



NORMAN

Norman Virus Control for Workstations

Version 5.2

Reference Guide

Limited warranty

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

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

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

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

This warranty expires 30 days after purchase.

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

The Norman logo is a registered trademark of Norman ASA.

Names of products mentioned in this documentation are either trademarks or registered trademarks of their respective owners. They are mentioned for identification purposes only.

NVC documentation and software are

Copyright © 1996-2001 Norman ASA.

All rights reserved.

August 2001

Last revised on 20 August 2001

Norman Offices

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 Web: <http://www.norman.com.au>

Norman Data Defense Systems AS

Dronningensgade 23, DK-5000 Odense C, **Denmark**

Tel. +45 6311 0508 Fax: +45 6313 3901

E-mail: normandk@normandk.com Web: <http://www.norman.no/dk>

Norman Ibas OY

Läkkisepäntie 11, 00620 Helsinki, **Finland**.

Tel: +358 9 2727 210 Fax: +358 9 2727 2121

E-mail: norman@norman-ibas.fi Web: <http://www.norman-ibas.fi>

Norman Data Defense Systems GmbH

Kieler Str. 15, D-42697 Solingen, **Germany**.

Tel: +49 212 267 180 Fax: +49 212 267 1815

E-mail: norman@norman.de Web: <http://www.norman.de>

Norman/SHARK BV

Postbus 159, 2130 AD, Hoofddorp, **The Netherlands**.

Tel: +31 23 563 3960 Fax: +31 23 561 3165

E-mail: sales@norman.nl Web: <http://www.norman.nl>

Norman ASA

Mailing address: P.O. Box 43, N-1324, Lysaker, **Norway**.

Physical address: Strandveien 37, Lysaker, N-1324 Norway.

Tel: +47 67 10 97 00 Fax: +47 67 58 99 40

E-mail: norman@norman.no Web: <http://www.norman.no>

Norman Data Defense Systems AG

Postfach CH-4015, Basel, **Switzerland**.

Tel: +41 61 487 2500 Fax: +41 61 487 2501

E-mail: norman@norman.ch Web: <http://www.norman.ch>

Norman Data Defense Systems (UK) Ltd

Lawn Farm, Oakhill Road, Woodhill

Milton Keynes, Bucks MK5 6AH, **United Kingdom**.

Tel: +44 1908 520 900 Fax: +44 1908 520 909

E-mail: norman@normanuk.com Web: <http://www.normanuk.com>

Norman Data Defense Systems Inc.

9302 Lee Highway, Suite 950A, Fairfax, VA 22031, **USA**

Tel: +1 703 267 6109, Fax: +1 703 934 6367

E-mail: norman@norman.com Web: <http://www.norman.com>

Training and Technical Support

For training or technical support, please contact your local dealer or Norman ASA.

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 key name with “[“ and ”]”, as in:

[Ctrl]

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

Start|Run

This means that you should click on “Start” and from there click on the “Run” menu item.

Important notes appear in boxes like the one below:

Note: Right-click to start on-demand scanning.

We use bold face type to identify anything that you can click or select, for example, button names and dialog box names.

Click **OK** to view the **Scheduled task** dialog box.

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

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



Paragraphs that are clearly intended for users in a network or for the system administrator, and hence of little or no interest for single-users, are identified by a network icon in the left margin.



This manual is intended for Windows’ as well as OS/2 users. Whenever platform specific differences affect NVC, this icon in the margin denotes a special consideration for OS/2.

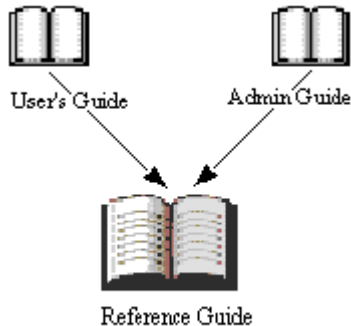
This is a ***beta version*** of NVC for OS/2 version, available at the end of June. The official release is scheduled for third quarter 2001.

System requirements

Norman Virus Control (NVC) v5 for Workstations can run on any machine that runs any national language version of Windows 95 / 98, Windows NT 4 with SP 4 or higher, Windows 2000, Windows ME, OS/2 Warp 4, OS/2 Warp Server, Workstation On-demand, and eComStation.

For Windows 95 and NT, Internet Explorer version 4 or higher is required.

Who should read this manual?



This manual covers all functions found in NVC and is therefore intended for all NVC users—single-users as well as administrators—with a need for in-depth information about the product.

In addition to this manual, the *Administrator's Guide* covers topics that are particularly useful for those responsible for network installations, and the *User's Guide* is a short introduction to the basic functions in NVC.

Installation is *not* discussed in this manual. For installation in networks and on stand-alone machines, refer to the *Administrator's Guide* or *User's Guide*, respectively.

Prerequisites

To take full advantage of all the functions in NVC, you should have a good understanding of the different modules in NVC and how they work together, as described in this document.

If you are running NVC in a network, you should have detailed knowledge about the operating system(s) on servers and workstations, as well as the network installation in your organization.

Technical support

Norman provides technical support and consultancy services for NVC and security issues in general. Technical support also comprises quality assurance of your anti-virus installation, including assistance in tailoring NVC to match your exact needs.

Note that the number of services available will vary between the different countries.

Contents

Conventions	iv
System requirements	v
Who should read this manual?	v
Technical support	vi
About NVC	11
What is NVC?	11
What's new in NVC v5?	11
NVC program groups	14
Groups, modules, and components	14
Shortcut to NVC modules and scanning	15
Configuration editor	17
List of components	18
List of products in the pipeline	18
Installation settings	18
Install	19
Start	20
Update mode	21
Internet	22
LAN/WAN	23
Authentication	23
Common settings	24
Scanning	25
Exclude list	27
Quarantine	28
On-demand scanner	30
Diagnostics	30

Scanning	31
About On-access scanning on Windows NT/2000	32
On-access scanner (interactive)	33
Scanning	35
Cleaning	37
On-access scanner (non-interactive)	37
Cleaning	39
NVC on Windows Terminal Server	40
About messages and logging	42
Message routing	42
Messages	43
Routing	44
Message handling	45
Message logger	46
Message console	48
Event Log	48
Task editor	49
General	50
Targets	50
Selecting targets	50
Common scanning options	52
Options	53
Schedule	54
About the scheduler	54
Utilities	55
Components	55
Task files	56
Quarantine	57
Messages	58
Messages tab	58
Message files tab	60
Updating NVC	62
Norman Internet Update	62

Starting NIU	62
NIU and Internet connection.....	63
How NIU works	64
LAN/WAN	65
Miscellaneous on NVC	66
The agent.....	66
About the Command line scanner.....	67
Starting the Command line scanner	67
Cleaning infected files	67
Command line scanning options	68
Combining Different Parameters	72
Command Line Scanner Errorlevels	73
FAQ	74

About NVC

What is NVC?

Norman Virus Control (NVC) is an anti-virus program that monitors your PC for malicious software, also referred to as *malware*. Malware is viruses, worms, and other varieties of destructive code. NVC can detect and remove known and unknown viruses from hard disks, floppy disks, e-mail attachments, etc.

NVC checks files when they are accessed, and possible viruses are removed automatically. If NVC is unable to clean an infected file, you will receive a warning and instructions how to proceed.

You can—and we encourage you to do so—perform manual scans of selected areas of your machine, and use the task editor and scheduler to define what to scan and when.

Note: NVC is shipped with pre-selected settings that we consider sufficient to protect you against virus attacks. Most modules can be configured, so that you can set up NVC to suit your needs.

What's new in NVC v5?

For those familiar with the previous version of NVC, the 4.x “generation”, the current version is distinctly different. And there is more than meets the eye. Behind the new GUI the functionality has been significantly improved. The increasingly popular use of right-click functionality has been implemented in NVC where appropriate, providing short-cuts to certain tasks.

Planning for NVC v 5 included the ambition of improving all facets of the product. First of all we wanted NVC to be more user-friendly, especially with regard to installation, administration, and distribution in networks. We also wanted NVC to be as ‘invisible’ as possible, knowing that the average customer wants an anti-virus product to be a silent partner that

keeps the PC virus free with a minimum of distraction for the user.

NVC v5 employs two different network mechanisms:

- For installation, distribution and configuration, regular file sharing using drive letters or UNC paths is employed.
- For messaging and logging, a proprietary network protocol layer has been devised.

The messaging system is part of the basic installation of NVC on a networked computer, and it is active as soon as the resident agent is running. Among a number of other vocations, the agent handles the traffic between the different input and output modules. The administrator merely has to configure the system in a way that messages of various importance are passed on to the correct message output modules.

Aside from the cosmetics, we have of course kept and further developed Norman's renowned core technology; the scanning engine. There is nothing wrong with a fancy GUI and clever programming, but the single most important task for an anti-virus application is to keep computers virus free.

The scanning engine will now detect and remove viruses based on Floating Point Unit (FPU) and Multi Media Extensions (MMX) instructions. Even though only a couple of today's viruses use FPU or MMX instructions, the number will grow.

The scanner's new 32-bit emulator will allow detection and help analysis of complex, encrypted, polymorphic viruses.

Summing up some of the most prominent modifications in NVC v5, the list includes:

- Simplified installation
- Simplified management
- Ease of use
- Invisibility

NVC v5 user interface is made up from four main groups:

- Configuration editor
- Task editor
- Utilities

- Internet Update

These appears as separate items in the Norman program group.



These groups are located in the Norman folder on the OS/2 desktop.

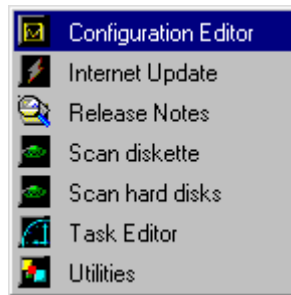
⇒ See 'Configuration editor' on page 17, 'Task editor' on page 49, 'Utilities' on page 55, and 'Norman Internet Update' on page 62.

NVC program groups

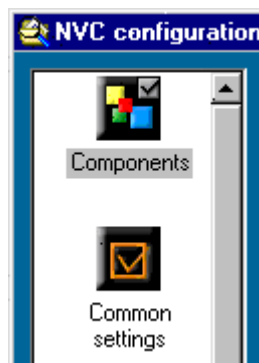
This chapter presents the groups and their matching modules and components that make up NVC v5. If a component has a related function elsewhere in the program, there will be a reference with title and/or page number to the relevant section. Sometimes we refer to the other two NVC 5 manuals: the *User's Guide* and the *Administrator's Guide*. Most components can be configured in different ways, and the following sections describes all available configuration options.

Groups, modules, and components

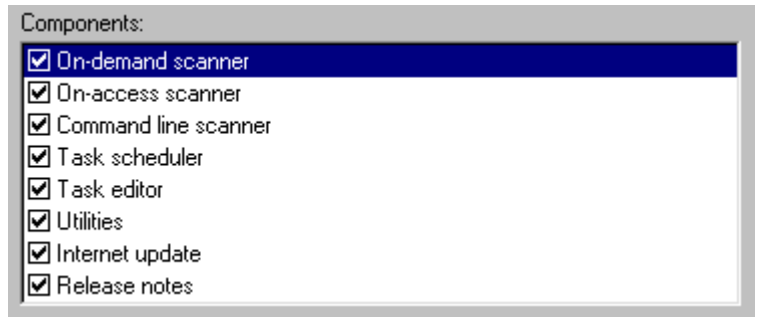
When we talk about a NVC **group**, we are referring to a larger entity that holds modules and components. Examples of NVC groups are: Configuration editor, Internet Update, Task editor, and Utilities:



Listed on the left-hand side in each group, there are **modules**:



And finally, the modules contains **components**, that often are a set of configuration options. You can view this list from **NVC configuration|Installation settings|Install**:



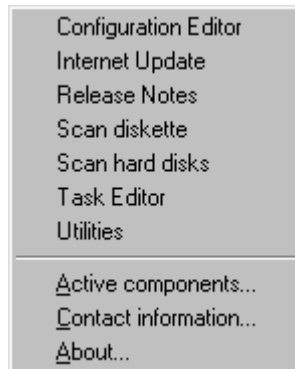
Shortcut to NVC modules and scanning



During setup, a Norman icon is placed in the system tray in the lower right-hand corner of the screen.

