



# **Norman Virus Control for Workstations**

**Version 5.7**

**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 © 1990-2003 Norman ASA.

All rights reserved.

Last revised on 19 November 2003.

---

## **Norman Offices**

### **Norman Data Defense Systems AS**

Blangstedgårdsvej 1, DK-Odense SØ, **Denmark**

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

E-mail: [normandk@normandk.com](mailto:normandk@normandk.com) Web: <http://www.norman.no/dk>

### **Norman Ibas OY**

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

Tel: +358 9 2727 210 Fax: +358 92727 2121

E-mail: [norman@norman-ibas.fi](mailto: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](mailto:norman@norman.de) Web: <http://www.norman.de>

### **Norman/SHARK BV**

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

Tel: +31 23 789 02 22 Fax: +31 23 561 3165

E-mail: [support@norman.nl](mailto:support@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](mailto:norman@norman.no) Web: <http://www.norman.no/no>

### **Norman Data Defense Systems AB**

P.O. Box 5044, SE-194 05 Upplands Väsby, **Sweden**

Tel: +46 11 230 330 Fax: +46 8 87 52 52

E-mail: [support.se@norman.no](mailto:support.se@norman.no) Web: <http://www.norman.com/se>

### **Norman Data Defense Systems AG**

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

Tel: +41 61 487 2500 Fax: +41 8 87 52 52

E-mail: [norman@norman.ch](mailto:norman@norman.ch) Web: <http://www.norman.ch>

### **Norman Data Defense Systems (UK) Ltd**

PO Box 5517, Milton Keynes MK5 6XJ, **United Kingdom**.

Tel: +44 08707 448044 Fax: +44 08717 176999

E-mail: [norman@normanuk.com](mailto: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](mailto: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



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.

## System requirements

This version supports installation of NVC v5 on Windows 95/98/Me, Windows NT/2000/XP/2003 machines, Linux, OS/2 Warp 4, OS/2 Warp Server, Workspace On-demand, and eComStation.

For Windows 95, Internet Explorer 4.0 or higher is required. WinSock2 must be installed.

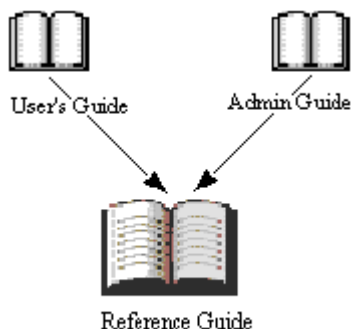
For Windows NT, version 4 with SP4 (or higher) and Internet Explorer 4.0 (or higher) are required.

For OS/2 we recommend Warp 4 fp 15 (or higher) and Java 1.1.8.

For Linux, glibc 2.2 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 .....	iv
Who should read this manual? .....	v
Technical support .....	v
<b>About NVC .....</b>	<b>11</b>
What is NVC? .....	11
General about NVC 5 .....	11
<b>NVC program groups .....</b>	<b>13</b>
Groups, modules, and components .....	13
Shortcut to NVC modules and scanning .....	14
<b>Configuration editor .....</b>	<b>17</b>
Installation settings .....	18
Install .....	18
Start .....	21
Updating NVC .....	21
LAN/WAN .....	22
Internet .....	27
Proxy server .....	30
Common settings .....	31
Exclude list .....	32
Quarantine .....	33
On-demand scanner .....	35
Diagnostic .....	35
Scanning .....	36
Log file .....	39
Archive files .....	41

Infected files within archives .....	42
<b>On-access scanner .....</b>	<b>43</b>
On-access scanning on Windows NT/2000/XP .....	43
About On-access scanning on Windows 95/98/Me .....	44
Configuration considerations .....	45
Scanning .....	45
Cleaning .....	50
On-access scanning in networks .....	51
<b>Norman Internet Protection .....</b>	<b>52</b>
Definitions.....	53
News reader .....	53
Winsock .....	53
Protocol .....	53
Port .....	54
How it works .....	55
Enable NIP .....	56
Virus scanning.....	57
Configuring NIP.....	58
Scanning .....	59
Attachment blocking .....	60
Messages .....	64
Advanced .....	65
<b>NVC on Windows Terminal Server .....</b>	<b>67</b>
<b>Messages and logging .....</b>	<b>69</b>
Message routing.....	70
Messages .....	70
Routing .....	72
Message handling.....	72
Message logger .....	73
Message console .....	75
User-defined message .....	75
E-mail, SMS, SNMP.....	75



---

Messages for E-mail, SMS, and SNMP .....	75
Configure E-mail messages .....	77
Configure SMS messages .....	79
Configure SNMP .....	81
<b>Task editor .....</b>	<b>83</b>
General .....	84
Targets .....	84
Selecting targets .....	84
Common scanning options .....	86
Options .....	87
Schedule .....	88
About the scheduler .....	88
<b>Utilities .....</b>	<b>89</b>
Components .....	89
Task files.....	90
Quarantine.....	91
Messages.....	93
Messages tab .....	93
Message files tab .....	94
<b>Updating NVC .....</b>	<b>96</b>
Norman Internet Update .....	96
Starting NIU .....	96
NIU and Internet connection.....	97
How NIU works .....	98
LAN/WAN .....	99
<b>Miscellaneous on NVC .....</b>	<b>100</b>
The agent.....	100
About the Command line scanner.....	101
Starting the Command line scanner .....	101
Cleaning infected files .....	101
Running task files from the command line .....	102

Command line scanning options .....	103
Combining Different Parameters .....	105
Command Line Scanner Errorlevels .....	106
<b>Appendix A - Sandbox .....</b>	<b>107</b>
Background .....	107
What is a sandbox? .....	107
Sandboxing techniques .....	108
How does sandboxing affect the user? .....	108
What to do when the sandbox detects a new virus .....	109
<b>FAQ .....</b>	<b>110</b>
<b>Index .....</b>	<b>115</b>

# 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.

## General about NVC 5

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.

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 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.

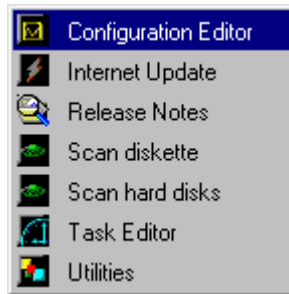
⇒ See 'Configuration editor' on page 17, 'Task editor' on page 83, 'Utilities' on page 89, and 'Norman Internet Update' on page 96.

# NVC program groups

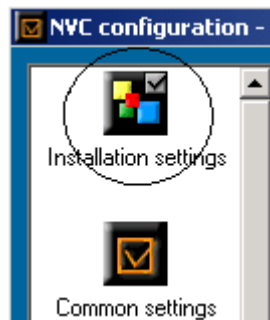
This chapter presents the groups and their matching modules and components that make up NVC v5. If a component has a related function elsewhere in the program, there will be a reference with title and/or page number to the relevant section. Sometimes we refer to the other two NVC 5 manuals: the *User's 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

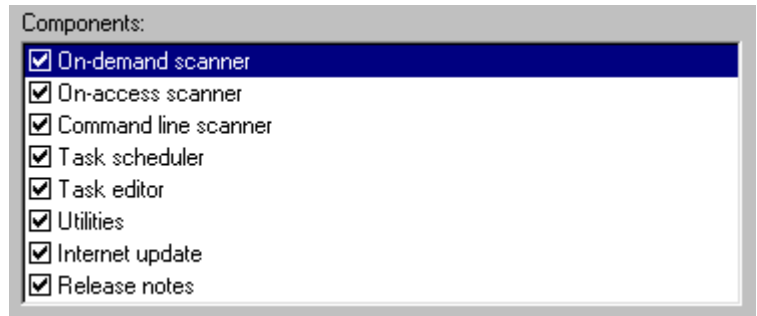
When we talk about a NVC **group**, we are referring to a larger entity that holds modules and components. Examples of NVC groups are: Configuration editor, Internet Update, Task editor, and Utilities:



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**:



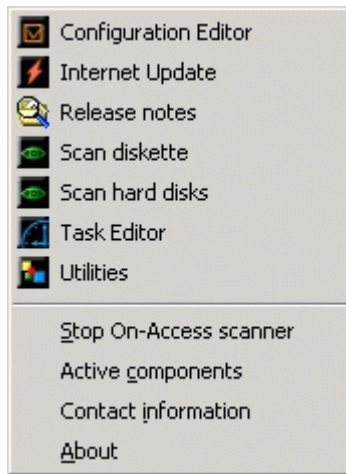
## Shortcut to NVC modules and scanning



During setup, a Norman icon is placed in the system tray in the lower right-hand corner of the screen. This icon confirms that NVC is installed on this machine. See also page 15.

**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 NVC 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 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 other information.

## Warnings

The Norman icon also provides information regarding the state of your NVC installation. If the icon appears like this:



it denotes that the NVC components currently running do not match those selected in the Start tab in the Configuration editor's **Installation settings**. Select "Active components" from the NVC menu to examine which components that run.

**Note:** During startup, the red symbol is visible until all modules have started. The older and slower the machine, the longer it takes for all modules to load. However, the "normal" symbol should appear after a maximum of 1-2 minutes.

If this icon appears in the system tray,



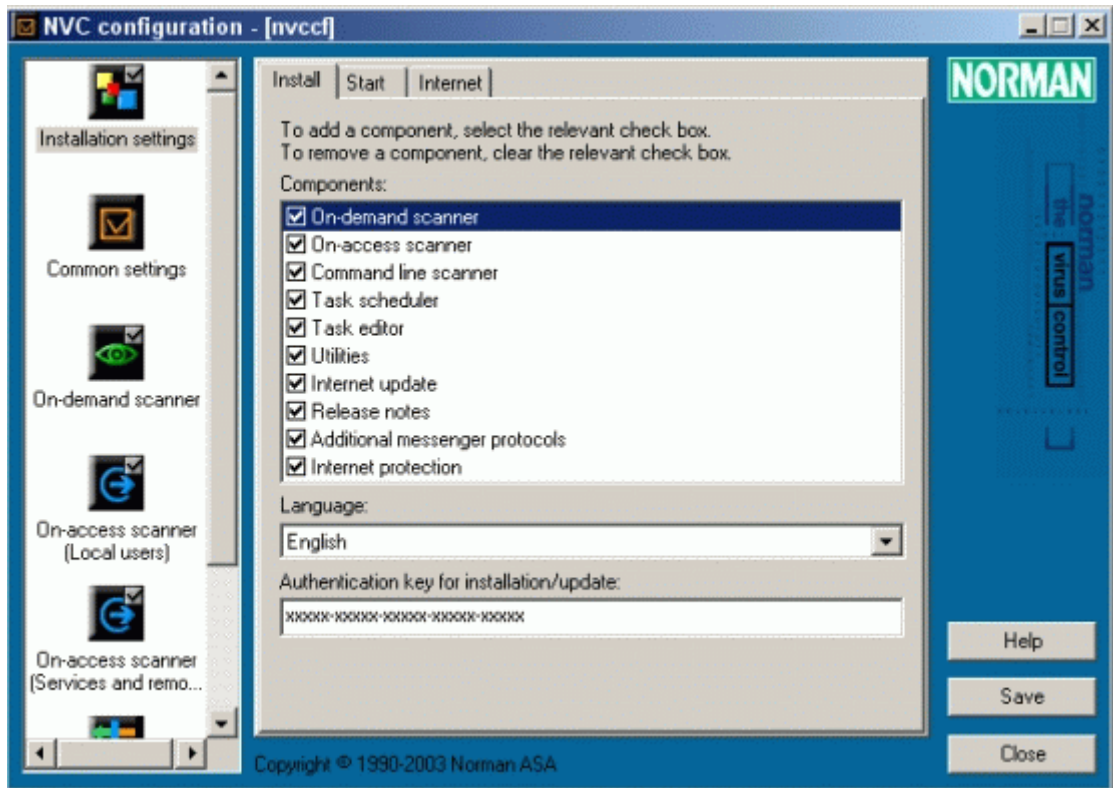
it signifies that one of these situations have occurred:

