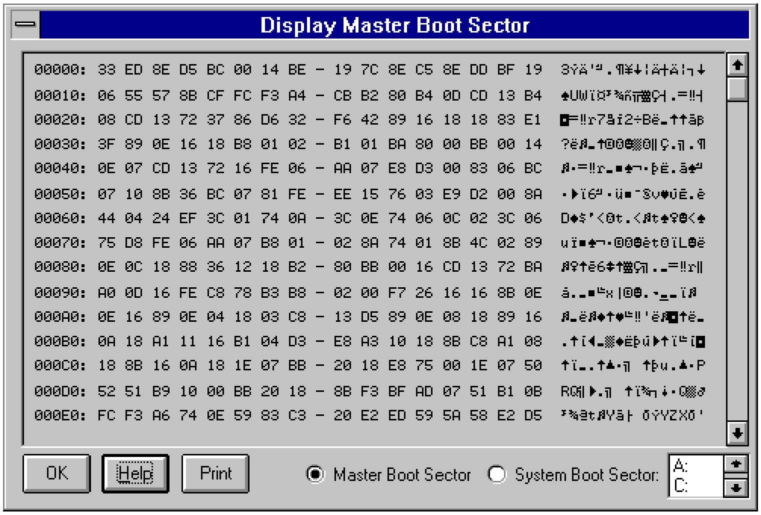
This function is especially useful when technical personnel want to look inside a file or sector for signs of a virus infection.

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

Close quits from the function and returns you to the main window. **Print** permits you to send the displayed file to the printer that is set up through Windows. **Help** gives you help on this function.

Display System Areas

If you choose the **Display system area** menu choice, this screen will appear:



Display Master Boot Sector

```
00000: 33 ED 8E D5 BC 00 14 BE - 19 7C 8E C5 8E DD BF 19   3YÄ'╝.¶¥↓¦Ä┼Ä¦┐↓
00010: 06 55 57 8B CF FC F3 A4 - CB B2 80 B4 0D CD 13 B4   ♠UWïõ³¾ñ╥▓Ç┤.=‼┤
00020: 08 CD 13 72 37 86 D6 32 - F6 42 89 16 18 18 83 E1   ◘═‼r7åi2÷Bë▬↑↑äβ
00030: 3F 89 0E 16 18 B8 01 02 - B1 01 BA 80 00 BB 00 14   ?ëß▬↑☺☻●▒☺║Ç.╗.¶
00040: 0E 07 CD 13 72 16 FE 06 - AA 07 E8 D3 00 83 06 BC   ß•=‼r▬■♠¬•þË.â♠╝
00050: 07 10 8B 36 BC 07 81 FE - EE 15 76 03 E9 D2 00 8A   •►ï6╝•ü■¯§v♥ÚÊ.è
00060: 44 04 24 EF 3C 01 74 0A - 3C 0E 74 06 0C 02 3C 06   D♦$'<☺t.<ßt♠♀☻<♠
00070: 75 D8 FE 06 AA 07 B8 01 - 02 8A 74 01 8B 4C 02 89   uï■♠¬•☺☺☻èt☺ïL☻ë
00080: 0E 0C 18 88 36 12 18 B2 - 80 BB 00 16 CD 13 72 BA   ß♀↑ê6↕↑▓Ç╗.▬=‼r║
00090: A0 0D 16 FE C8 78 B3 B8 - 02 00 F7 26 16 16 8B 0E   á.▬■╚x|☺☻.¬▬▬ïß
000A0: 0E 16 89 0E 04 18 03 C8 - 13 D5 89 0E 08 18 89 16   ß▬ëß♦↑♥╚‼'ëß◘↑ë▬
000B0: 0A 18 A1 11 16 B1 04 D3 - E8 A3 10 18 8B C8 A1 08   .↑í◄▬▒♦Ëþú►↑ï╚í◘
000C0: 18 8B 16 0A 18 1E 07 BB - 20 18 E8 75 00 1E 07 50   ↑ï▬.↑▲•╗ ↑þu.▲•P
000D0: 52 51 B9 10 00 BB 20 18 - 8B F3 BF AD 07 51 B1 0B   RQ╣►.╗ ↑ï¾┐↓•Q▒∂
000E0: FC F3 A6 74 0E 59 83 C3 - 20 E2 ED 59 5A 58 E2 D5   ³¾ªtßYâ├ ÕÝYZXÕ'
```

● Master Boot Sector ○ System Boot Sector: A: C:

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:. In addition, you can view the SBS on all floppy drives.