OS/2: NVC appears as an entry in the desktop menu. Right-click on the desktop and select *Norman Virus Control*.

The items listed above the separation line on the menu that appears when you click on this icon, are copies of the items that at any time appear on the Start|Programs|Norman Virus Control menu.



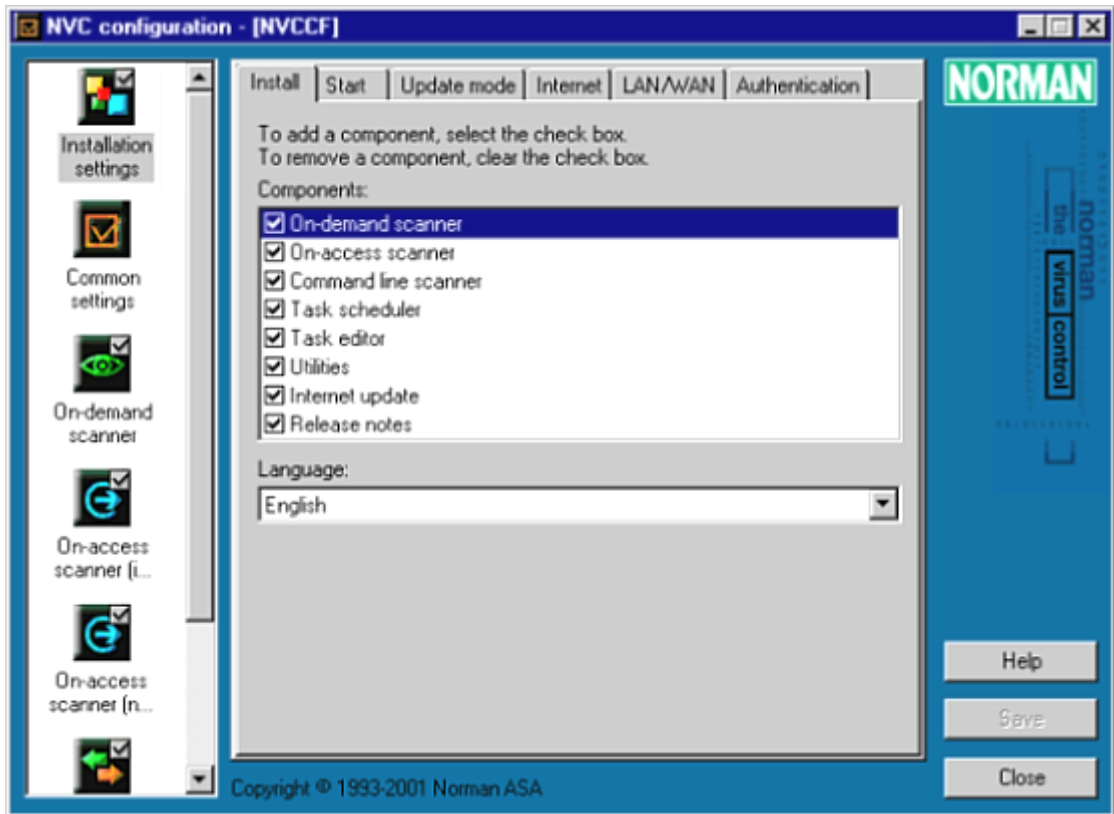
This is a shortcut to NVC's main modules, as well as some typical scanning tasks. In Windows, you can click on either mouse button to display this menu. In addition to easy access to the NVC modules and scanning options, you can read the release notes for the current version, view active components, display a list of Norman offices with street, web, and e-mail addresses. The "About" option displays information about the

current scanner engine, including signature date and number of viruses for the virus definition files.

This function is also the originator of messages regarding outdated virus definition files, expiration of licence period, and a warning if you shut down your computer while a floppy is inserted in the floppy drive.

Configuration editor

You can configure the different functions in NVC from one central point — the Configuration editor. Select *Configuration editor* from the Norman group/folder:



The configuration editor's different modules are listed on the left hand side of the dialog box. The list inside the dialog box reflects which components you have installed. Components like *Message router* and *Messages*, for example, will not appear on a single-user, stand-alone installation.

Each component has its own tabbed dialog box with a set of configuration options. Click on the component you wish to

configure and make your selections from the corresponding tabbed dialog box.

List of components

Since NVC is made up from different plug-ins, the list of components is subject to change. The present version of NVC features these components:

- On-demand scanner
- On-access scanner
- Command line scanner
- Task scheduler
- Task editor
- Utilities
- Message router
- Messages
- Norman Internet Update

List of products in the pipeline

The following plug-ins are in the pipeline for release in the near future. Some items on the list already exist as products in their own right, but need to be implemented in the new version 5 framework:

- E-mail, SMS, SNMP messaging
- Internet proxy
- NVC for Novell - FireBreak
- NVC for Lotus Domino
- NVC for MS Exchange
- Norman Personal Firewall
- NVC for MIMESweeper

Installation settings

NVC comes with a set of components that will be installed during setup. When setup is complete, you can remove possible undesired components. NVC is a plug-in based application, and new plug-ins, i.e. components, are likely to be introduced as new technology and security threats commence.



Common for all tabs:

In a network environment, the **Access field** at the bottom of each tab will appear if you have administrator's rights. The system administrator decides what should be visible and/or configurable from the workstations. The average user may therefore view all or some of the tabs, but is not necessarily entitled to change the settings.

Install

Note that you at any time can go back to this tab to add and/or remove components. By default, all components are added when NVC is installed.

☒ **On-demand scanner**

The On-demand scanner enables you to perform periodic scans of selected areas of your computer. If you are using the Task scheduler (see below), you need to install the On-demand scanner.

⇒ 'On-demand scanner' on page 30.

☒ **On-access scanner**

The On-access scanner is an ongoing process that monitors critical activities on your system. Depending on your configuration, this can involve file access and copy/move to other drives or directories.

⇒ 'On-access scanner (interactive)' on page 33.

☒ **Task scheduler**

The Task scheduler is a tool that is used for running task files at scheduled times.

⇒ 'About the scheduler' on page 54.

☒ **Task editor**

Use this tool to create task files and to view/change events entered in the Task scheduler. A task file shortcut can be placed on the desktop as an icon, or added to the Start menu as an item. Scheduled task files must reside in `... \nvc\tasks`.



You can place the OS/2 shadow for the task file wherever you wish. The actual file(s), however, must reside in
... \nvc\tasks.

⇒ 'Task editor' on page 49.

☒ **Utilities**

This tool lets you view and edit task files, quarantined files, and displays status for installed components.

⇒ 'Utilities' on page 55.

☒ **Internet update**

Use this tool to download the latest version of NVC automatically. Internet update can be configured to download updates at scheduled intervals.

⇒ 'Norman Internet Update' on page 62.

☒ **Release notes**

Presents useful information in web browser format about the current release, including links to downloading areas, etc.

Language:

Select which language version of the components you want from the pull-down menu. Click on the arrow to display available languages. This list is subject to change as new language versions are included.

Start

You can choose to start some of the components automatically, i.e. they are loaded when you start your computer. Some components are by definition not intended to start automatically, such as the On-demand scanner.

On the other hand, the On-access scanner is designed to monitor your system in real-time, and the default setting is consequently ON.

You can also select automatic start for the Task scheduler.

Whenever you make a change for a component, you must click on **Save** to activate the change. A component will remain selected/deselected until you manually change and click **Save** again.

Update mode

New viruses appear every day, and Norman provides frequent updates to the virus definition files, as well as regular program updates.

You can update NVC in different ways, and the alternatives are:

Update from physical media

○ Manually from CD-ROM

Use this option when you receive a version update from Norman.

Note: When you receive the CD-ROM, the virus definition files are already outdated and replaced by newer versions on the Norman server. This is due to time spent on production and shipping. Whereas new files can be available on the web a minute after they are ready, it will take a week or two to prepare and distribute the same files on diskette/CD-ROM. *Always* check the Norman server for new virus definition files and updated software after you have installed a new program version from CD-ROM. Norman provides a tool for this purpose—Norman Internet Update (NIU). See page 62.

Update from the Internet

Note: If your machine is protected by a firewall or proxy server, you may have to enter the required information in the **Internet** tab (page 22).

The program Norman Internet Update (NIU) handles NVC updates. Updates are available as packages, and NIU decides which packages are relevant for you based on the operating system and language. The selection you make in this section affects the way NIU handles updates from the Internet.

Do not use the option **Manually from CD-ROM** if you update from the Internet.

☒ **On-demand only**

Select this option if you prefer to start NIU manually to check for updated packages.

☐ **Daily on dial-up connection (wait for connect)**

If you use a modem to connect to the Internet, select this option for daily checks for updates on Norman's servers. You just access the Internet like you normally do, and the program will figure out if updated files are available.

If you connect to the Internet several times per day, NIU checks for updates the first time you connect only. If you connect to the Internet once a week, for example, NIU will check once as soon as you're connected.

☐ **Daily on direct connection at scheduled time**

You can select this option if you have a permanent connection to the Internet. First specify when NVC should check for updates. Enter the time of the day in the **Scheduled time** field, and then use the '+'- field to allow the system a time slot to fit in the task at the most convenient time to avoid possible overloads.

Update from LAN/WAN

☐ **Automatically from server**

If you select this option, make sure that you enter the relevant information in the **Software** field in the tab **LAN/WAN**, so that the machine can locate the server where the updates are placed.

Note: You must select this option if you intend to fill in the fields in the **LAN/WAN** tab (page 23).



Internet

If you have selected updates from the Internet, Norman Internet Update (NIU) will use the information you enter in the **Internet** tab. This information is only required if your local network is protected from the Internet by a firewall.

Proxy server



Enter the address and port for the firewall's HTTP proxy.

If you have specified information for HTTP proxy in your browser, you should enter exactly the same settings here.

LAN/WAN

Note: Before you change anything in this dialog, you ***must*** refer to the instructions in the *Administrator's Guide*.



Common for these fields: from this tab the administrator can update the workstations (may include other servers) with NVC software updates, configuration, and task files. The fields in the tab represent the location from where the ***workstation*** will fetch updated software.

Where to look for updates

Software:

Identifies the server path where NVC software updates can be fetched after they are downloaded from the Internet, for example. Make sure that you have selected the option **Automatically from server** in the tab **Update mode** (page 21).

Configuration:

Where the machine looks for changes that the administrator have done to the configuration file(s).

Tasks:

Where the machine looks for changes that the administrator have done to the task file(s), for example edited existing files or added new task files.

⇒ 'Task editor' on page 49 and 'About the scheduler' on page 54.

Authentication

Like all virus control applications, NVC is perpetually updated because new viruses are added to the virus definition files, or viruses of a nature that require software changes occur. You will need to confirm your licensing information before you're allowed to install and/or update NVC.

Serial number

The serial number that you received when you purchased NVC, and that you typed in during installation.

The number appears in this field and contains license information that enables you to use NVC in accordance with the licensing agreement.

Server logon



Note: Before you change anything in this dialog, you *must* refer to the instructions in the *Administrator's Guide*.

This section is only displayed in a network environment.

Account:

Enter an account name in accordance with the syntax required by the operating system you're running.