1. The On-access scanner is installed, but has been manually disabled. To start the On-access scanner, select the shortcut from the menu, or go to the Start tab in the Configuration editor's **Installation settings**.
2. You have probably selected **Reboot later** on a previous prompt, and NVC is waiting for a reboot.
3. An installation error that a reboot might fix.



# 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 *E-mail, SMS, SNMP*, 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.

## Installation settings

The purpose of this module is to:

- install (or remove) NVC components by selecting and deselecting from the list of available components
- select/deselect components that should be launched automatically at start-up
- define how you should update and distribute your NVC installation - via the local network or directly from the Internet - and configure your selection(s)

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 35.

---

**☑ 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’ on page 43.

**☑ Command line scanner**

The Command line scanner is an alternative to the GUI-based scanner and offers the possibility of running batch jobs and other scanning tasks from the command line. The Command line scanner is a good alternative for those familiar with this environment.

⇒ ‘Starting the Command line scanner’ on page 101.

**☑ Task scheduler**

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

⇒ ‘About the scheduler’ on page 88.

**☑ 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 83.

**☑ Utilities**

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

⇒ ‘Utilities’ on page 89.

☒ **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 96.

☒ **Release notes**

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

☒ **Additional messenger protocols**

In addition to NVC’s internal messaging system, a separate module handles e-mail, SMS, and SNMP messages. Select this option to include this module.

⇒ ‘E-mail, SMS, SNMP’ on page 75.

☒ **Internet protection**

Norman Internet Protection (NIP) is a module designed to intercept incoming and outgoing mail, stripping or blocking all infected attachments for undesired content.

**Note:** NIP is a *workstation* module. Do *not* use NIP on servers that run separate SMTP service, or on terminal servers. On a terminal server NIP may protect the first logged on user *only*, and is therefore worthless in such an environment.

NIP is installed as a default module the first time you install NVC—also on servers and terminal servers. We therefore recommend that you uninstall or stop NIP on these platforms.

⇒ ‘Norman Internet Protection’ on page 52.

**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.

**Authentication key for installation/update:**

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.

**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.

**Updating NVC**

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

**Note:** The virus definition files and the other components are so closely integrated that you should update **all** available components. It is not sufficient to install updated definition files only.

You can update NVC in different ways, via the Internet, the internal network, or from the program CD. The update mechanisms cater for servers and networks as well as standalone machines, and there is a number of configuration options you can choose from.

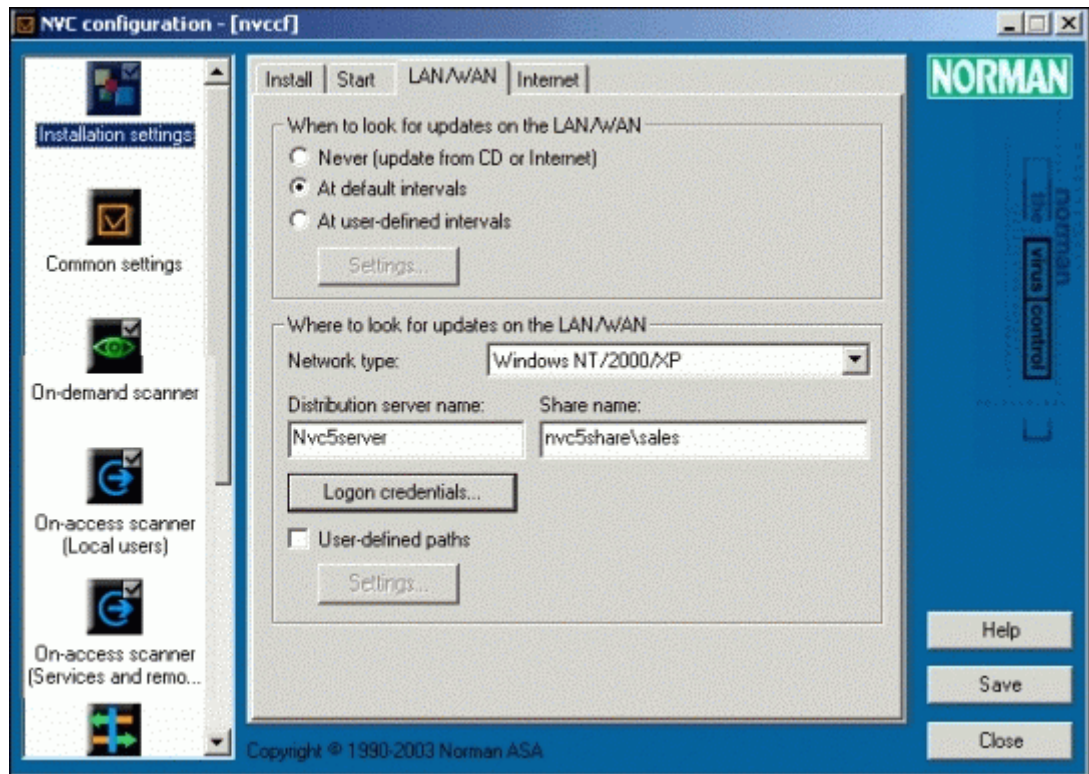
## LAN/WAN



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

This tabbed dialog is for updating NVC in networks and is therefore for system administrators.

From this dialog you can enter the required information about your network and how frequent NVC should look for updated software, configuration, and task files, and configure the different options.



### When to look for updates on the LAN/WAN

#### ○ **Never (update from CD or Internet)**

If you don't intend to update NVC via your internal network, select this option and go to the next tabbed dialog to specify how to update from the Internet. Also, use this option when you receive a version update on CD-ROM 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 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 96.

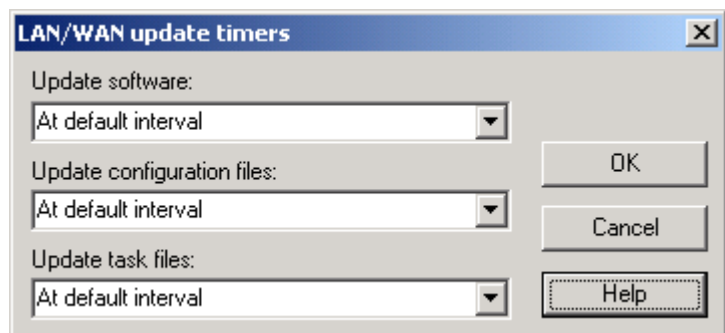
### ☉ At default intervals

Updates are performed at intervals established by Zanda - the agent. Zanda distinguishes between NVC distribution servers and clients.

⇒ Please refer to the section about Zanda in the *Administrator's Guide* (especially the passage “Update intervals and network traffic” for a comprehensive discussion on these mechanisms).

### ○ At user-defined intervals

This option allows you to specify update intervals for software, configuration files, and task files. Click on **Settings** to display the following dialog:



The default option for all updates is “At default interval”, and replaces the option “Automatically from server” in previous NVC5 versions. If you select the default interval, updates are

replicated from the distribution server about 3 minutes after you log in, then once every hour on workstations and once every 5 minutes on distribution servers. These are the default settings, but as of NVC v5.5 you may configure other update schemes. Select other update intervals from the drop-down-menus in the dialog.

**Note:** If you don't have a permanent connection to the Internet, we do not recommend the default option, which will generate many and costly dial-ups. It's a better solution to select every hour, for example. Moreover, with a dial-up connection to the Internet, the distribution server should be located locally.

Where to look for updates on the LAN/WAN

When you've entered the update intervals, you must specify where the updates are located.

First, specify which network you're running by selecting from the **Network type** list. You can choose between:

- Windows NT/2000/XP
- Workgroup or peer-to-peer network, and
- Novell NetWare.

For Windows NT/2000/XP and Workgroup or peer-to-peer network, enter:

- Distribution server name
- Share name

For Novell NetWare, enter:

- Distribution server name
- Volume name and root directory

**Note:** Simply enter the name of the distribution server without backslashes or any other special characters.

When the three fields in the Where to look for updates on the LAN/WAN are completed, NVC interprets the information to establish complete file paths.

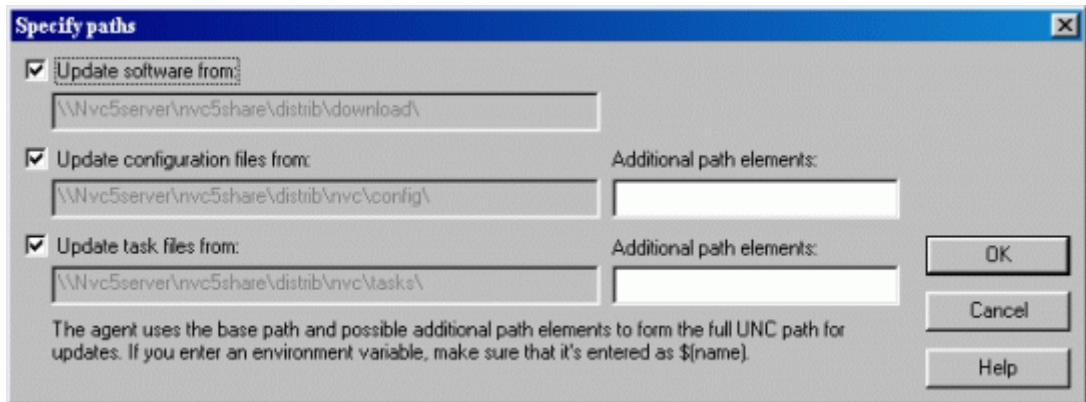


## Logon credentials

If you're running a Windows network, you can enter User name, Password, and Domain name by clicking the **Logon credentials** button.