See the sections “Master Boot Sector (MBS)” and “System Boot Sector (SBS)” on page 40 for an explanation of these terms.

Examples of Common Uses of the Scanner

Because of the scanner's configuration flexibility, there are many ways to run scans. You will no doubt find the best methods for your organization's needs. To get you started, here are several techniques that might be helpful.

Automatically Scan Different Areas at Different Times

Goals: To automatically scan the entire hard drive in the beginning of the day, to automatically scan only the C:\FINANCES directory during lunch, and to automatically scan only the C:\WORDS directory at the end of the day. If any infected files are found, repair infected files if possible, or move them to the C:\NORMAN\INFECTED directory.

What we will use: Styles and the scheduler.

Steps:

1. Setup 3 styles: ALLOFC, $ONLY, WORDONLY (for example), and configure each style accordingly for scanning areas, scanning options, reporting options, etc.
2. In the scheduler, specify the day and the hours at which to run each of the styles.
3. Remember to click on **Add** and **OK** before exiting the "Scheduled scan" dialog box.
4. Exit the scheduler dialog box.
5. Do **not** exit NVCNT.

Decrease Screen Output During Scan

Goal: To have the scanner run **once** and display only critical messages on the screen.

We will use the following options:

[x] **Report to file** and/or [x] **Report to printer**,

[x] **Report only if infection**,

[x] **Exit upon completion**,

[x] **Ignore locked files**,

[x] **Minimize while scanning**, **and**

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

Steps:

1. Start the scanner.
2. Click on Options|Scanning options.
3. In the "Scanning" tabbed dialog box, ensure that [ ] **Don't stop on virus** is checked.
4. In the "Scanning" tabbed dialog box, ensure that [ ] **Exit upon completion** is checked.
5. In the "Scanning" tabbed dialog box, ensure that [ ] **Ignore locked files** is checked.
6. In the "Reporting" tabbed dialog box, ensure that [ ] **Report to printer** and/or [ ] **Report to file** are checked.
7. In the "Reporting" tabbed dialog box, ensure that [ ] **Report only if infection** is checked.
8. In the "Additional options" tabbed dialog box, ensure that [ ] **Minimize while scanning** is checked.

When all of this is done, the scanner will run as a minimized icon, and you will only see a report on the screen if an infection is found. Otherwise, the scanner will exit when it has finished scanning.

This method is great for running a single scan at night. If you leave your NT machine on during the night and use this method, the next morning you will see a report on the screen if a virus was found.

Note: If you are running more than one nightly scan, please refer to the section "Scheduling Several Unattended Scans" on page 55 for details about scheduling more than one nightly scan.

Consequently, any user who wishes to use the machine in the morning will see this notification. If no virus was found, then nothing is displayed on the screen, and the user can continue as normal.

> *Remember: if you have set the scanner up to always report to a file, then you can always view the most recent report by clicking on View|Report.*

Create Icons and Customize the Scan

Goal: To create icons that sit on the Desktop and perform customized scans on demand. By doing so, you can bypass clicking on the scanner's icon and spending time configuring your scan. Instead, you can configure your scan beforehand and then click on your customized icon when you wish to perform the scan. For instance, if you would like to scan the C:\DOS directory on demand simply by clicking on an icon, follow the steps outlined below.

What we will use: Styles and the parameter associated with styles.

Steps:

1. Create a style that you wish to use for this purpose. For the example that we gave above, we would create a style named DOSONLY, we would choose the C:\DOS directory as the search area, and then we would select other configurations such as reporting, etc.

2. Switch to Program Manager and either create a new group and then make a new item or create a new item in an existing group.
3. For the new item's properties, you can utilize the parameter /ST:. Then the scanner will launch the scan immediately after you click on the icon.

   The syntax for the command line is:

   ```
   drive:path\nvcnt.exe st:[name of
   style]
   ```

   For example, if NVCNT.EXE resides in the C:\NORMAN\WIN32 directory and you wish the icon to start scanning immediately using the DOSONLY style, then your command line for the new program item will be:

   ```
   c:\norman\win32\nvcnt /ST:DOSONLY
   ```

You can, of course, combine this method with the configuration described in "Decrease Screen Output During Scan" above by altering the settings in the style.