Password:

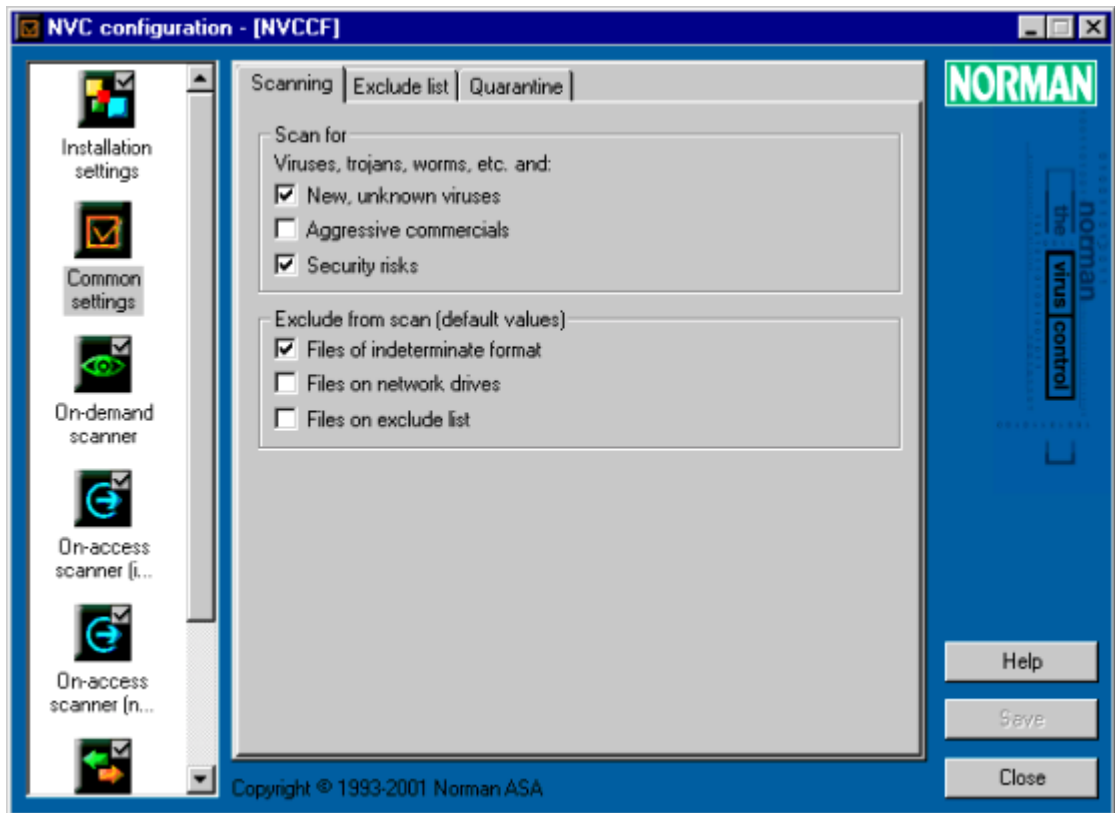
Enter a password for the account.

NDS tree:

Enter the name of the NDS tree.

Common settings

Common settings primarily affect malware handling, including detection and cleaning, and this module is consequently a supplement to the scanning modules *On-demand* on page 30, *On-access (interactive)* on page 33, and *On-access (non-interactive)* on page 37.



Scanning

Scan for

NVC scans for viruses, trojans, worms, and other malicious code or unwanted programs that can harm your PC.

In addition, you can instruct NVC to scan for:

☒ **New, unknown viruses**

NVC employs heuristic methods to detect new, unknown viruses. Select this option if you want NVC to look out for new virus variants. Note that this option may induce false alarms. In that case, you should clear this option temporarily until the problem has been taken care of.

☐ **Aggressive commercials**

Sometimes unwanted programs are attached to programs that you download from the Internet for evaluation purposes, for example. They do not inform you about their presence, and if you uninstall the original program, the hidden program may still be on your machine. It is hard to find and has no uninstall procedure. At odd intervals these programs will log on to the Internet and download commercials all by themselves. They are not harmful like a traditional virus, but it is annoying and creates unnecessary network traffic. NVC can detect and remove such programs. Note that free software that you have installed may not work when this option is selected.

☐ **Security risks**

This option instructs NVC to scan for objects that represent a possible security risk. Some administrators have installed programs like password crackers and remote administrative tools that are perfectly legal and probably useful too. However, the lack of security features in some of these tools can expose machines to unauthorized users and crackers. NVC detects the activity of such tools and will warn against potential security risks. Warnings will report the name of the program, and you can therefore decide if it is a legitimate program or cracker activity that triggers the alarm.

Exclude from scan (default values)

You may want to speed up the scanning process by excluding certain files from scanning. Note that excluding files or areas from scanning is a decision at the expense of security.

NVC employs the following settings during all scans (On-demand and On-access). Use the **Exclude list** tab to specify files that you do not want to scan.

☒ **Files of indeterminate format**

Select this option to instruct NVC to skip files of indeterminate format. Such files are most likely files with an unknown format.

☐ **Files on network drives**

In networks, not all users are allowed to scan files on the server. Select this option if you are only permitted to scan files located on the workstation.



❑ Files on Exclude list

In certain situations, you may want to include the files that are currently on the Exclude list. If you clear this option, the Exclude list is disabled. Since file exclusion affects security in a negative way, we recommend that you consider carefully the files you put on the list. Files that are time-consuming to scan, or that cause false alarms may be placed on the Exclude list.

⇒ ‘Exclude list’ on page 27,

Exclude list

Note well: Exclude lists should be handled with great care, as they represent a potential security risk. We recommend that you scan the Exclude list manually (using the On-demand scanner) on a regular basis, and also include these files or areas in scheduled scans.

Specify files, directories, or entire drives that you don’t want NVC to scan. Follow these steps to exclude items from being scanned:

1. Click on the **Add** button enter a file, directory, or drive letter. Wildcards (* and ?) are accepted.

Examples:

`c:\dir`

Excludes all files in the directory, including subdirectories

`*.xyz`

Excludes all files with the extension .xyz

`c:\dir*.xyz`

Excludes all files with this extension in the directory.

`example.exe`

Excludes the specified file regardless of where it’s found.

`c:\winnt\system32\xyz.sys`

Excludes this particular file.

Note: Do *not* use apostrophes (“ or ‘) when you specify items for exclusion.

2. Use the **Comment** field to type in optional explanatory text for the different entries. We recommend that you revise the Exclude list regularly. During revision it's useful to be reminded of the reason for excluding an item from scanning.
3. To change an existing entry, highlight it and click on **Edit** or **Remove**.
4. Click on **Save** when you're done.

Quarantine

From this tab you decide how to handle files that NVC has identified as infected or in other ways suspicious. If you don't clean or delete such files, we recommended that you isolate them to a designated area, a quarantine.

Properties

Minimum time to keep file in quarantine:

Specify a period ranging from one day to one week. Files newer than the specified minimum time will never be deleted.

Maximum time to keep file in quarantine:

Specify a period ranging from one to four weeks. Files older than the specified maximum time are deleted without warning.

Maximum size of quarantine (% of partition size):

Specify how much disk space of the current partition quarantined files are allowed to occupy. The maximum size can be exceeded in the case quarantined files have yet to reach their specified *minimum time*.

Options

☒ **Back up files to quarantine before repair**

Before NVC repairs an infected file, you can back it up. In general, repairing a file represents a minor risk.

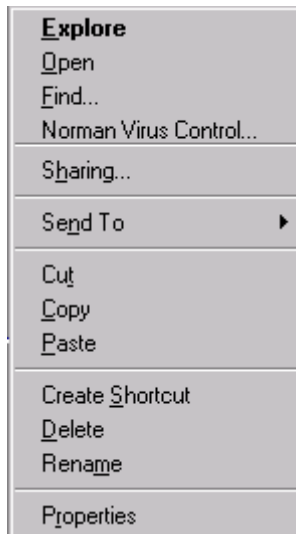
☐ **Move unrepairable files to quarantine**

If NVC cannot repair a file, you can choose to move infected files to the quarantine area.

For security reasons, NVC may move unrepairable files to quarantine regardless of your selections.

Note: Regardless of what you choose, NVC will move unrepairable files to quarantine if you have selected **Scan new or changed files** in the On-access scanner (non-interactive) module (page 37). The reason is that the option of scanning new and changed files represents a strategy that requires a virus free environment. When repair fails, the infected file is therefore not permitted to reside on the machine.

On-demand scanner



The On-demand scanner is frequently referred to as the Right-click scanner, because that's what you do when you use it: select one or more file system object(s) and click on the right mouse button to launch the scanner: The purpose of the On-demand scanner is to make periodic inspections of selected areas on your system. The scanner has its own entry on the menu that pops up when you place the cursor on file system objects such as disks, directories, and files and click on the right mouse button.

Many users consider virus scanning a necessary evil. We believe that the easier virus scanning becomes, the more often it will be performed. The On-demand scanner does not require double-clicking an icon or running an executable file. You simply select the area(s) you want to scan from Windows Explorer or OS/2's desktop, for example, and then *Norman Virus Control* from the right-click menu.

The On-demand scanner will use the settings you specify under Common settings 'Scanning' on page 25 and 'On-demand scanner' on page 30.

The On-demand scanner can detect and remove all types of viruses automatically, except for boot sector viruses on hard drives.

⇒ 'Cleaning infected files' on page 67.

Diagnostics

When the on-demand scanner has completed the scan of the selected area(s), all relevant information appears in the scanning dialog. There are separate entries for infected files and for files that could not be scanned. The ***Diagnostics*** field advises you

why NVC couldn't scan a particular file. The most common reasons are:

Diagnostic	Explanation
Access denied	The file is most likely in use and unavailable for scanning.
Damaged file	NVC didn't recognize the format of the file, which is probably damaged.
Error opening archive	NVC encountered an error when trying to open the archive for scan.
Sharing violation	The file is being used by another application.
Password protected file	NVC cannot scan password protected files.
Password protected archive	NVC cannot scan password protected archives.
Damaged archive	NVC didn't recognize the format of the archive, which is probably damaged.
I/O error	I/O errors occur in different situations, e.g. when a file is damaged in a way that NVC cannot handle in a scan, or files that reside on damaged floppies.

Scanning

See also the tabbed dialog box 'Common settings' on page 24 for basic configuration of the On-demand scanner. These settings are your primary scanning options, and the ones that will be used if you choose the default value in this dialog box.

If you have a temporary need for scanning with a different set of options, this tab allows you to do so.

Exclude from scan

You may want to speed up the scanning process by excluding certain files from scanning. Note that excluding files or areas from scanning is a decision at the expense of security.

☉ **Use default values (from Common settings)**

This instructs NVC to employ the basic settings specified in the **Common settings** module.

○ **Specify files to exclude from scan**

Note that by selecting this option, you will overrule the default settings, and activate the following three options:

☐ **Files of indeterminate format**

Select this option to instruct NVC to skip files of indeterminate format. Such files may be damaged files, or files with an unknown format.

☐ **Files on network drives**

In networks, you may not allow all users to scan files on the server. Select this option if you are only permitted to scan files located on the workstation.

☐ **Files on Exclude list**

Select this option if you want to activate the Exclude list. We don't recommend that you select this option, because the files on the Exclude list should be scanned regularly.



About On-access scanning on Windows NT/2000

The on-access scanner options for this platform are divided into two different modules; *Interactive* and *Non-interactive*. Under normal circumstances, a workstation runs in Interactive mode, while a server runs in Non-interactive mode. In any case, you should configure both modules to cover the different roles that Windows NT/2000 can play. This is how these roles are defined with regard to scanning in NVC:

Interactive:

Virus control for a logged on user, which includes everything that the user does on the local machine. If the user is logged off or the machine acts like a server, the non-interactive mode applies.