## User-defined paths

If you want to differentiate Configuration and Task files between different departments in your organization, for example, you must select **User-defined paths** and click on **Settings**. The following dialog appears:



In this dialog, the fields are already completed based on the information you provided for *Server name* and *Share name* (*Volume name and root directory* on Novell).

### ☒ **Update software from:**

Identifies the server path where NVC software updates can be fetched after they are downloaded from the Internet, for example. This box displays the server and share/volume name entered in the previous dialog, plus the default path to the location where software packages are located.

### ☒ **Update configuration files from:**

This box displays the server and share/volume name entered in the previous dialog, plus the default path to the location where the configuration files are stored.

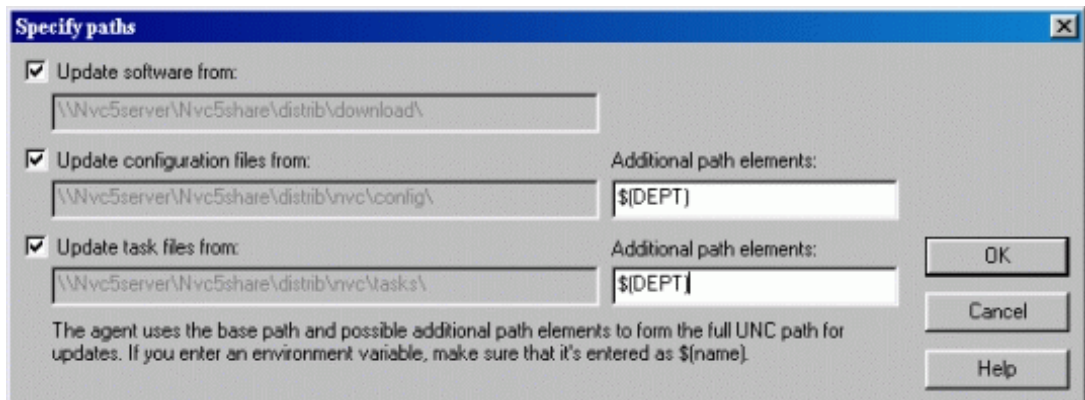
☒ **Update task files from:**

This box displays the server and share/volume name entered in the previous dialog, plus the default path to the location where task files are stored.

**Additional path elements:**

The additional field for *Configuration files* and *Task file* update gives you the opportunity to distribute custom-made config and task files to specific entities within your organization.

If you enter an additional path element, make sure that you enter the environment variable in the format \$(name), which enables the agent to establish a full UNC path. Example:



The image shows a Windows-style dialog box titled "Specify paths". It contains three sections, each with a checked checkbox and a text field. The first section is "Update software from:" with the path "\\Nvc5server\Nvc5share\distrib\download\". The second section is "Update configuration files from:" with the path "\\Nvc5server\Nvc5share\distrib\nvc\config\" and an "Additional path elements:" field containing "\$(DEPT)". The third section is "Update task files from:" with the path "\\Nvc5server\Nvc5share\distrib\nvc\tasks\" and an "Additional path elements:" field containing "\$(DEPT)". At the bottom, there is a note: "The agent uses the base path and possible additional path elements to form the full UNC path for updates. If you enter an environment variable, make sure that it's entered as \$(name)." On the right side, there are three buttons: "OK", "Cancel", and "Help".

**Specify paths**

☒ Update software from:  
\\Nvc5server\Nvc5share\distrib\download\

☒ Update configuration files from:  
\\Nvc5server\Nvc5share\distrib\nvc\config\ Additional path elements:  
\$(DEPT)

☒ Update task files from:  
\\Nvc5server\Nvc5share\distrib\nvc\tasks\ Additional path elements:  
\$(DEPT)

The agent uses the base path and possible additional path elements to form the full UNC path for updates. If you enter an environment variable, make sure that it's entered as \$(name).

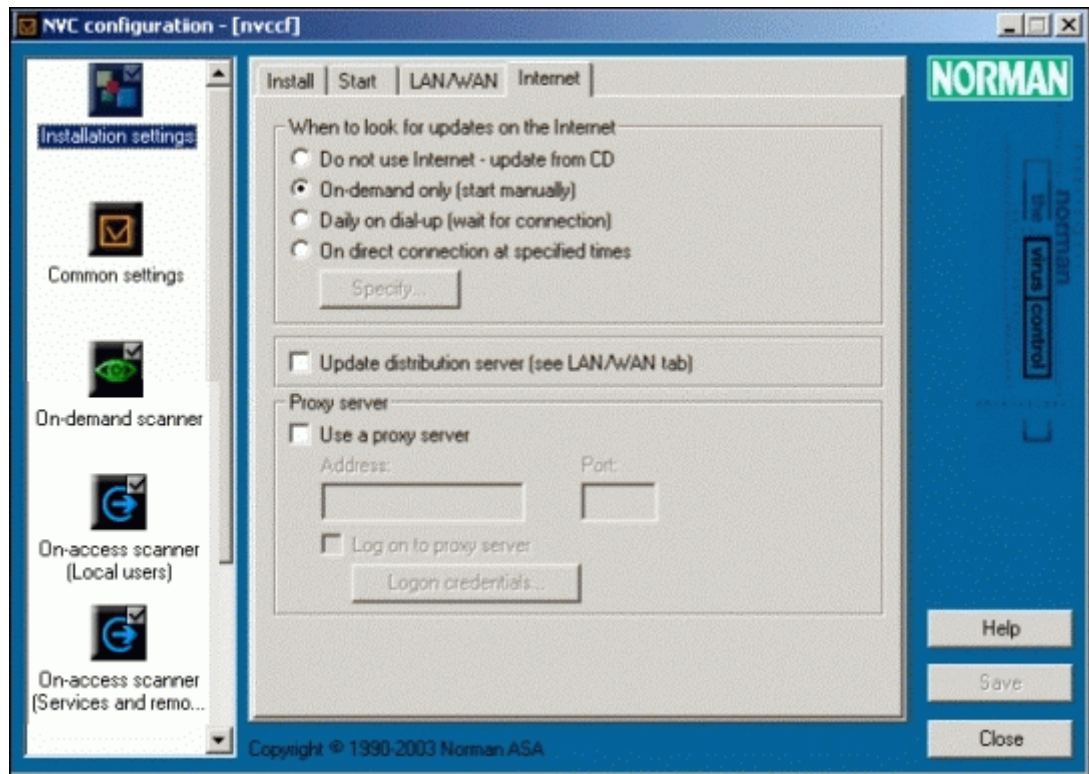
OK  
Cancel  
Help

## Internet

Your selection in this section affects the way NIU handles updates from the Internet.

Internet is the most efficient and swift method of distributing updated virus definition files and upgrades for the other NVC components. You need to download all these updates as soon as possible to maintain full protection. You should therefore be careful to select the option that suit your needs best.

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. However, a network often runs several operating system platforms and different language versions of NVC. In heterogeneous environments you therefore have to run a separate configuration tool for NIU (NIUcf), to make sure updates for the entire network are downloaded. NIUcf is described in the “Installing and distributing” sections for Windows NT and Novell NetWare in the *Administrator's Guide*.



### When to look for updates on the Internet

**Note:** If your machine is protected by a firewall or proxy server, you may have to enter the required information in the **Proxy server** section of this dialog (page 30).

#### **○ Do not use Internet - update from CD**

If you select this option you will never be prompted or reminded about available Internet downloads. Since CDs normally are distributed only when a new version of NVC is released, you will only receive CDs from Norman every three months or so. We do **not** recommend this option, as your NVC installation will be outdated after maximum one week.

☒ **On-demand only (start manually)**

Select this option if you prefer to start NIU manually from the NVC menu to check for updated packages, or use Windows' **Scheduled Tasks** utility (located in **Control Panel**).

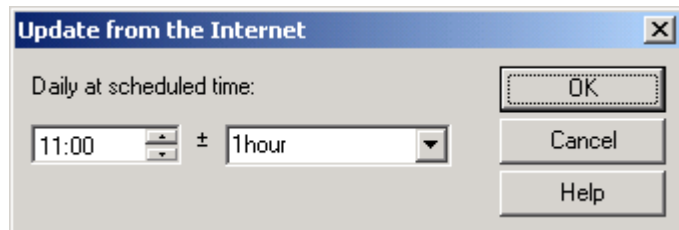
☐ **Daily on dial-up (wait for connection)**

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.

☐ **On direct connection at specified times**

You can select this option if you have a permanent connection to the Internet. Click on **Specify** to schedule a time:



First specify when NVC should check for updates. Enter the time, and then use the '+-' pull-down menu to allow the system a time slot to fit in the task at the most convenient time to avoid possible overloads.

☐ **Update distribution server (see LAN/WAN tab)**

If you select this option, you enable a client to download updates to a NVC distribution server. In addition, successful updating requires that the logged on user has write access to the distribution directory (...\\Norman\\Distrib\\Download).

The **Update distribution server** is not a default option. Hence any client trying to run Internet Update (NIU.EXE) will update

its own download path (. . . \Norman\Download), and not the distribution directory (. . . \Norman\Distrib\Download). This is for example useful for laptops, which will be updated from the distribution server when they're on-site, and by running NIU individually when they're on the road.

If the *client* that runs NIU has enabled **Update distribution server**, and the client is not connected to the network, neither the local NVC installation nor the distribution server will be updated.

If NIU is run from the *distribution server*, **Update distribution server** should not be selected.

The **Update distribution server** option is typically selected only for a couple of machines that is usually in the network all of the time. (See the section on distributing diverse configuration and task files to individual workstations in the *Administrator's Guide* for more info).

In installations where Novell Netware is distribution server, this option must be selected for at least one machine (for example the the NVC administrator's machine).

## Proxy server

Proxy servers may require user authentication. If you use the proxy server options in this dialog, you must enter the same information for proxy server log on and authentication as configured on the proxy.

The two prevalent authentication schemes are:

1. Basic, and
2. Windows NT challenge/response *aka* NTLM.

### Proxy server

#### ☐ Use a proxy server

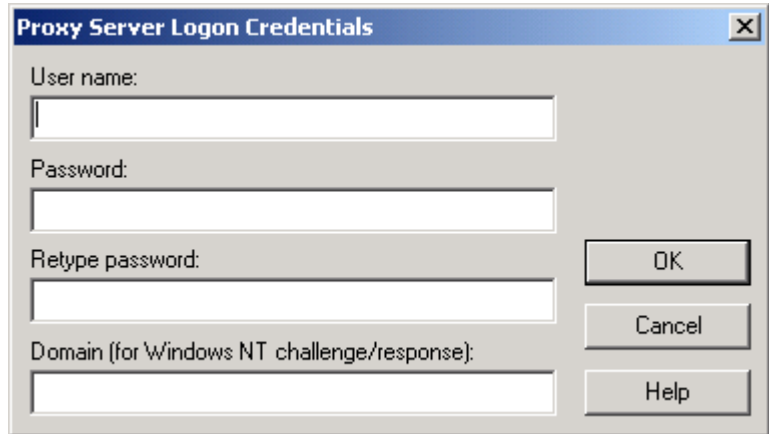
Enter the **Address** and **Port** for the firewall's HTTP proxy.