Scan Automatically after Downloading Programs

Goal: To automatically scan programs that you have downloaded onto your PC.

What we will use: A batch file and styles. The batch file will run your communications software (CompuServe, AmericaOnLine, etc.) and then run the scanner against the files that you have downloaded.

Steps:

1. If possible, set up your communications software to store all downloaded files in one directory. (If you cannot do this, then find out where the downloaded files are stored by default.)
2. Create a style for this purpose and configure it accordingly. For the search area, you must specify the directory in which your downloaded files are stored.

And since a fair number of downloaded files are archived, you should use the "Scan archive files" option.

3. Create a batch file which first runs your communications software and then NVCNT /ST: with the style you have created.

   For example:

   ```
   DOWNSCAN.BAT
   rem the next line runs PCPLUS.
   pcplus
   rem the next line runs NVCNT immediately
   rem after PCPLUS exits.
   c:\norman\win32\nvcnt /ST:DWNLOAD
   rem the above line tells NVCNT to use the
   rem DWNLOAD style. I have set PCPLUS to
   rem put all my downloads into the
   rem C:\PCPLUS\SCANME directory.
   rem Therefore, in the DWNLOAD style, I
   rem have specified the search area to be
   rem C:\PCPLUS\SCANME.
   ...etc
   ```

4. Now you can create an icon that runs this batch file from the Desktop.

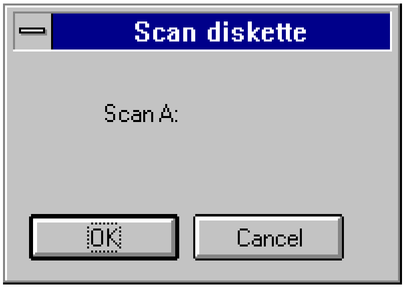
Shortcut for Scanning Floppies

Goal: Use a shortcut when you want to scan floppy disks for viruses.

What we will use: NVCNT and your mouse.

Steps:

1. Place the mouse-pointer anywhere inside the main window of the scanner.
2. Click the **right mouse button**, and you will see this dialog box:



3. You can only choose one floppy drive at a time. When this is done, click the **OK** button and the scanner will use the *current* style to start scanning the disk in the selected floppy drive.

Updating NVC

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:

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

Norman Internet Update

The polling program Norman Internet Update automatically checks for updated files to the scanning engine (definition files, DLL/VxD) on Norman servers and it's available for Windows 9x and Windows NT.

NIU will appear as a separate item in the Norman group. To run NIU, you need a TCP/IP (Internet) connection. You can start the program by placing it in the Startup group or doubleclicking the icon in the Norman group. When you run NIU, the program will check a Norman server for updated virus definition files. These files reside in the NSE directory.

Configuration Settings

When Norman Internet Update is installed, the section NSE Update is added to the configuaration file (`nvc32.cfg`).

The default settings that apply if you accepted to place NIU in the Startup group, or when you run the program manually bly doubleclicking the icon, are:

`-hidden -wait:5`

`Hidden`: without appearing on the screen, the program checks the validation key and the time stamps on your files in the NSE directory versus the time stamps on the available files on the Norman server. You will be notified if the validation key is missing or wrong, if updated files are available, or if any problems occur.

`Wait`: after the program has started, it waits for 5 minutes before it starts working. The `-wait` parameter requires the `-hidden` parameter.

Note: NIU will not be invoked on a PC that is running continously. In such instances you can use the scheduler in Windows 98 or Windows NT to invoke the program. On Windows 95, however, you'll have to log out and in, or start NIU manually.

Note well:

If you're running NIU with a modem, make sure that you hang up when a download is completed. You may configure your dialer to hang up two minutes after a download is complete, for example.

How to Use Norman Internet Update

1. Enter the CD key in the Authentication field.
2. Click on **Validate**. The CD key you entered is checked by a Norman server, as well as the time stamp on the virus definition files.
3. When the key is validated, the **Download** button is activated if there are updated files available.
4. Click **Download** for fetching the package with the latest updates. The new files will replace the old files at next reboot.

For network administrators: see the *Administrator's Guide* for more details.

Index