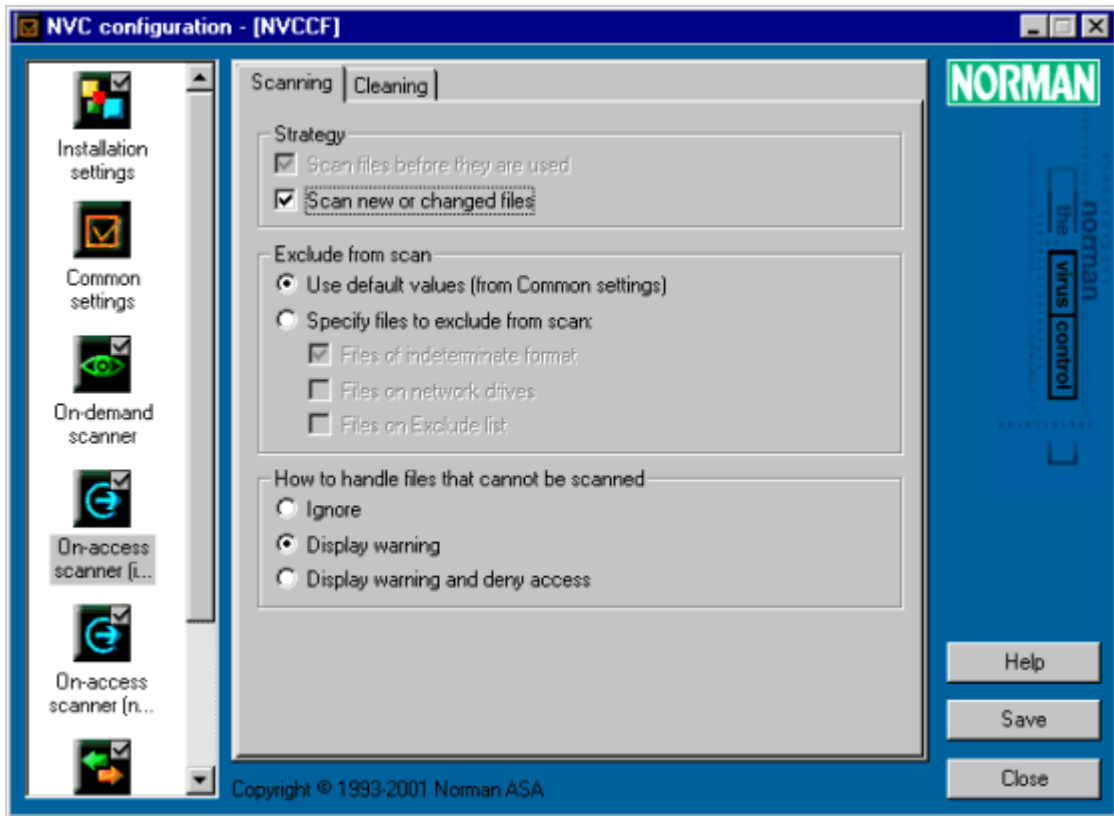
Non-interactive:

All other activity that takes place on the logged on machine, such as access from other machines to directories that are shared out on the logged on computer. Non-interactive mode applies to any NT/2000 machine that is logged off.

The typical scenario is that non-interactive activity takes place on the server. However, if someone physically logs on the server, the interactive mode applies.

On-access scanner (interactive)

Note: These settings apply to workstations running Windows 95/98/ME, Windows NT 4.0/2000, and OS/2 acting as *workstations*. See *Interactive* and *Non-interactive* mode above.



On-access scanning involves constant monitoring of the file system. For an anti-virus application, it's imperative to detect and block a virus before it's activated. In on-access scanning, NVC is communicating with the operating system at a low level and enables the scanner to "see" all activities on the system. This process gives NVC a head-start versus the virus and allows NVC to take immediate action.

Whenever a file is accessed in a read/write operation or a program is executed, the On-access scanner is notified and scans the file on the fly.

Like the On-demand scanner, NVC's On-access scanner detects and repairs all types of viruses. Whenever possible, an infected file is repaired before the file is handed over to the application. If repair fails, NVC denies access to the infected file.

⇒ ‘Cleaning infected files’ on page 67.

Scanning

Strategy

If you don't want NVC to scan all files that are accessed, you can do so by selecting a scanning strategy. Regardless of the strategy you select, NVC will monitor your system in real-time.

Note that when you open a document with a macro virus, the macro is executed and therefore scanned by NVC.

☐ **Scan files before they are used**

This option instructs NVC to scan files that are opened for read/execute, and it is mandatory for security reasons.

☒ **Scan new or changed files**

If you don't want the presence of viruses on your machine, not even dormant ones, you should select this option. You should scan the entire hard drive(s) and remove possible viruses before you select this option.

Exclude from scan

You may want to speed up the scanning process by excluding certain files from scanning. Note that excluding files or areas from scanning is a decision at the expense of security.

There are two mutually exclusive option buttons in this section.

☒ **Use default values (from Common settings)**

Instructs NVC to use the basic settings specified in the **Common settings** module.

☐ **Specify files to exclude from scan**

When you select this option, the following alternatives are available to make the On-access scanner more efficient and save system resources. Because file exclusion represents a possible security risk, you should be careful which files you exclude from scanning.

☐ **Files of indeterminate format**

Select this option to instruct NVC to skip files of indeterminate format. Such files may be damaged files, or



files with an unknown format.

☐ **Files on network drives**

In networks not all users are allowed to scan files on the server. Select this option if you are only permitted to scan files located on the workstation.

☐ **Files on Exclude list**

Files on the Exclude list are not scanned. We do not recommend that you select this option, because files on the Exclude list should be scanned regularly. Reasons for not scanning certain files may be that they trigger false alarms, or they are too time-consuming to scan.

How to handle files that cannot be scanned

In some situations NVC is unable to scan a file. Examples are Word 8 files with password protection, damaged files, or when internal system errors occur. There are three available options for how NVC can treat files that cannot be scanned:

☐ **Ignore**

NVC will not warn about files that elude scanning.

☒ **Display warning**

NVC warns when you access a file to inform you that this file has not been checked. You may, however, proceed at your own risk.

☐ **Display warning and deny access**

NVC warns that access is denied because the file could not be scanned.

For network environments:



The Access field at the bottom of each tab is invisible unless you have administrator's rights. The system administrator decides what should be visible and/or configurable from the workstations. The average user may therefore view all or some of the tabs, but is not necessarily entitled to change the settings.

Cleaning

When viruses, trojans, worms, or other malware are detected, you can select how NVC should treat them.

☐ Deny access

If you try to run an infected program, access is denied. Infected documents are blocked.

☐ Remove

NVC will try to remove the virus from the infected file. Select this option to instruct NVC to repair infected files automatically. NVC can remove most viruses on the fly, except for boot sector viruses. NVC will always prompt for user intervention before boot sector viruses are removed. Note that a file is deleted altogether if it contains nothing but malware.

☐ Ask user what to do

If you neither want automatic removal of viruses nor denied access for infected files, you can check this option. When you try to open an infected file, you'll receive information about the incident. From the dialog that appears, you can choose between removal and exit.

On-access scanner (non-interactive)

Note: This module is available on Windows NT/2000 and OS/2 machines only.

Strategy

If you don't want NVC to scan all files that are accessed, you can do so by selecting a scanning strategy. Regardless of the strategy you select, NVC will monitor your system in real-time.

However, you can decide that NVC should scan a file only when it's handled in such a way that a possible virus can be activated. A file that contains a virus is no threat if it is opened for write only. You may not want to check files that cannot activate possible viruses due to the way they are treated by the system.

☐ **Scan files before they are used**

This option instructs NVC to avoid scanning of files that are opened for write. Even if the file contains a virus, the virus will not be activated in an open for write operation. When the same file is opened for read, however, it will be scanned. The reason is that a possible virus will be activated in this situation.

Scanning time increases when this option is selected.

☒ **Scan new or changed files**

If you have zero tolerance for viruses on your machine, even dormant ones, you should select this option. All changed and new files will be scanned. Remember to scan the entire hard drive(s) and remove possible viruses before you select this option.

Scanning time is reduced when this option is selected.

IMPORTANT

If you only have selected the option **Scan new or changed files**, you have selected a strategy that relies on a clean server. Theoretically, an infected file can be copied to server where cleaning *fails* for some reason. The presence of an infected file is in conflict with the zero tolerance for viruses. Consequently NVC moves the infected file to quarantine--even if you haven't selected **Move unrepairable file to quarantine** (see 'Quarantine' on page 28).

Exclude from scan

You may want to speed up the scanning process by excluding certain files from scanning. Note that excluding files or areas from scanning is a decision at the expense of security.

By default, NVC scans files of certain types, for example .exe, .com, and .doc. All critical file types are listed, including file types that we know are likely to be exposed to viruses. Refer to the Readme file for a complete list of file extensions that NVC includes in a scan. Consequently, certain files are excluded from a default scan. There are two mutually exclusive option buttons in the section Exclude from scan.

☒ **Use default values**

The on-access scanner checks all files with the file extensions listed in the Readme file. These default file extensions are updated on a regular basis.

☐ **Specify files to exclude from scan**

When you select this option, the following alternatives are available to make the on-access scanner more efficient and save system resources. Because file exclusion represents a possible security risk, you should be careful which files you exclude from scanning.

☒ **Files of indeterminate format**

Select this option to instruct NVC to skip files of indeterminate format. Such files may be files that are damaged, or with an unknown format.

☐ **Files on network drives**

In networks, you may not allow all users to scan files on the server. Select this option if you only permit scanning of files located on the workstation.

☐ **Files on exclude list**

Select this option if you want to include the exclude list. In other words, you activate the exclude list by selecting it. We do not recommend that you select this option, i.e. activate the exclude list, because files on this list should be scanned regularly.



Cleaning

How to handle viruses, trojans, worms, etc.

When viruses, trojans, worms, or other malware are detected, you can select how NVC should treat them.

☐ **Deny access**

If you try to run an infected program, access is denied. Infected documents are also blocked.

☒ **Remove**

NVC will try to remove malicious code. Select this option to instruct NVC to repair infected files automatically. NVC can

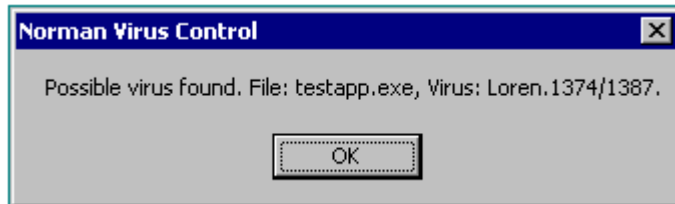
remove most viruses on-the-fly, except for boot sector viruses. NVC will always prompt for user intervention before boot sector viruses are removed.

NVC on Windows Terminal Server

In a Windows NT or Windows 2000 terminal services environment users may be connected to the server via terminal services clients. Using this configuration, the terminal services clients do not run applications locally, but instead they depend on the server to run instances of the applications they use. The server distributes screen layout to each user that logs on and runs applications on behalf of the user.

This design simplifies the administrator's maintenance of files and applications in an environment of multiple users. NVC adds value to the design by making it easy for an administrator to configure NVC accordingly.

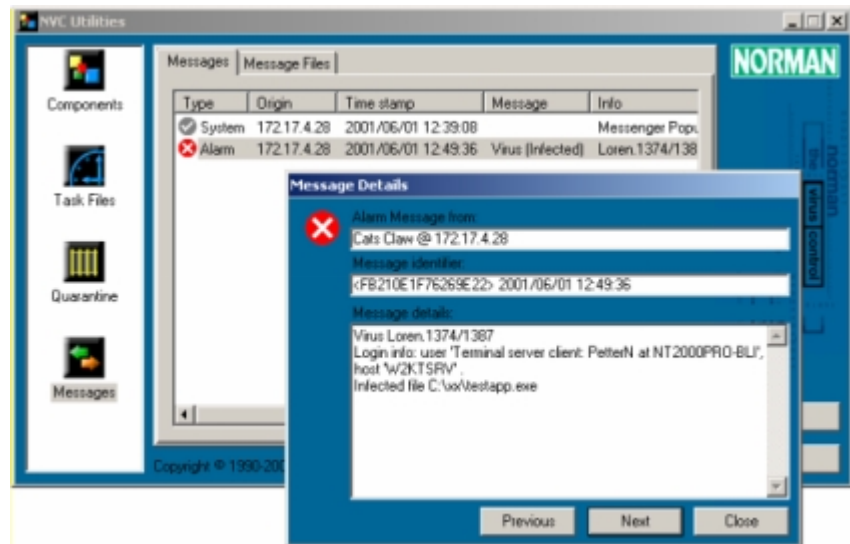
During on-access scanning for Terminal server client sessions, NVC will always use the "non-interactive" (or server) configuration. This means that no virus alert dialog box will appear on the Terminal server when a virus is found. On the Terminal server client's machine however, a message box like this will appear:



This message is purely informational. The terminal server client is not allowed to change the behavior or the configuration of the scanner.