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

## ☐ Log on to proxy server

**Note:** This option is only relevant if your proxy server requires authentication.

Click on **Logon credentials** to display this dialog:

A screenshot of a Windows-style dialog box titled "Proxy Server Logon Credentials". It contains four text input fields: "User name:", "Password:", "Retype password:", and "Domain (for Windows NT challenge/response):". To the right of the fields are three buttons: "OK", "Cancel", and "Help". The dialog has a standard Windows XP-style border with a close button in the top right corner.

The information you enter here should match the information you normally specify when you log on to your proxy server.

### **User name:**

Enter a valid user name.

### **Password:**

Enter the password.

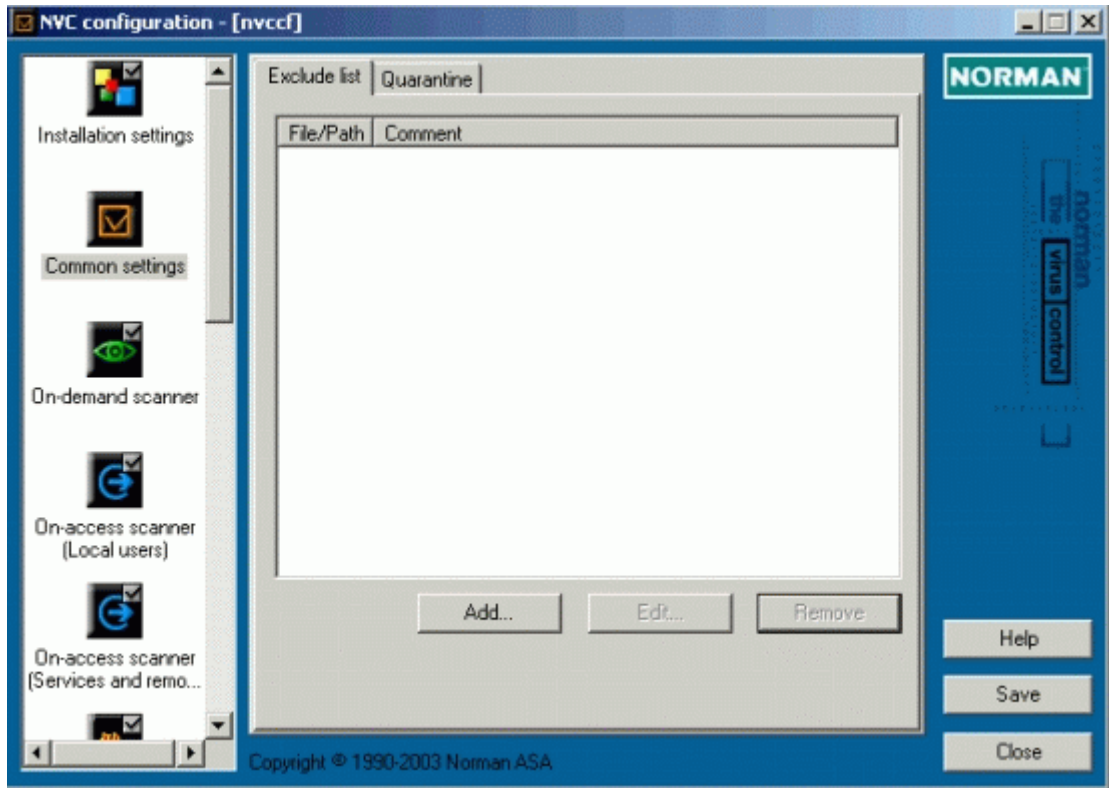
### **Domain (for Windows NT challenge/response)**

This field is not intended for proxy servers using basic authentication.

Enter the domain name. If the field is left blank, the *machine name* is used.

## Common settings

Common settings primarily affect malware handling, and this module is consequently a supplement to the scanning modules *On-demand* on page 35, *On-access (Local users)* on page 43, and *On-access* on page 43.



## 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. You can also use the browse button in the "File/Path to exclude" field to select the desired object(s). 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.

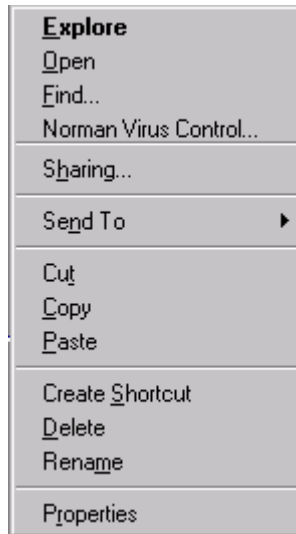
☒ **Move unrepairable files to quarantine**

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 (Services and remote users) module (page 43). 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 Right-click scanner will use the settings you specify under 'On-demand scanner' on page 35.

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 101.

## Diagnostic

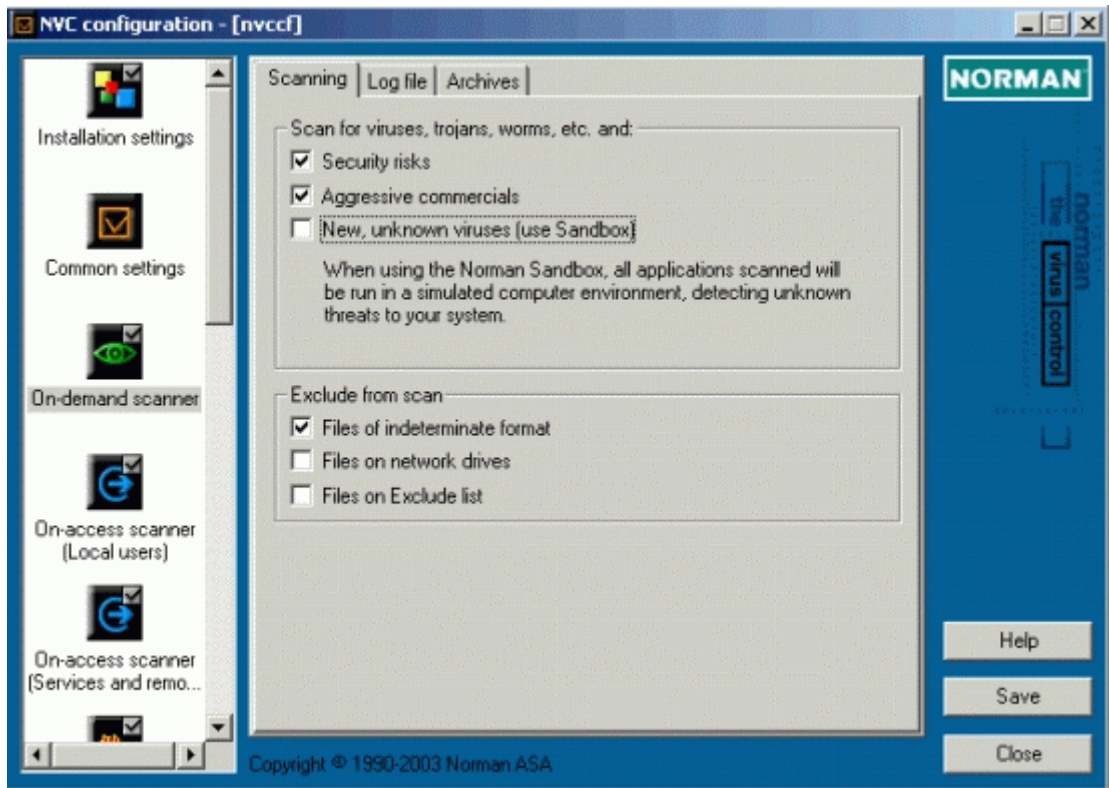
When the on-demand scanner has completed the scan of the selected area(s), all relevant information appears in the scanning dialog. There are separate entries for infected files and for files that could not be scanned. The **Diagnostic** field advises you why NVC couldn't scan a particular file. The most common reason is that the file is damaged. A 'damaged' file is not necessarily

useless to the user, but NVC cannot recognize the file format and consequently not scan the file. If other, less likely situations occur, you'll be informed about the reason why a file cannot be scanned. The log file(s) will provide additional information.

## Scanning

See also the tabbed dialog box 'Common settings' on page 31 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.



Scan for viruses, trojans, worms, etc., and:

☒ **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.

☒ **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.

☐ **New, unknown viruses using sandbox**

NVC employs its sandbox functionality to detect new, unknown viruses. Select this option if you want NVC to look out for new virus variants. The sandbox is particularly tuned to find new email-, network- and peer-to-peer worms and file viruses, and will also react to unknown security threats. When a new piece of malicious code is detected, the system administrator receives a message through NVC's messaging system listing the vital facts. (See page 109 for an example.)

When this option is selected, scanning time will increase, but it is not likely to affect the performance considerably. For more information about the sandbox, please refer to 'Appendix A - Sandbox' on page 107.

### 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.

☒ **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**



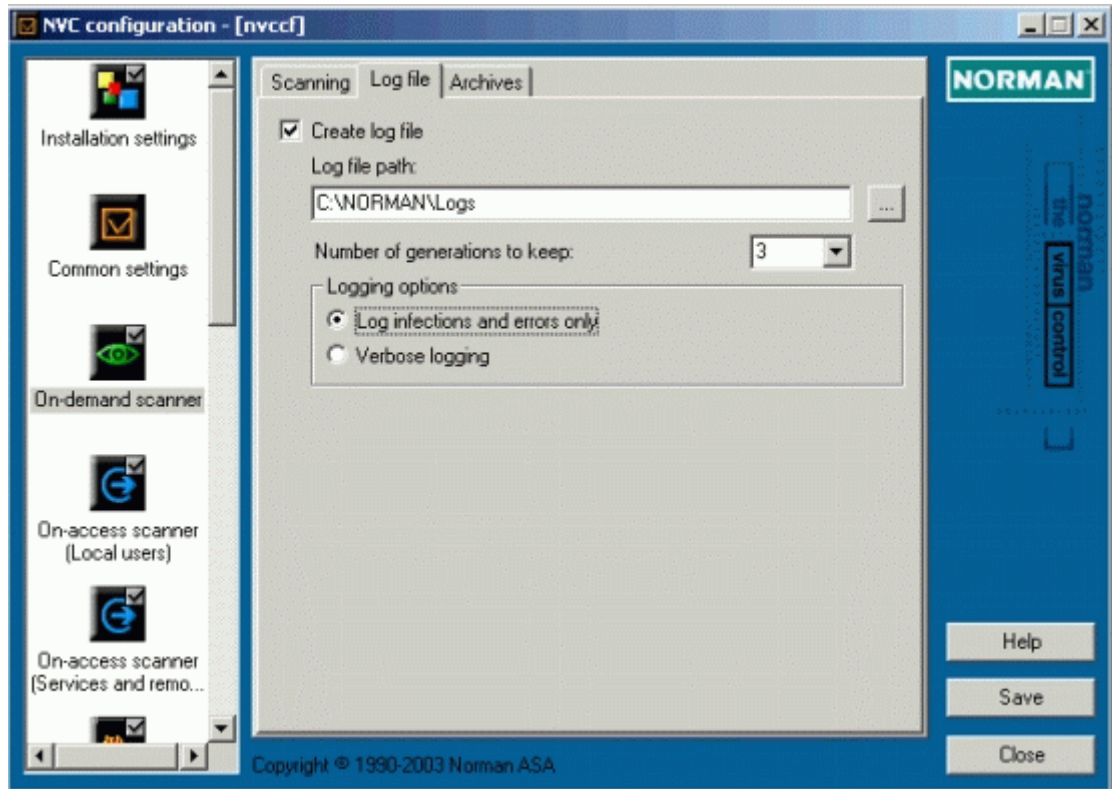
In networks, you may not allow all users to scan files on the server. Select this option if you are only permitted to scan files located on the workstation.

☐ **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.

## Log file

By default, NVC generates a log file when you run a manual scan. The log file has a default name and location, and you can choose between a detailed report and a log file that only reports infections and errors.



### ☒ Create log file

Creates a log file whenever you run an on-demand scan. If you deselect this option, no log file is generated for on-demand scans.

#### Log file path:

The default path for the log file is `c:\norman\logs`. Click on the browse button to specify a new path.

### Number of generations to keep:

If you select the default value of 5, NVC will overwrite the oldest log file when log file number 6 is generated. The first log file is named `nvc00000.log`, then `nvc00001.log` etc. Similarly, if you keep 10 generations, the first log file is overwritten rather than generating `nvc00010.log`.

### Logging options

#### ☉ **Log infections and errors only**

This is the default log file which delivers a summary of the scanned area including scanning time and number of files scanned, details on possible infections and program errors, scanning engine version, and virus definition file dates.

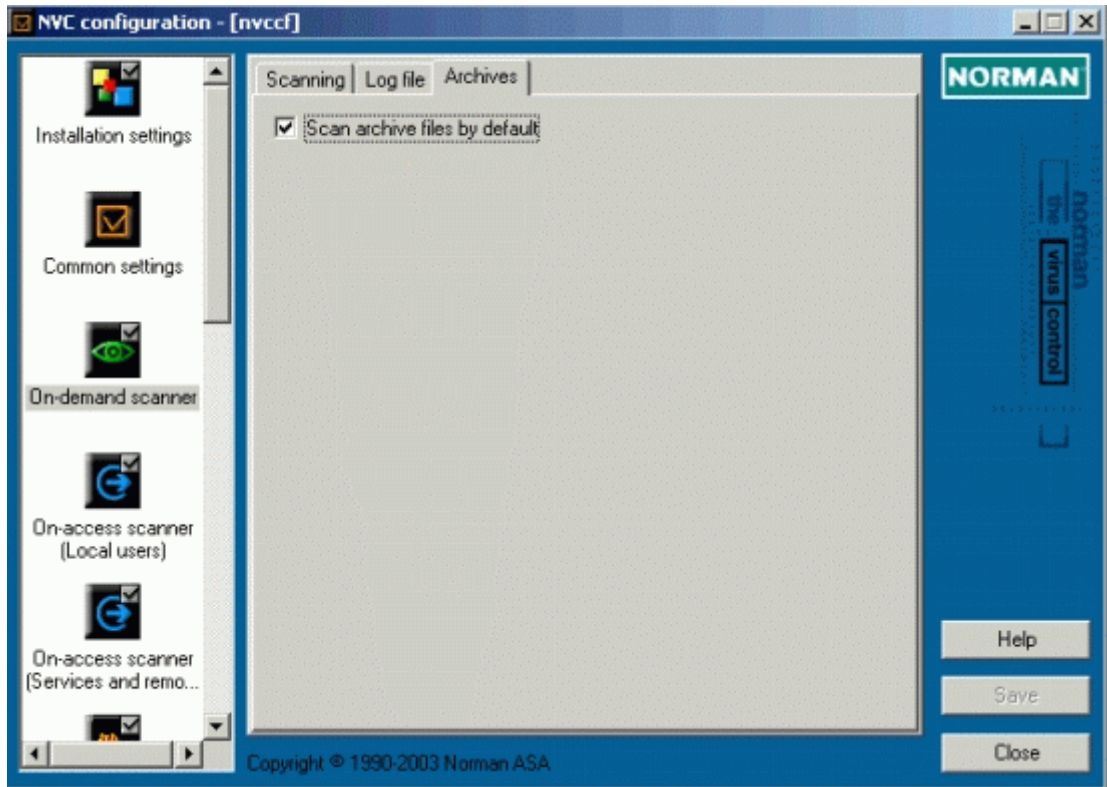
#### ○ **Verbose logging**

Verbose logging generates a very detailed report, specifying each file that was scanned, scanning time per file, status, etc.



## Archive files

Archive files are sometimes large and may hold a very high number of files.



### ☒ Scan archive files by default

NVC is configured to always scan archives.

Users familiar with previous versions will note that former limitations with regard to archive file size and depth, i.e. levels of archives within archives, have been solved in the new scanning engine. Just be aware of how NVC handles non-repairable files within archives (see below).

## Infected files within archives

If an infected file is detected within an archive, NVC will try to repair first. If repair is not possible, the infected file is deleted from the archive, and the original file is quarantined.

The On-demand scanner will act according to the quarantine option(s) you specified in the **Common settings** module.

---

# On-access scanner

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, if configured to.

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 101.

## On-access scanning on Windows NT/2000/XP

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

### **Local users:**

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 'Services and remote users' mode applies.

**Services and remote users:**

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. The ‘Services and remote users’ mode applies to any NT/2000/XP machine that is logged off.

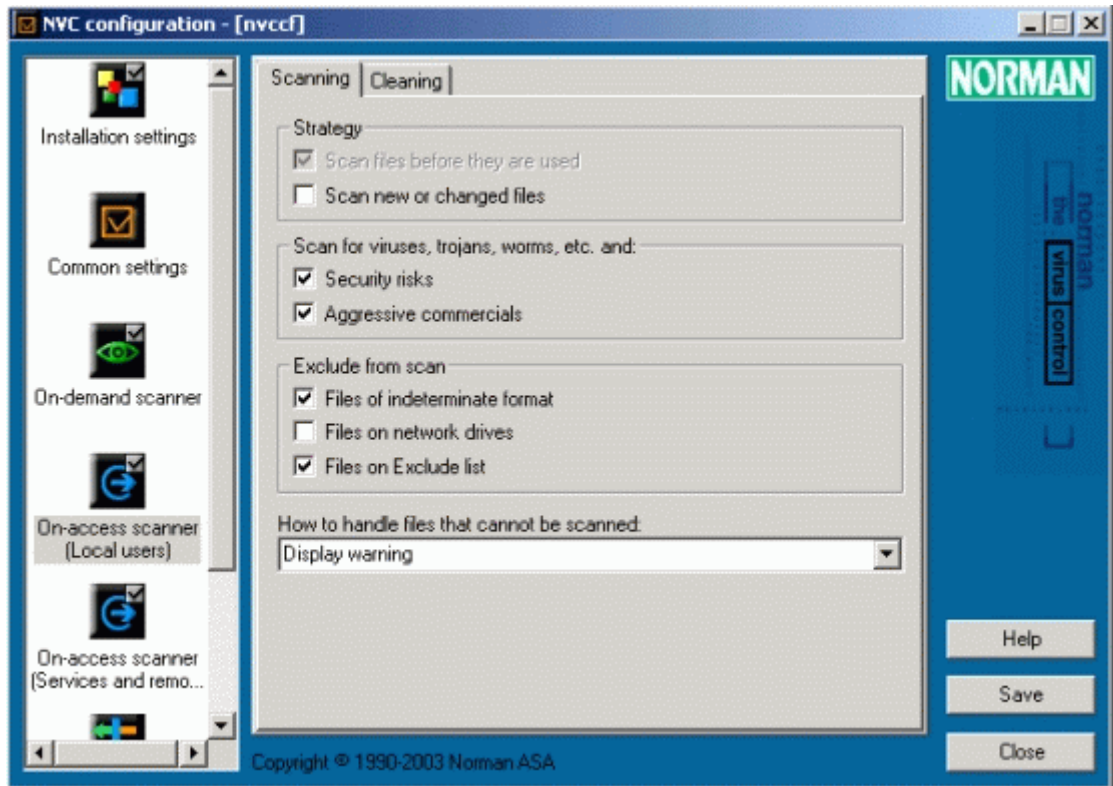
The typical scenario is that ‘Services and remote users’ activity takes place on the server. However, if someone physically logs on the server, the ‘Local users’ mode applies.

## **About On-access scanning on Windows 95/98/Me**

Unlike the On-access scanner in Windows NT/2000/XP installations, the On-access scanner on Windows 95/98/Me consists of only one module. By default this module will scan files when a logged on user access them. In the configuration tabs for this module you may change the way the On-access scanner behaves— like which operations to monitor, which files to exclude from scanning, and how to behave when viruses or other malware are detected.

# Configuration considerations

## Scanning



### Strategy

**(Applies to Windows 95/98/Me and the 'Local users' module on Windows NT/2000/XP and OS/2)**

In this section you select whether you want to scan files both before they are used and when new files are created or changes are done to existing files. In other words, you select a strategy for the on-access scanning that takes place when a user is locally logged on to the computer.

**You may think of these options as 'workstation' settings.**

**☒ Scan files before they are used**

This option instructs the On-access scanner to scan files that are opened for read/execute and is mandatory for security reasons.

**Example:** When you open a file from a floppy, a document from your hard disk, or an e-mail attachment, the On-access scanner will scan the file on the fly and take action if malware is detected. Of course this requires that your virus definition files are up-to-date.

**☐ Scan new or changed files**

This option instructs the On-access scanner to scan files that are opened for write, such as when changes are made to documents or new files are created on your hard disk.