Note that scan of changed or new files only is the default setup for the "non-interactive" configuration. Files read or executed from a terminal server client are therefore not affected by on-access scanning.

On the administrator's NVC Messages console the following message has been added:



The name of the logged on terminal client as well as the terminal client's machine is added to the virus alert message. In the example above the user PetterN on the machine NT2000PRO-BLI caused the virus alert message on the terminal server W2KTSRV.

NVC on-demand scanning is still possible from each terminal session. The functionality in this respect is no different from on-demand scanning on any other configuration.

About messages and logging

Messaging is made up from three modules: **Message routing**, **Message handling**, and **E-mail, SMS, SNMP**.

Note: The **E-mail, SMS, SNMP** module is currently available as a beta version only. It is scheduled for release in third quarter 2001.

Message routing allows administrators to select what kind of messages that will be routed to other PCs running NVC in the network. Please refer to the chapter “Messaging” in the *Administrator’s Guide* for a detailed technical description of the messaging system.

Message handling allows users as well as administrators to select what kind of messages that are displayed or kept locally. The messaging functionality is an effective way of keeping track of all activity related to the NVC components locally as well as in the network.

You may not have access to the network at all times, but the **E-mail, SMS, SNMP** module allows administrators as well as single users to be notified by e-mail or SMS messages when certain incidents occur on workstations or servers.

You should use the messaging tool to determine which incidents you wish to be warned about.

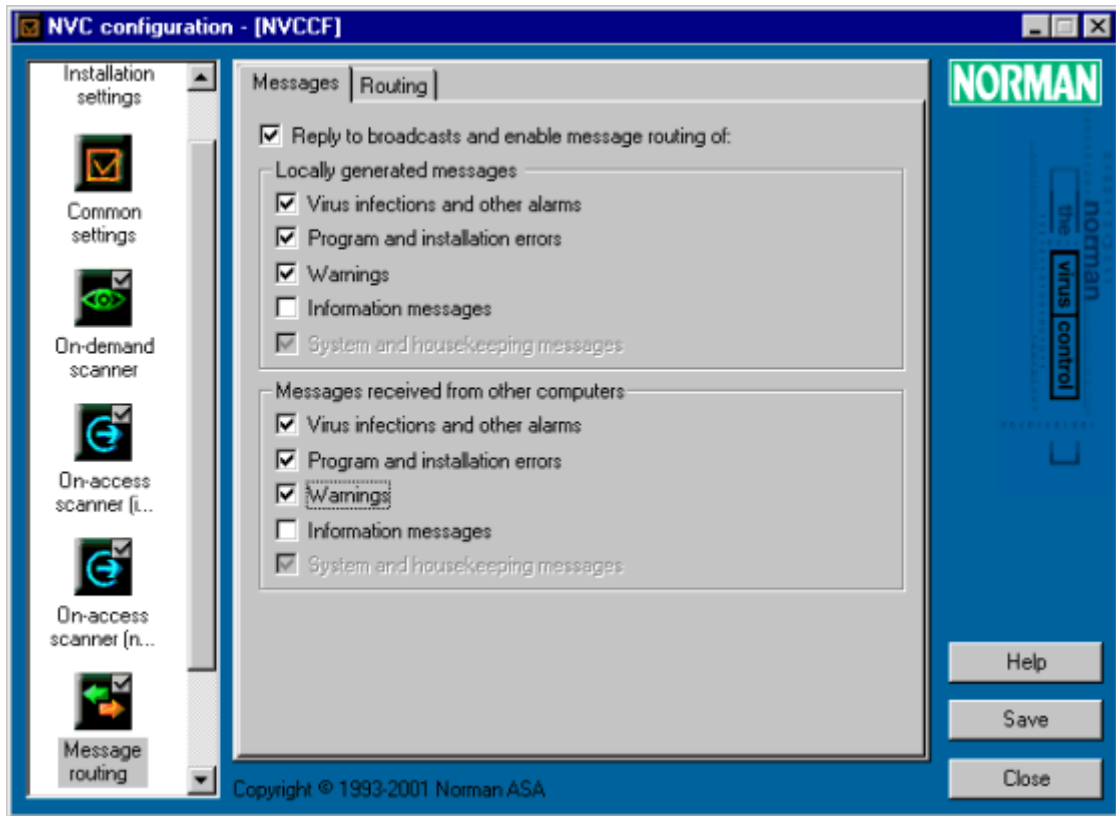
The traditional way of logging is to write messages to a log file. In NVC v5, this functionality is taken care of by one of the standard output modules that are loaded by the agent. Accordingly, messages received by the agent are passed on to the log file output module, **Messages** in the **Utilities** group (page 58). This is the only tool for viewing the log file.

Message routing



Note: This module is only available in a network installation.

Messages



This output module for messages supports IP as well as IPX networks. It is connection-based, using TCP/IP and/or SPX.

Note: Refer to the *Administrator's Guide* for detailed information on how NVC handles messages and alarms.

☒ Reply to broadcasts and enable message routing of:

You must select this option to get access to the remaining options in this dialog. If you clear this check mark, you have turned the message router off.

Broadcasting is to simultaneously send the same message to multiple recipients.

Locally generated messages

Select which incidents that occur on the **local** machine that the message router should pass on.

☒ **Virus infections and other alarms**

Forward message if virus or other harmful code is detected.

☒ **Program and installation errors**

Forward message if an installed NVC program reports an error, or if there are error messages during installation of NVC.

☒ **Warnings**

Forward warnings that appear.

☐ **Information messages**

Forward message of an informative nature.

☒ **System and housekeeping messages**

Forward messages regarding network related activities on the system. This option is always on.

Messages received from other computers

In the previous section you selected which incidents that occurred on the **local** machine that should be sent. In this section you can decide which messages of incidents on **other** computers that you want the message router to pass on.

You can select from exactly the same set of options as in the previous section.

Routing

If you enabled message routing, specify the receiver(s) of the messages here.

Forward incoming messages to:

Click on **Add** and enter the address and name of the receiver. You must repeat the operation for each recipient you wish to add to the list. Names and addresses can be edited or removed from the list by clicking on the appropriate buttons.

Normally only one receiver should be specified in order to avoid message duplication. Refer to the *Administrator's Guide* for further details.

☒ **Forward messages**

Select this option to send incoming messages to the member(s) on the list. You can also select when incoming messages expire, where the options are 1, 8, or 24 hours, 1 or 4 weeks, or never. The default value is 1 week.

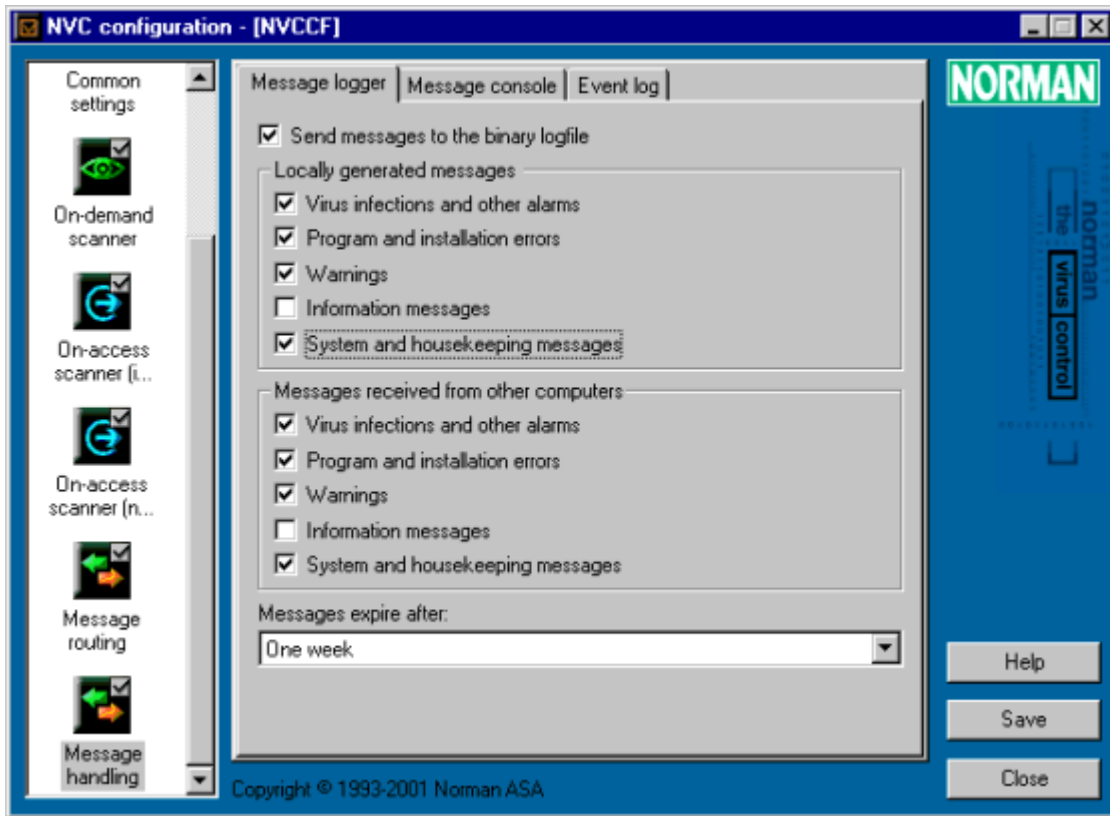
Message handling

Message handling selects messages to a log file, displays messages on a message console, and decides what should go into the Event Log in Windows NT/2000. Therefore there are three tabs with identical options in this dialog. The selections you make decide which entries that appear in the NVC log file, on the message console, and in the Event Log in Windows NT/2000.

NVC stores messages in the *system error log*.



Message logger



☒ Send messages to the binary log file

You must select this option to get access to the remaining options in this dialog. If you clear this check mark, you have turned the message logger off.

Note: The log file is encrypted and can only be viewed from the Utilities module (the Messages component). See page 58.

Locally generated messages

The selections you make in this section decide which incidents that occur on the *local* machine that appear as entries in the log file.

☒ **Virus infections and other alarms**

Create log file entries of virus detection or if other harmful code is found.

☒ **Program and installation errors**

Create log file entries of an installed NVC program that reports an error, and if there are error messages during installation of NVC.

☒ **Warnings**

Create log file entries of warnings that appear. Examples of warnings are:.

☐ **Information messages**

Create log file entries of messages of an informative nature. Examples of information messages are:...

☒ **System and housekeeping messages**

Create log file entries regarding network related activities on the system. This option is always on.

Messages received from other computers

In the previous section you selected which incidents that occurred on the *local* machine that should be entered in the log file. In this section you decide which messages of incidents on *other* computers that you wish to store in the log file.

You can select from exactly the same set of options as in the previous section.

Messages expire after:

Select for how long you wish to keep messages in the log file. You can choose to let messages expire after one day, two days, one week, one month, or never.

Message console

You must select

☒ **Send messages to the message console**

in order to access the configuration options, which are identical to those discussed in the “Message logger” section, starting on page 46.

Messages expire after:

Specify how long you wish to keep messages on the console.

You can choose to let messages expire after one hour, eight hours, one day, two days, one week, one month, or never.

The message console is located in the module **Utilities** (page 55).