On Windows NT/2000/XP the ‘Services and remote users’ module will prevent other (remote) users from saving infected files onto your computer. For local users, we do not recommend combining this option with **Scan files before they are used**, as it may seriously affect the machine’s performance on read/write extensive applications.

However, we *do* recommend selecting this option on Windows 95/98/Me clients where file and/or print sharing are enabled.

**Strategy****(Applies to Windows NT/2000/XP and OS/2 machines only)**

In this module you select whether you want to scan files before they are used and/or when new files are created, or when existing files are changed. In other words, you select a strategy for the on-access scanning that takes effect when other computers write files to your computer/server.

**You may think of these options as ‘server’ settings.**

**☐ Scan files before they are used**

This option instructs the On-access scanner to scan files that are opened for read/execute.

**Example:** If files on a server share (where this option is selected) are opened from a workstation, the files are scanned before the users can access them.

However, scanning time increases significantly when this option is selected. You should therefore not select this option on servers unless you have a heavy spreading virus infection in your network.

☒ **Scan new or changed files**

This option instructs the On-access scanner to scan files that are opened for write, for example when users in a network save their work or create files on a server.

The **Scan new or changed files** option is selected by default. We don't recommend that you combine this option with **Scan files before they are used** unless you have a heavy spreading virus infection in your network, as this usually will affect performance significantly.

**Important:** More specifically, scanning on write means that new or changed files are scanned on close. Suppose you have an unprotected client computer, which is infected with a virus that spreads across network shares. Whenever this virus infects a file on a server, where the On-access scanner is configured to scan new or changed files, the On-access scanner detects and removes the virus. Unfortunately, detection and removal with traditional file scanners happens *after* the actual infection has taken place. For viruses like VBS/Loveletter, this means that the virus may trash a lot of files on its way. Anyway, infected files will be quarantined so they are unavailable for users in the network to reactivate the infection in the network.

*Scan for viruses, trojans, worms, etc. and*

**(Applies to all supported platforms)**

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:

☒ **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.

☒ **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.

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.

☒ **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**

Enable this option if you don't want NVC to scan shares that you have access to on remote computers.

☒ **Files on Exclude list**

Files on the Exclude list are not scanned. Reasons for not scanning certain files may be that they trigger false alarms, or they are too time-consuming to scan. Anyway, we recommend that you scan files on the exclude list regularly by running scheduled or On-demand scans.





How to handle files that cannot be scanned**(Applies to Windows 95/98/Me and the 'Local users' module on Windows NT/2000/XP and OS/2)**

In some situations NVC is unable to scan a file. Examples are password protected Word documents, damaged files, or when internal system errors occur. There are three available options for how NVC can treat files that cannot be scanned. From the pull-down menu you can choose between:

**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.

**On-access scanner mode (NOT applicable on Windows)**☐ **Use scanning mode for services and remote users only**

When the the on-access scanner is running in 'Local users' mode, dialogs that need to be responded to pop up regularly. If this option is selected, these dialogs don't appear on the server and the configuration options for 'Services and remote users' scanning apply.

This option is only valid for networks with OS/2 servers.

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.

**Note:** For On-access scanner (Services and remote users), this option is only relevant if you selected **Scan files before they are used** as scanning strategy. In other words, if you use the default settings, you should **not** select this option.

### ⊙ 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.

### Recommendations:

- Make sure that your NVC installation is up-to-date. This is the best protection against virus attacks, so you are able to stop viruses before they enter the system.
- Install antivirus software on e-mail servers and gateways.
- Restrict user rights on shares as much as possible, for example by setting read-only attribute where applicable on files that are not frequently changed.
- Back up your files regularly.

---

## On-access scanning in networks

NVC will by default scan files that are accessed on network drives. The On-access scanner's behavior will depend on the user rights of the logged on user when scanning files residing on network drives. When the On-access scanner sees a file that is opened from a network drive, it will scan the file as usual. However, it will not be able to repair, remove or quarantine an infected file, unless the logged on user has write access to the directory/file in question. Still, access to the infected file will be denied.

The paragraph above is not a recommendation to be less restrictive with user privileges. If an up-to-date On-access scanner protects your servers as well as the clients, it is not likely that On-access scanner on the clients ever will detect malware on network drives. Anyway, if such a situation occurs, the protection is there.

When the On-access scanner detects viruses or other malware on network drives, it will display the location as UNC paths and not mapped drives. Many users know network drives as X, Y, Z etc. The popup alerts from the On-access scanner will for example display `\\Server\Share\InfectedFile` instead of `X:\Infected file`.

On-access scanning in networks is intended where servers don't run virus control, simply to avoid that the same files are scanned twice—once on the server and then again when they are opened on the client. The consequence of such double scanning could be that network log-ons and backup becomes slower. However, the individual system administrator must make the final decision where security on one hand, and network operation on the other are two major factors to consider.

You may deactivate On-access scanning of files on the network by checking the **Files on network drives** 'Exclude from scan' option.

---

# Norman Internet Protection



**Note:** The current version of Norman Internet Protection is for the Windows platform only, and will *not* work with OS/2.

Norman Internet Protection (NIP) is a filter that protects against viruses that spread through

- Internet mail, and
- news readers.

The majority of viruses reported today use mechanisms that enable them to spread through e-mail. Statistically, one of 30 e-mails sent during major virus epidemics contains some sort of malicious software. The need for protection against such virus attacks is imperative.

NIP is a NVC 5 module designed to intercept incoming and outgoing mail and news, stripping or blocking all infected attachments for undesired content.

NIP is not only capable of scanning e-mails for known viruses; it can also warn the sender about a possible infection and block file attachments depending on content and file extensions.

NIP monitors the most prevalent messaging protocols and supports most popular e-mail clients. As an integrated component in NVC 5 it can be distributed throughout your network, establishing yet another barrier against the increasing threat from e-mail viruses.

## **Important limitations:**

The current version of NIP is best fitted for home users rather than professional environments. Presently, it's more a workstation than a server module and is not well fitted in installations with separate SMTP servers, for example businesses that use one server for internal e-mail and another for Internet e-mail.

NIP doesn't scan local mail servers for malware.

# Definitions

## News reader

A **news reader** is an application that enables you to read messages posted to Internet newsgroups and to post your own messages. Popular browsers like *Internet Explorer* and *Netscape* feature their own news readers, and several stand-alone news readers are also available.

## Winsock

**Winsock**—short for *Windows Socket*—is a programming interface and the supporting program that handles input/output requests for Internet applications in Windows. Each Windows version is equipped with its own version of `winsock.dll`. Simply put, Winsock is the bridge between Windows programs and TCP/IP (Internet) connections.

It's worth noting that other vendors supply freeware and shareware versions of `winsock.dll` that do **not** follow Microsoft's standards. Each such version may differ in minor ways. This is hardly of benefit for the user or third party programmers of Internet applications for the Windows platform.

**Note:** All Norman products that involve `winsock.dll` are in compliance with Microsoft's standards.

## Protocol

A **protocol** is a defined format for transmitting data between two devices. You can think of it as a language. Your only concern as a user, is that your machine supports the relevant protocols when communicating with other computers.

These **protocols** are supported by the current version of NIP:

- POP3, for incoming e-mail
- SMTP, for outgoing e-mail
- NNTP, for newsgroups

## Port

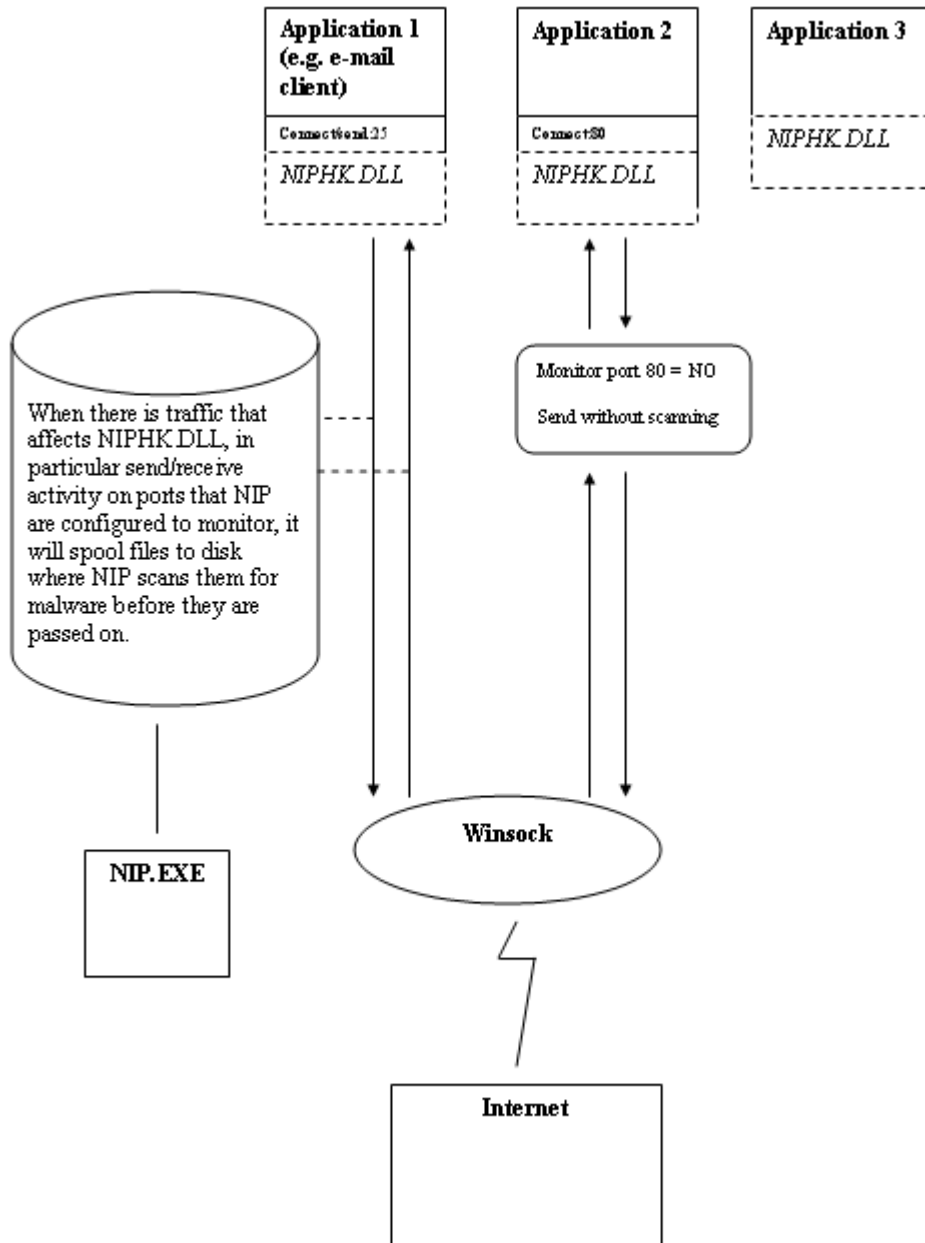
A port is a “logical connection place” within programming, and specifically— using the Internet’s protocol TCP/IP—the way a client program specifies a particular server program on a computer in a network. Applications that use TCP/IP, like the web protocol HTTP, have ports with preassigned numbers. These are labelled “well-known ports” that have been assigned by an official, international committee (IANA). Other application processes are given port numbers dynamically for each connection. When a service (server program) initially is started, it is said to bind to its designated port number. As any client program wants to use that server, it also must request to bind to the designated port number.