Event Log

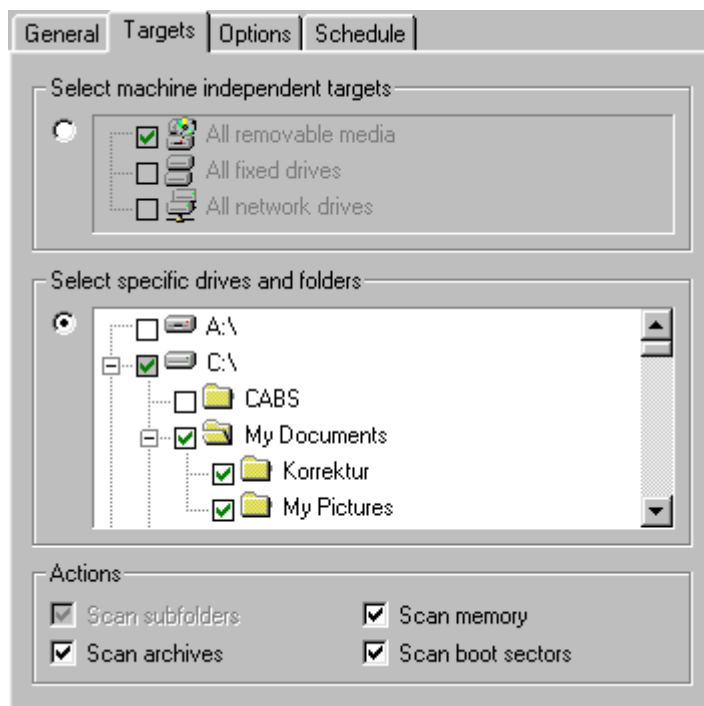
You must select

☒ **Send messages to the Win NT/2000 Event Log**

in order to access the configuration options, which are identical to those discussed in the “Message logger” section, starting on page 46.

Task editor

Sometimes it's convenient to define tasks that should be performed several times and/or at regular intervals. Scanning for viruses is a good example of a task that needs to be carried out regularly, and the Task editor is the tool NVC provides for that purpose.



You can create a task file for scans that you wish to perform on a regular basis, or special scans that you intend to run in certain situations. For example, if you download files from the Internet to designated areas, you can create a task file that scans these areas only and run the task manually after downloads. In addition, you can schedule the task to run at a preselected time.

Administrators can create task files and distribute them to all workstations in the network to ensure consistent checking of areas that require special attention.

The default location for storing task files is `... \nvc\tasks`. You can view, edit, run, and delete your task files from NVC Utilities (see page 55).

The following sections describe the four tabs in the **Task Editor**.

General

From the tab **General**, use the **Description** box to enter a short description of the task. If you create several tasks, it may be helpful at a later stage to see why you created this particular task at the time, for example it may have been spurred by a particular incident.

From **Utilities|Task files** you can view the complete list of existing task files.

⇒ ‘Utilities’ on page 55.

Targets

In this tab you can specify which areas you wish to scan, and how the scan should be performed and save your selections in a Task file.

There are two sections in this tab; the first for larger entities like multiple hard drives, and the second for more specific scanning targets.

Within a single task file, you cannot combine a selection from the first section with one from the second. For example, you cannot select all removable media and a specific folder on a hard drive.

Selecting targets

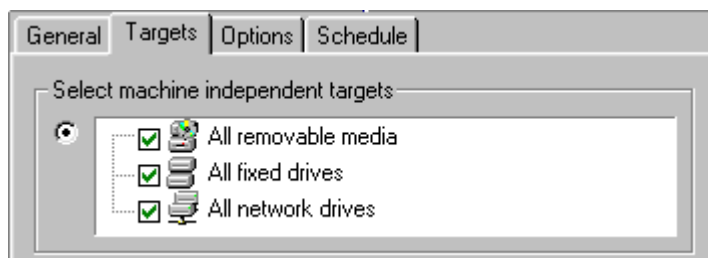
For both sections in this tab, this is the procedure you should follow to include areas for scans and save your selection(s) in a task file:

1. Click on the radio button ☒ to activate the section you wish to select from.
2. Click on the areas you wish to include in the scan. You can add several areas for scanning within each section.
3. If you select specific drives and folders, all subfolders under the selected drive/folder are automatically selected. You can clear the option for subfolders that you don't want to include.
4. When you are done, click on **Save** to store your selections in a task file. By default the task file is stored in
... \nvc\tasks.

Note: If you schedule a task file, it **must** be located in the directory ... \nvc\tasks.

5. To change an existing task file, click **Open** and select the file from the Open file dialog. Make the desired changes and click on **Save**.

Select machine independent targets



You can choose one, two, or all options in a single task file.

☒ **All removable media**

Selects all floppy drives, CD-ROM drives, and other removable media drives available on your system.

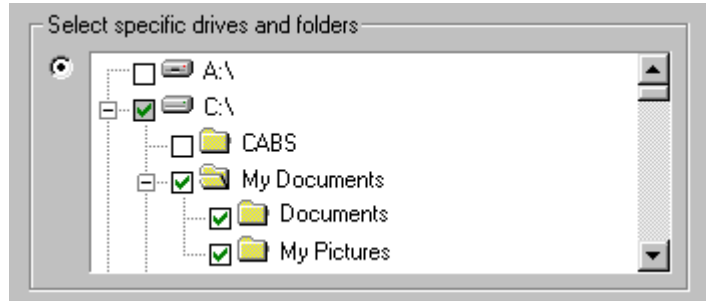
☒ **All fixed drives**

Selects all local hard drives on your system.

☒ **All network drives**

Selects all network drives known to your system.

Select specific drives and folders



When you select a drive, for example, all folders and subfolders under the drive are automatically selected for scan. Similarly, if you select a folder or subfolder, all folders below the selected one are included. To exclude a subfolder from scanning, click on it to deselect it.

Common scanning options

At the bottom of the page, there is a common set of scanning options located under Actions:

☒ **Scan subfolders**

If you have selected one or more drives or directories, select this option to include subdirectories in the scan.

☒ **Scan archives**

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

☒ **Scan memory**

When you scan the memory area, NVC looks for resident viruses. You should always make sure that no viruses exist in memory.

☒ **Scan boot sectors**

When you select this option, NVC will check the boot sector of the area(s) that are being scanned.

Options

Use this tab to decide how visible NVC should be during a scan, and how much system resources you want to allocate to NVC.

Scanner window:

☐ **Hidden until cleaning fails**

Instructs NVC to work in invisible mode. NVC will appear only if a virus that cannot be cleaned is found. Note that it is cumbersome to cancel a task that runs in hidden mode. This might serve as a useful hint for an administrator who wants scheduled tasks to run as planned, and as a warning to single-users who might find it hard to cancel an ongoing scan. A scheduled task starts automatically if this option is selected.

☐ **Minimized until cleaning fails**

Instructs NVC to work in a minimized window. NVC will appear only if a virus that cannot be cleaned is found. A scheduled task starts automatically if this option is selected.

☒ **Minimized until infection found**

Instructs NVC to work in a minimized window. NVC will appear only if a virus is found. A scheduled task starts automatically if this option is selected.

☐ **Open**

Instructs NVC to run in an open window during scanning. When you schedule a scan with the **Open** option on, the scanning dialog appears at the scheduled time and you must start it *manually* by clicking on **Scan**.

Resource usage:

Under normal operating conditions, a computer rarely runs so low on internal resources that the operating system is forced to put tasks on a priority list. If such a situation should arise, a task from NVC will have to wait for system resources to be freed up before it can be performed if you select **Low**, while **Normal** will place the NVC task among any other task waiting to be executed.

Note that the effect of selecting **Low** rather than **Normal** will vary depending on the operating system you're running.

Schedule

When you have set up a task file using the tabs discussed in this chapter, you may want to schedule a task for repetitive scans on your machine.

☒ **Scheduled task**

Make sure that you select this option if you wish to use the scheduler. The two requirements for a scheduled task to run are: 1) The **Scheduled task** option must be checked, and 2) The task file must reside in the directory `... \nvc\tasks`.

Frequency

The next step is to decide when the task should be run, and you can choose from different intervals, ranging from **Once** to **Every month**.

Start date/time:

Specify the day/month/year the scheduled task should be run for the first time. Use the keyboard arrow keys (or click the arrows in the box) to change the date. You can highlight date, month, and year and change the values by pressing the keys. The day of the week will automatically change according to the selected date.

☐ **Universal Time Coordinates (UTC)**

This option is for companies with offices all over the world that want to perform simultaneous scans regardless of local time.

About the scheduler



The scheduler's primary objective is to run task files at a specified time. A task file can be scheduled to run daily, weekly, monthly, or just once. You must enter start date and time, and the default values are the current date and time.

For companies with offices in different time zones, the Universal Time Coordinates (UTC) feature permits a task to be run concurrently regardless of time zones.

The scheduler will always look in the subdirectory "Tasks" for scheduled jobs, and it is therefore necessary to keep the structure `... \nvc\tasks` in order to perform a scheduled task.

Utilities

NVC utilities is a tool that presents an overview of the current state of affairs for the NVC components on your PC. In addition to viewing key information, you can change certain elements by selecting some of the entries, for example task files. Other functions, like components, provide information only and cannot be edited from the Utilities module.

In this version the utilities module is made up from four major categories:

- Components
- Task files
- Quarantine
- Messages

Components

At installation time, you have a number of components to choose from. This dialog box provides a list of installed components with corresponding information.

The **Components** dialog box displays a list of all installed NVC components, including information on version number, time stamp (date and time the component was created by Norman), and the current state for each component. The latter indicates if the component is running.

This dialog box is purely informational. You cannot remove, stop, or change the installed components in any way. To add or remove components, go to the **Installation settings** module (see page 18).

Fields in the Components dialog box:

Component

Displays the name of the installed component.

Version

Displays the version number.

Time stamp

Displays the day, month, and time the component was created by Norman.

State

Displays status for the component. Possible states are: Installed, Copied deferred, Copying files, and Archive found.

Task files

When you create a task file using the NVC Task editor, the file is by default stored in `... \nvc\tasks`.

Note: If you want to schedule a task, the task file must be located in this directory.

You can for example use Windows Explorer or the Task editor to view this directory. However, the most flexible tool is the current dialog box, that allows you to view, edit, create, and open task files in different ways. In addition, you will find the status for all your task files in one single dialog box.

Fields in the Task files dialog box

Task file

Displays the name of the task file.

Schedule

Displays if the task file has been scheduled and at which intervals.

Next run time

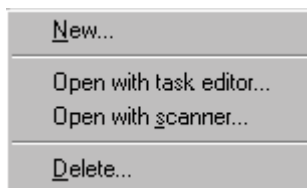
Displays at which day, month, and time the task file will run next. If the task is not scheduled, this field is empty.

Last run time

Displays the last time the Task file was successfully ran. If the task is not scheduled, this field is empty.

Right-click options

You can highlight one entry at the time, click on the right mouse button, and choose from this menu:

**New**

Opens the Task editor where you can create a new task file.

Open with task editor

Opens the task file in the task editor. Allows you to make changes to the current file.

Open with scanner

Opens the task file in the scanner. Allows you to run the selected task file immediately.

Delete

Deletes the selected file.

Quarantine

If you have enabled the quarantine options in the module Common settings ('Quarantine' on page 28), files that qualify for quarantine will appear as a list in this dialog box. These files are either infected or have an unknown format.

Fields in the Quarantine dialog box**Quarantined file**

Displays path and file name of the quarantined file.

Date

Displays the date the file was placed in quarantine.

Size

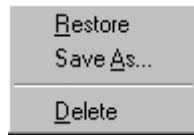
Displays the size of the quarantined file.

Diagnostic

Displays status for the file. Possible diagnostics are: Infected, Unknown.

Right-click options

You can highlight one entry at the time, click on the right mouse button, and choose from this menu:



Restore

Will restore the file to its original shape in the original folder.

Save As

Save the file with the name and location you wish.

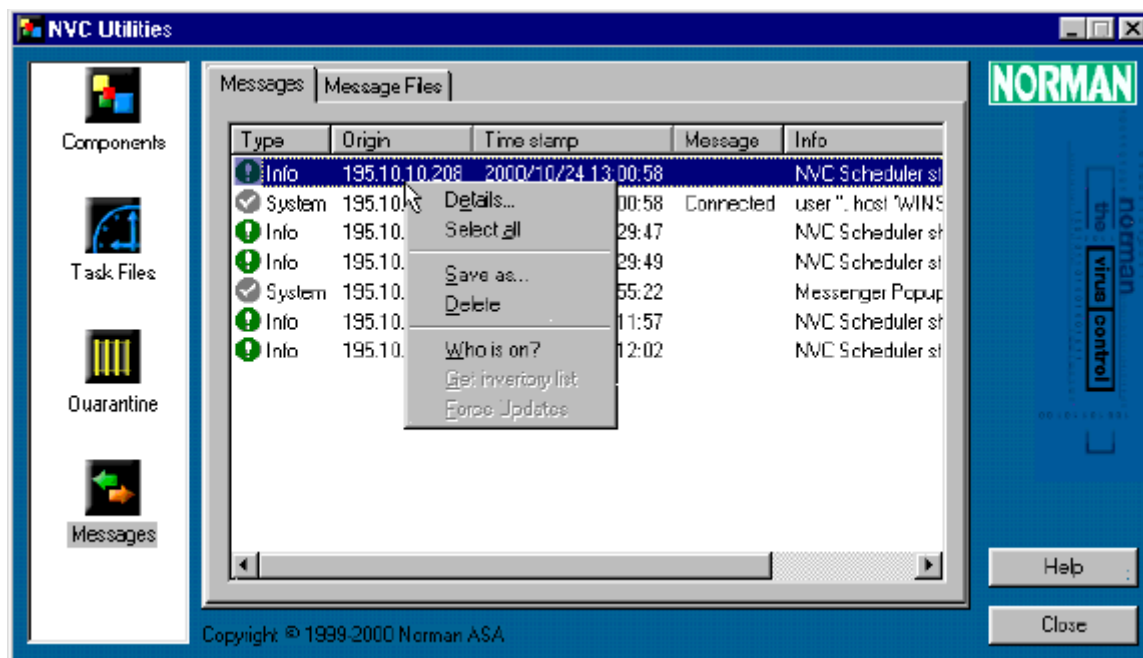
Delete

Deletes the file altogether.

Messages

Messages tab

If you have enabled the message service (see ‘Message logger’ on page 46), the message types you selected there are displayed in this tab. You can view and edit these messages from here. Select an entry in the list and click the right mouse button:



Fields in the Messages tab

Type

Description of the message type/category accompanied with an icon indicating type/severity. The entries that might appear are the type of messages specified in the Message logger.

Origin

The IP address of the machine that generated the message.

Time stamp

Year/month/day and hour/minute/second the incident that triggered the message occurred.

Message

Key word related to the incident, for example "Virus", "Connected", etc.

Info

Descriptive text about the message entry.

Right-click options:**Details**

Displays a dialog box with information about where the message originated, a message identifier, and a text box for further information.

Select all

Selects all files for saving or viewing details, deleting, etc.

Save as

Saves one or more entries with whatever name you like. If you save one or more entries, you can access them at any time from the next tab, **Message files**. Saved message entries are assigned the file extension .nps.

Delete

Deletes the entry.

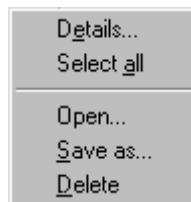
Who is on?

Broadcasts the message.

Message files tab

If you have saved one or multiple message entries as files with the **Save as** function in the **Messages** tab, you must open them in the **Message files** tab.

The fields in the tab are identical to those in the **Messages** tab.

Right-click options

The right-click options are identical to those in the **Messages** tab, except for:

Open

Place the cursor in the empty text box, right-click and select **Open** to display the Open file dialog box. You will see all saved files (file type .nps) in the default directory
... \norman\msg.

Updating NVC

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

For those who don't update NVC by letting the agent distribute updates in a local network, Norman Internet Update (NIU) is the alternative method. NIU is a program that ensures that you are running the current version of NVC for your platform. Any changes to NVC, such as actual program changes, bug-fixes, new scanner engine, and updated definition files are available from Norman's servers. When you run NIU, the program will compare the NVC components installed on your machine with the corresponding version on Norman's product server. If the time stamp is different, you are offered to download the updates. Theoretically, the entire program can have been changed and therefore subject to download.

NIU appears as a separate item in the Norman group.

To run NIU, you need a TCP/IP (Internet) connection.

NIU can be used by single-users for downloading updates directly to their local machine, and by administrators who download updates to a server and let the agent distribute the updated packages to all workstations in the network.

Norman Internet Update

Starting NIU

You start NIU by choosing Start|Programs|Norman Virus Control|Internet Update, or you can select **Internet Update** from the menu that appears when you click on the Norman icon in the system tray (lower right corner on the screen).

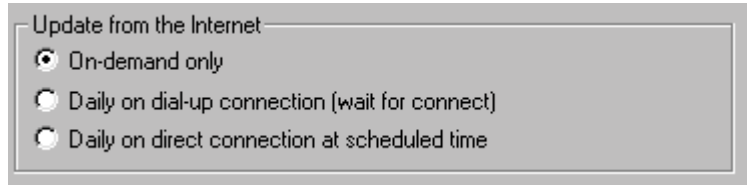


Right-click on the desktop and select *Norman Virus Control*.

NIU and Internet connection

To run NIU, you need a TCP/IP (Internet) connection.

Specify how you want to run NIU in NVC Configuration, the **Installation settings** module, **Update mode** tab. This is the NIU section of the tab:



These options are also discussed in the section ‘Update mode’ on page 21.

The option **On-demand only** is entirely based on manual action from the user. You must remember to start NIU at whatever interval you wish, and you will not be reminded to run the program. The exception is if the definition files are more than two months old.

The **Daily on dial-up connection** instructs NIU to check for updates once a day. This check is performed when you have a dial-up connection to the Internet.

If you have a direct connection to the Internet (leased line or cable modem), you can choose **Daily on direct connection at scheduled time**. This allows you to plan when NIU should run and possibly integrate NVC updates with other planned tasks.

In other words, the last two options offer an automated process for updating NVC via NIU.

Note: If the machine you are downloading to are protected by a firewall, you may have to enter the address and port for the firewall’s HTTP proxy. See ‘Internet’ on page 22.

How NIU works

Except for the **On-demand** option which is based on manual input, NIU starts in “hidden mode”, which means that you will not see anything until NIU has established that updates are available. If no updates are available, NIU exits.

In this initial phase, NIU sends the validation key to Norman’s server to verify your licence, as well as a “profile string”. The profile string contains information such as the operating system and language version on your machine, elements that determines which updates are eligible for your machine.

For administrators:



NIU also handles networks with workstations running different operating systems. When the administrator runs the program `niucf.exe` (stored in the folder `... \nvc\bin`), a file called `niucf.ndf` is created in the folder `... \nvc\config`. This file is an ordering form where all necessary information about platform, language and products is stored. NIU makes sure that everything in the file appears on the list for eligible updates, provided that your licence covers the ordered items. You must run NIUcf before you run NIU for the first time.

NIU’s activities can best be described as a three phase operation:

Phase 1:

Sends validation key and profile string to a Norman validation server. The server returns a list of packages. The packages contain NVC program code, virus definition files, or other NVC functionality.

Phase 2:

NIU checks the time stamp of a package on the product server against the corresponding time stamp of the package in the local download directory. A package on the Norman product server is considered eligible for download if the timestamp of the local package is different, or if the package is missing.

If new packages are available, a dialog appears specifying the total size of the package(s). The dialog has a timer function, and unless you select **Yes/No** within 15 seconds, downloading starts.

Phase 3:

The actual downloading of new packages to the download directory.

When downloading is completed, NIU exits and the agent takes over and updates NVC on your machine.

LAN/WAN



In a network environment, you can update the workstations by selecting **Automatically from server**.

Note that the server update option uses the information you enter in the tabbed dialog box **LAN/WAN**.

Miscellaneous on NVC

The agent

The agent deserves a more detailed explanation than the other components—partly because it’s fundamental to NVC, partly because it cannot be configured directly, it is invisible and always running.



The agent’s file name is `Zanda.exe`—short for Zero Administration Network Distribution Agent. It may not be a “true” component insofar as it’s untouchable and unnoticeable. The agent is the link between those components that need to communicate, and thus essential to NVC.

The agent resides *locally*, i.e. on the workstation or the server. When instructed by the workstation, the agent will fetch files from the server. For example, if the configuration file specifies that the workstation should look for updates at the server every day at noon, it is the agent that *picks up* the files. In addition, the agent will *send* messages from the workstation to the server.

The agent is always running.

These are some of the tasks that the agent takes care of:

- Handle NVC updates.
 - Manage all network traffic, like virus alerts, and all other message handling.
 - Ensure that the configuration is in accordance with the administrator’s requirement for the individual workstation.
 - Fetch software updates, new configuration and task files.
- ⇒ ‘LAN/WAN’ on page 23.
- Clean up the quarantine area.
 - Features its own scheduler.

About the Command line scanner

In addition to the GUI-based On-demand and On-access scanners, NVC offers a command line version of the scanner.

NVC's command line scanner has the same basic functionality as the menu-driven scanners.

The command line scanner is not dependent on any other modules. It can be run from batch files.

Starting the Command line scanner

1. From the DOS or OS/2 prompt, go to the directory where NVC resides.
2. The syntax is:
`nvc32 [drive]:[path] [/parameters] [Enter]`
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.
⇒ See 'Command line scanning options' on page 68 for a complete overview and explanation of available parameters.

Cleaning infected files

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 of the NVC scanners (On-demand, On-access and Command line scanner) is the scanning engine. The scanning options reflect the capability of the engine. In addition to detecting 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.

The scanners can remove all types of viruses automatically from hard drives and floppies, except for *boot sector viruses*. Boot sector virus can be removed automatically from floppies, but not from hard drives.

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 on hard drives.

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

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 files by file extension.
/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.

Param.:	Function:
/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. <i>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.</i>
/CL	Repair files when possible. With this parameter, NVC will prompt you to confirm prior to cleaning infected boot sectors and files. When /CL is used concurrently with /U or /Q, however, NVC will not prompt you before cleaning.
/D	Overwrite and delete infected files. Recovery of an overwritten file is not possible.
/D-	Delete infected files. Infected files are automatically deleted. Since we are not overwriting the file before we delete, recovery of the infected file is possible with tools such as the Norton Utilities. <i>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.</i>
/FL	Flush temporary log file for every event logged.
/H	Show help.
/HUM	Handle uncertified macros (needs NSE\NVC\MACRO.CRT from CatsClaw).

Param.:	Function:
/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. Logging is by default off.
/LG	Append log to existing report file. Default is overwrite.
/LQ	Create report file only when infections found.
/LS	Log all scanned directories. <i>Note that in order to produce a report, you must specify one of the L* options above.</i>
/MOV	Move infected files to quarantine.
/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\nvc\bin, the infected directory will be c:\norman\nvc\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.
/OPD	Run Once Per Day if same command line.
/Q	Quiet mode, i.e. no screen output at all. Overrides the /O and /U parameters.
/R	Repeat the scan. Useful for checking several floppies.

Param.:	Function:
/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.
/SF	Scan files by file extension.
/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.

Parameter:	Function:
/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. Overrides the /O parameter.
/WORK :	Specify where NORMAN .RPT and INFECTED directory are 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 scans by using error levels in batch files. The error levels 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.
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.

FAQ

If you don't find what you're looking for on the following pages, please visit our web site and check for updates. This FAQ will be updated on www.norman.com, and in future revisions of this manual.

Your input to this document is appreciated. Send your comments and suggestions for improving the FAQ as well as the documentation in general to documentation@norman.no.