Port numbers are from 0 to 65536. Ports 0 to 1024 are reserved for use by certain privileged services. For the HTTP service, port 80 is defined as a default and it does not have to be specified in the Uniform Resource Locator (URL).

Please refer to the section ‘Advanced’ on page 65 and onwards for an overview of NIP’s supported protocols and corresponding port numbers.

As these definitions demonstrate, the interconnection between protocols, ports and deviating standards represent a possible risk for “conflicting interests”.

## How it works



The DLL (Dynamic Link Library) *niphk.dll* is inserted in all running applications and is capable of monitoring/scanning all

Winsock traffic. Winsock, which is discussed on page 53, handles input/output requests from Internet applications on the Windows platform.

The current version of NIP supports three protocols: POP3 (incoming e-mail), SMTP (outgoing e-mail), and NNTP (newsgroups).

Whenever `niphk.dll` detects an operation that uses any of these protocols, it will invoke `nip.exe` for scanning. Say it is an incoming mail with attachments on port 110. NIP *spools* (temporarily stores) to the hard drive where the scanning takes place. However, if NIP's not configured to monitor incoming mail on port 110, it will ignore whatever activity that takes place on that port.

NIP relates to the standard ports for the traffic it is monitoring. If you have installed other applications that use other ports for the same type of traffic, then you may have to reflect this in your configuration.

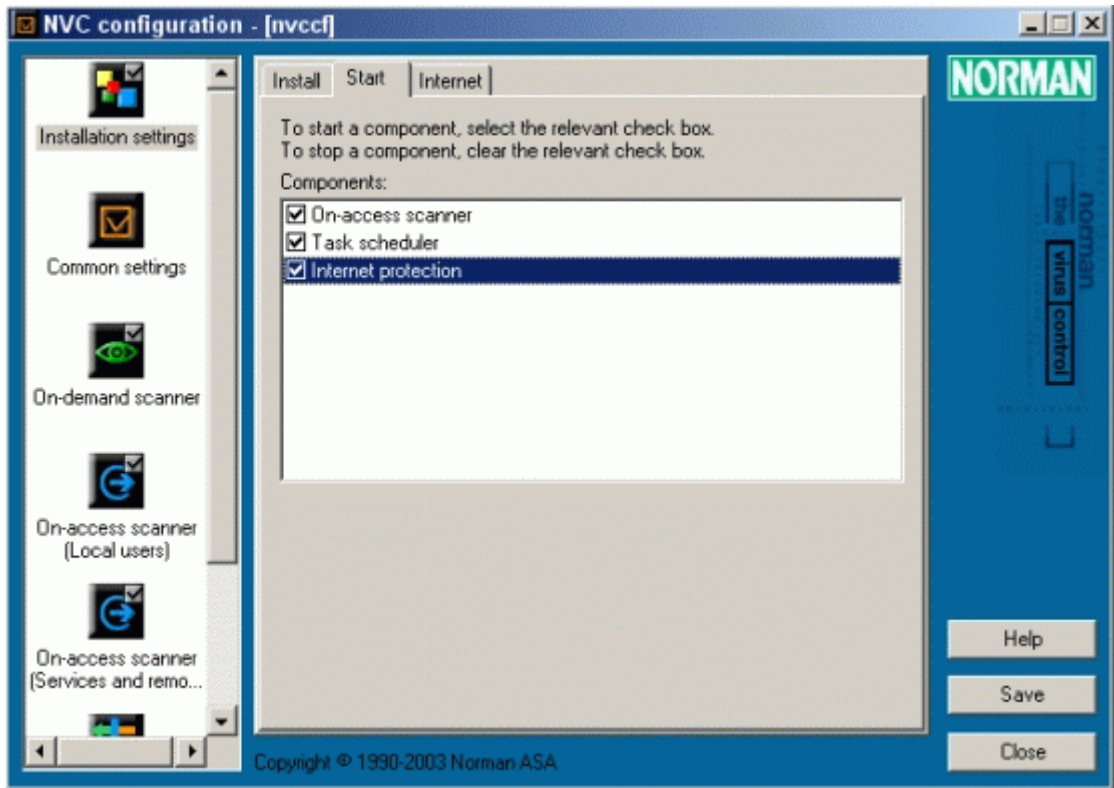
## Enable NIP

**Note:** The rights defined in `default.ndf` decide which changes a user can do to the local installation.

To install this module, go to the **Install** tab in **Installation settings** in the Configuration editor (see page 18). Select ***Norman Internet Protection*** at the bottom of the list and click **Save**.

After a few seconds, ***Norman Internet Protection*** appears as a separate entry under the **Start** tab. Again, select it and click **Save**.





You will have to exit and restart the Configuration Editor to be able to configure NIP's options.

To stop NIP, clear the check box and click **Save**.

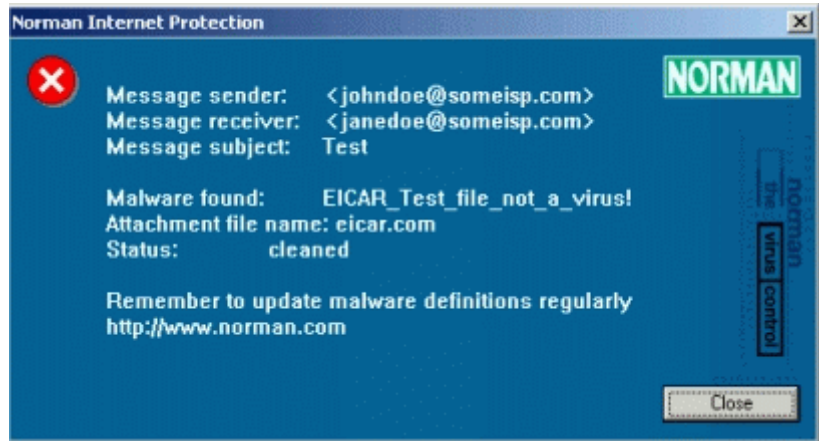
## Virus scanning

Downloaded attachments are temporarily stored on the client's hard disk and scanned for viruses before they are handed over to the user.

NVC will try to clean infected attachments before they are deleted or quarantined. Sometimes cleaning equals deletion, for example *trojans*, where the entire file makes up the malware.

**Note:** A copy of the deleted or blocked attachment is quarantined by default.

SMTP/POP3 mail and NNTP news pop up a message box and put the data stream on hold if viruses, worms or trojans are found:

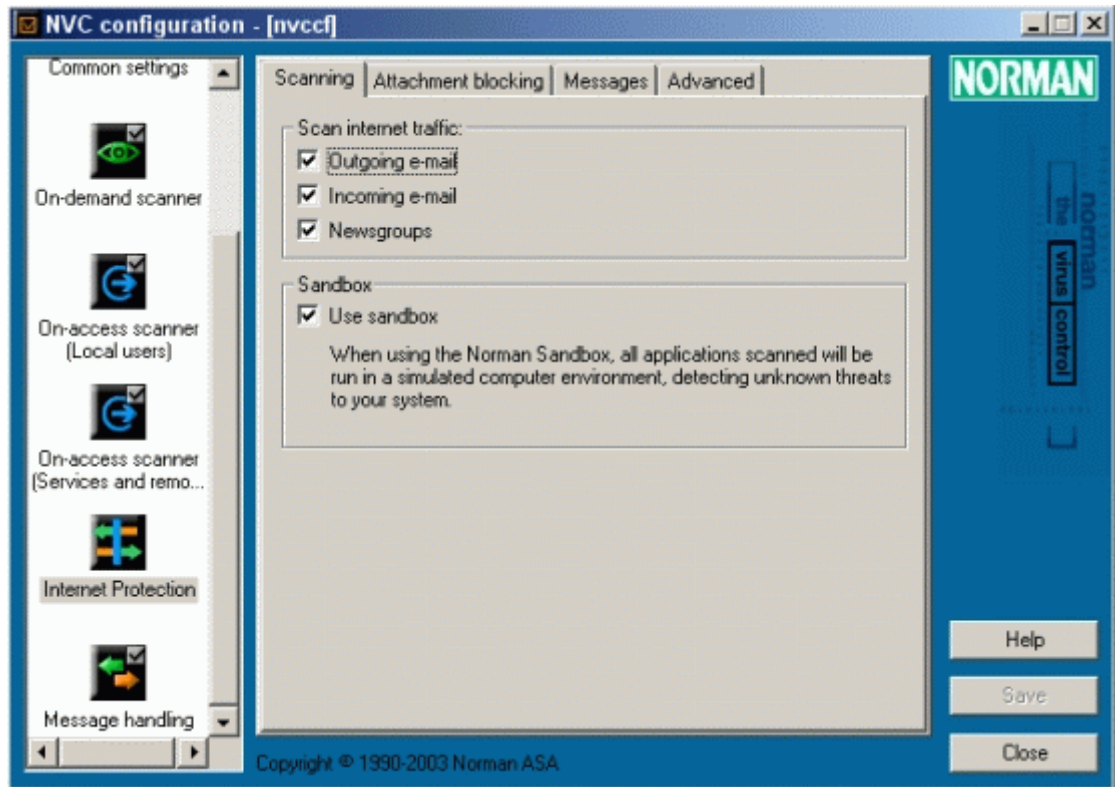


You can configure NIP to send automatic mail messages about infected attachments to the creator/sender and multiple receivers as well as to the Norman logging and messaging system. Please refer to 'Messages and logging' on page 69 for more details.

## Configuring NIP

NIP is made up from four dialog boxes where you decide what elements that should be scanned, block attachments generically or specifically, send warning messages when viruses are detected, and define port numbers for their corresponding protocols.

## Scanning



Select which elements of the Internet traffic you want to scan. The default is to scan all.

### Scan Internet traffic

#### ☒ **Outgoing e-mail**

Scans all e-mail that is sent from your system. If your machine is infected by malware which you are unaware of, you could unintentionally send infected mails to friends and business associates, for example.