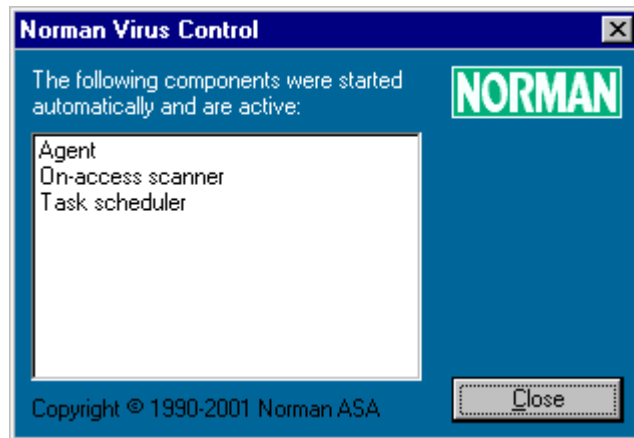
How do I start NVC?

NVC's key components are started automatically when the operating system is loaded. Look for the little green Norman 'N' in the system tray:

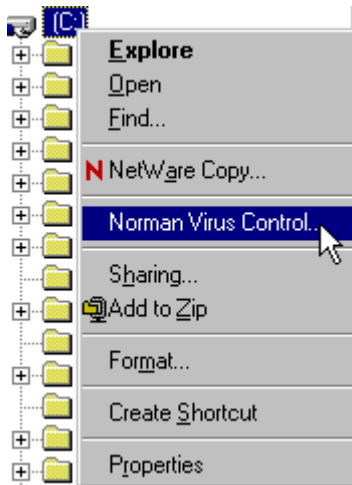


How can I verify that the different components are running?

Click on the Norman icon described above, select "Active components" from the menu, and you will see a message box like this:



The tabbed dialog **Start** in the Configuration editor (Installation settings module) allows you to start and stop certain components.



For a list of installed components, select NVC Utilities|Components.

How do I scan my machine for viruses?

On-access scanning is the cornerstone of virus control in NVC v5. When you access a file, NVC checks it for viruses. The “problem” is that on-access scanning is invisible, and you may wish to perform a more tangible check. You can:

1. Highlight any file system object, for example the drive letter (C:) in Windows Explorer,
2. Click on the right mouse button,
3. Select “Norman Virus Control” from the menu,
4. Click on the **Scan** button for a manual check of all files on the selected drive(s) or directories.

Starting and stopping the on-access scanner

We recommend that you stop the on-access scanner when you perform system maintenance tasks like disk defrag or disk scan. If you stop the on-access scanner, it will not start again in the current session or after rebooting unless you do it manually. To stop and start the on-access scanner, go to the tabbed dialog **Start** in the Configuration editor (Installation settings module).

Should I scan my machine on a daily basis?

Not necessarily. If you combine periodic on-demand scans with scheduled scans, the on-access scanner will monitor your PC for malicious code. However, if you perform frequent downloads from the Internet, it’s a good idea to scan more often.

Can I automate virus scanning?

Yes. From the Norman program group, select “Task Editor” where you can specify which area(s) to scan and when.

How do I update NVC?

Use the module “Norman Internet Update” (NIU) for updating NVC. To configure NIU, use the tabbed dialog **Update mode** in the Configuration editor (Installation settings module). This dialog allows you to decide if NIU should update NVC on-demand, when you access the Internet (depending on what type of connection you’ve got), or from a server in a network.

How do I handle downloaded updates?

Leave everything to NVC. Once NIU has downloaded a package, the NVC agent will perform the actual update automatically. After an update, NVC may prompt you to restart your computer.

How often should I update NVC?

We recommend that you run NIU once a day. Norman's web sites supply news about new viruses, and in some markets virus alert message services are available on e-mail and SMS.

Should I contact Norman if NVC detects a virus?

In general, no. NVC can remove most viruses. Follow the instructions on the screen to remove the virus.

Index

—A—

- Access denied 31
- administrator's rights 19, 36
- Agent
 - zanda.exe 66
- Aggressive commercials 26
- Authentication tab
 - Account 24
 - NDS tree 24
 - Password 24
 - Serial number 24
 - Server logon 24
- Automatically from server 22

—B—

- Back up files to quarantine before repair 28
- boot sector virus 30, 37, 40, 68

—C—

- Combining different parameters 72
- command line scanner 67
- Common settings
 - Aggressive commercials 26
 - Aggressive commercials 26
 - Exclude from scan 26
 - Files of indeterminate format 26
 - Files on exclude list 27
 - Files on network drives 26
 - New, unknown viruses 25
 - scanning 25
 - Security risks 26
- Components
 - Update mode tab 63
- Configuration editor 12
- Conventions iv

—D—

- Daily on dial-up connection (wait for connect) 22
- Daily on direct connection at scheduled time 22
- Damaged archive 31
- Damaged file 31
- Default scanning options 38
- Deny access, on-access scanner (non-interactive) 39
- Diagnostics
 - Access denied 31
 - Damaged archive 31
 - Damaged file 31
 - Error opening archive 31
 - I/O error 31
 - Password protected archive 31
 - Password protected file 31
 - Sharing violation 31

—E—

- E-mail 18
- Error opening archive 31
- Exclude from scan 26, 31, 35
- Exclude from scan, on-access scanner (non-interactive) 38

—F—

- Files of indeterminate format 26, 32
- Files of indeterminate format, on-access scanner (non-interactive) 39
- Files on exclude list 27, 32
 - on-access scanner (non-interactive) 39
- Files on network drives 32
 - on-access scanner (non-interactive) 39
- FireBreak 18
- Firewall 22
- Floating Point Unit (FPU) 12
- Forward messages 45

—H—

- Handle files that cannot be scanned 36
- Hidden until cleaning fails 53
- How to handle viruses, trojans, worms,
on-access scanner (non-inter-
active) 39
- HTTP proxy 63

—I—

- I/O error 31
- Information messages
 - Message routing 44
- Install tab
 - Internet update 20
 - Language 20
 - On-access scanner 19
 - On-demand scanner 19
 - Task editor 19
 - Task scheduler 19
 - Utilities 20
- Internet proxy 18
- Internet tab
 - Proxy server 22
- Internet Update 13
- Internet update 20
 - NIU 62

—L—

- LAN/WAN 22
 - Automatically from server 65
- LAN/WAN tab
 - Configuration 23
 - Software 23
 - Tasks 23
 - Where to look for updates 23
- license information 24
- Log file 46

—M—

- malware 37
- Memory, scanning 52
- message console 48

- Message files tab
 - Right-click options 60
- Message logger
 - Information messages 47
 - Locally generated messages 47
 - Messages received from other
computers 47
 - Program and installation errors 47
 - Send messages to the binary log
file 46
 - System and housekeeping messag-
es 47
 - Virus infections and other alarms
47
 - Warnings 47
- Message routing
 - Information messages 44
 - Messages received from other
computers 44
 - Program and installation errors 44
 - Reply to broadcasts and enable
message routing of 43
 - System and housekeeping messag-
es 44
 - Virus infections and other alarms
44
 - Warnings 44
- Messages
 - Fields in the Messages tab 59
- Messages tab
 - Info 59
 - Message 59
 - Origin 59
 - Right-click options 60
 - Time stamp 59
 - Type 59
- Messaging
 - E-mail 42
 - SMS 42
 - SNMP 42
- Minimized until cleaning fails 53
- Minimized until infection found 53
- Move unrepairable files to quarantine 28
- Multi Media Extensions (MME) 12

—N—

New, unknown viruses 25

NIU 22

 Daily on dial-up connection 63

 Daily on direct connection at
 scheduled time 63

 downloading packets 64

 On-demand only 63

 packages 64

niucf.exe 64

Norman Internet Update 22

 Configuration Settings 63

Norman Personal Firewall 18

NVC components 15

NVC for Lotus Domino 18

NVC for MIMESweeper 18

NVC for MS Exchange 18

NVC for Novell 18

NVC group 14

NVC modules 14

NVC update 21

—O—

On demand scanner

 Exclude from scan 31

On-access scanner 19

 Ask user what to do 37

 Deny access 37

 Display warning 36

 Display warning and deny access
 36

 Exclude from scan 35

 Files of indeterminate format 35

 Files on exclude list 36

 Files on network drives 36

 Handle files that cannot be
 scanned 36

 Ignore 36

 Remove 37

 Scan files before they are used 35

 Scan new or changed files 35

 Specify files to exclude from scan
 35

 Strategy 35

 Use default values 35

 Virus removal 37

On-access scanner (non-interactive)

 , files on network drives 39

 deny access 39

 Exclude from scan 38

 Files of indeterminate format 39

 files on exclude list 39

 Handling viruses, trojans, worms
 39

 Remove 39

 Scan files before they are used 38

 Scan new or changed files 38

 Specify files to exclude from scan
 39

 Strategy 37

 Use default values 39

on-access scanning

 Terminal services 40

On-demand only 22

On-demand scanner 19, 20

 Files of indeterminate format 32

 Files on exclude list 32

 Files on network drives 32

 Right-click scanner 30

 Specify files to exclude from scan
 32

 Use default values 32

OS/2 iv, v

—P—

Parameters

 combining 72

password crackers 26

Password protected archive 31

Password protected file 31

Program and installation errors

 Message routing 44

Proxy server 22

—Q—

Quarantine

- Options 28
- Quarantine properties 28
- Quarantine tab
 - Back up files to quarantine before repair 28
 - Move unrepairable files to quarantine 28
- Quarantined files
- Right-click options 58

—R—

- real-time scanning 37
- Release notes 20
- remote administrative tools 26
- Remove viruses, trojans, worms, on-access scanner (non-interactive) 39
- removing viruses 67
- Repair infected files automatically, on-access scanner (non-interactive) 39
- repairing files 68
- Reply to broadcasts and enable message routing of
 - Message routing 43
- Requirements, system v
- Resource usage 53
- right-click scanner 30
- rights 19, 36

—S—

- Scan files before they are used 35, 38
- Scan new or changed files 35, 38
- Scheduled task 54
- Select machine independent targets 51
- Select specific drives and folders 52
- Send messages to the binary log file 46
- Send messages to the message console 48
- Send messages to the Win NT/2000 Event Log 48
- Serial number 24
- Server logon 24

- Sharing violation 31
- SMS 18, 42
- SNMP 18, 42
- Specify files to exclude from scan, on-access scanner (non-interactive) 39
- Start tab
 - On-access scanner 20
 - Task scheduler 20
- Strategy, on-access scanner (non-interactive) 37
- System and housekeeping messages
 - Message routing 44
- System requirements v
- system tray 15

—T—

- Task editor 12, 19, 49
 - All fixed drives 51
 - All network drives 52
 - All removable media 51
 - Frequency 54
 - General tab 50
 - Hidden until cleaning fails 53
 - Minimized until cleaning fails 53
 - Minimized until infection found 53
 - Open 53
 - Options tab 53
 - Resource usage 53
 - Scan archives 52
 - Scan boot sectors 52
 - Scan memory 52
 - Scan subfolders 52
 - Scanner window 53
 - Schedule tab 54
 - Scheduled task 54
 - Select machine independent targets 51
 - Select specific drives and folders 52
 - Selecting targets 50
 - Start date/time

54
Targets tab 50
Universal Time Coordinates 54
task file
 schedule 56
Task files
 Last run time 56
 Next run time 56
 Right-click options 56
 Schedule 56
 Task file 56
Task scheduler 19, 20
TCP/IP 62, 63
terminal services 40

Message routing 44

—W—

Windows NT/2000 terminal services
 40

—Z—

Zanda 66

—U—

Update from LAN/WAN 22
Update from physical media 21
Update from the Internet 21
Update mode tab
 Automatically from server 22
 Daily on dial-up connection (wait
 for connect) 22
 Daily on direct connection at
 scheduled time 22
 Manually from CD-ROM 21
 On-demand only 22
Use default values, on-access scanner
 (non-interactive) 39
UTC 54
Utilities 12, 20
 Components 55
 Components dialog box 55
 Message files tab 60
 Messages tab 58
 Quarantine dialog box 57
 Task files 56
Utilities module 55

—V—

view quarantine 57
virus definition file 21
Virus infections and other alarms