### ☒ **Incoming e-mail**

Scans all e-mail that you receive from others. Again, even your best friend or closest business associate may be ignorant of a virus infection

### ☒ **Newsgroups**

Scans the traffic generated between your computer and the other participants in the group/forum you are active in.

⇒ See 'Definitions' on page 53 for more information on this subject.

### Sandbox

### ☒ **Use sandbox**

NVC employs its sandbox functionality to detect new, unknown viruses. Select this option if you want NVC to look out for new virus variants. The sandbox is particularly tuned to find new email-, network- and peer-to-peer worms and file viruses, and will also react to unknown security threats. When a new piece of malicious code is detected, the system administrator receives a message through NVC's messaging system listing the vital facts. (See page 109 for an example.)

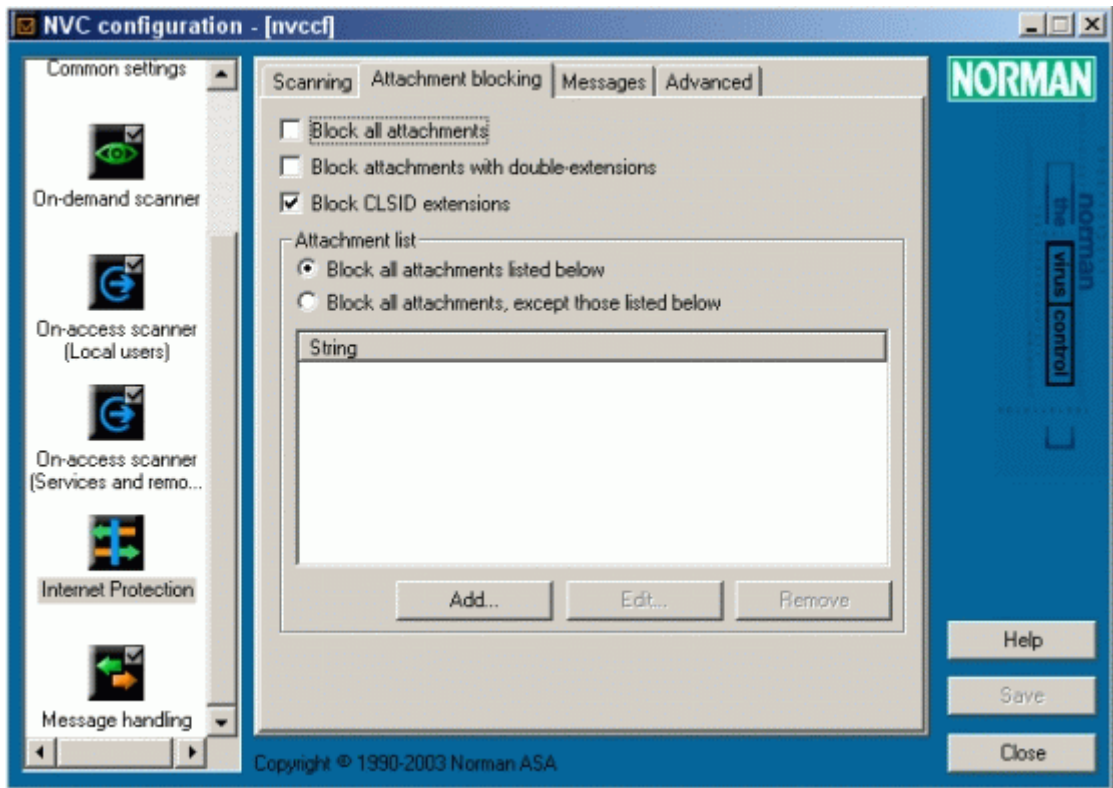
When this option is selected, scanning time will increase, but it is not likely to affect the performance considerably. For more information about the sandbox, please refer to 'Appendix A - Sandbox' on page 107.

## **Attachment blocking**

You can block attachments by entering the exact file name or files with certain extensions, for example. This feature is particularly useful when e-mail worms are roaming and the worm can be identified by name. Attachment blocking is also a useful feature to stop file types that you do not want to receive in your mailbox.

When NIP blocks an attachment, it will *move* the attachment to quarantine area rather than *delete* the attachment. This serves as a backup if it proves that the attachment was legitimate after all. In the quarantine area it cannot do any harm anyway. For example, if you have specified that all executables (\*.exe) should

be blocked, it's reassuring to know that you can recover a file that you needed after all.



☐ **Block all attachments**

All attachments are blocked.

☐ **Block any attachment with double extensions**

Many worms and e-mail viruses apply a technique where an additional extension is added, for example `<filename>.jpg.vbs`. Most e-mail clients will hide the last extension so that the attachment appears to only have the extension `.jpg`. However, this feature is not only used by viruses—legitimate files with names like `myfile.hlp.zip` and `todolist 20.dec.doc` are both treated as double extensions.

### ☒ **Block any CLSID extensions**

Some recent worms and e-mail viruses apply a CLSID technique to fool e-mail scanners and blocking software. They take advantage of a feature in Windows which makes it possible to replace an .exe extension with a {...} extension and thus evade blocking of .exe files. Since there is no reason for legitimate attachments to use this type of extension, this behavior is blocked by default.

#### Attachment list

Use this function to explicitly select attachments you want to block—or certify. You can enter the exact name of an attachment, or use wildcard (\*) to block certain extensions. To block all .exe files, for example, click on **Add** and enter \*.exe. Click **OK**, and the entry appears in the list box, where you later can edit or remove it.

### ☒ **Block all attachments listed below**

All names that you **Add** to the list are *blocked*. Enter a specific name, or use wildcard (\*) to identify attachments to stop.

### ☐ **Block all attachments, except those listed below**

All names that you **Add** to the list are *accepted*. Enter a specific name, or use wildcard (\*) to identify attachments to accept.

**Note:** It is *very* important that you distinguish carefully between these two options, as they represent two extremes: *block* all on the list, or *accept* all on the list.

### **Recommendations**

The extension lists below are not static, and will be modified to reflect the prevailing virus and malware threat situation. You can employ these recommendations if you selected ☒ **Block all attachments listed below**.

### Security level: Medium

Add the following extensions to the list of files you want to block:

*.BAT	*.CHM	*.CMD	*.COM	*.CPL
*.EXE	*.HLP	*.HTA	*.HTM	*.INF
*.JS	*.JSE	*.LNK	*.MSI	*.PIF
*.REG	*.SCR	*.SHS	*.SWF	*.VBE
*.VBS	*.WSC	*.WSH	*.URL	*.PL
*.SH	*.CLA	*.PI	*.DLL	

### Security level: High

Select the option ***Block all attachments, except those listed below***. If you choose a high security level, you must be careful to use the **Add** function to list which file types you accept. Depending on what kind of files you normally receive or exchange, you probably have a good idea of the file types you should put on the list.

**Note:** Remember that a copy of a blocked attachment is placed in quarantine—*not* deleted—so it is possible to restore a file that was mistakenly blocked.

In case you still want to exchange valid \*.exe files, for example, with your e-mail contacts, and don't want NIP to block them, all attachments should be encrypted or exchanged in a compressed format like \*.zip.

### String

In this field you can specify file names that should be blocked. Wildcard ('\*') is accepted for blocking of specified extensions. For obvious reasons, only wildcard for file names is allowed, i.e. \*.vbs. To the average user, file types like .vbs, .pif or .lnk are hardly critical. You should also consider to block extensions/file types like .exe, .com and .bat as these also represent a potential risk for virus infections.

In this field you can also block specific attachments with names known to contain viruses, such as

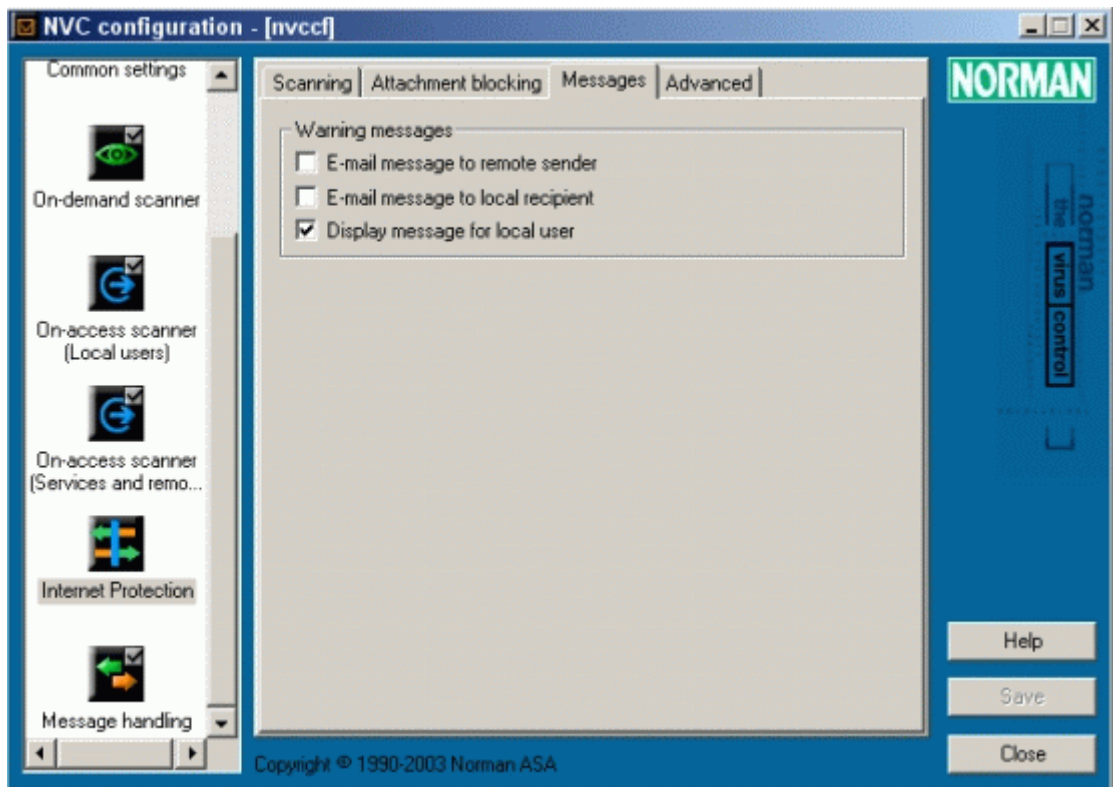
AnnaKournikova.jpg.vbs. Theoretically, you may block a

virus before updated virus definition files are released from the vendor.

**Note:** Outlook 2002 also features an attachment blocking functionality that will be applied *after* the attachments have passed through NIP.

## Messages

The options in this dialog represent which action you may take if malicious software is detected.



### Warning messages

- ☐ Mail message to remote sender
- ☐ Mail message to local recipient
- ☒ Display message for local user



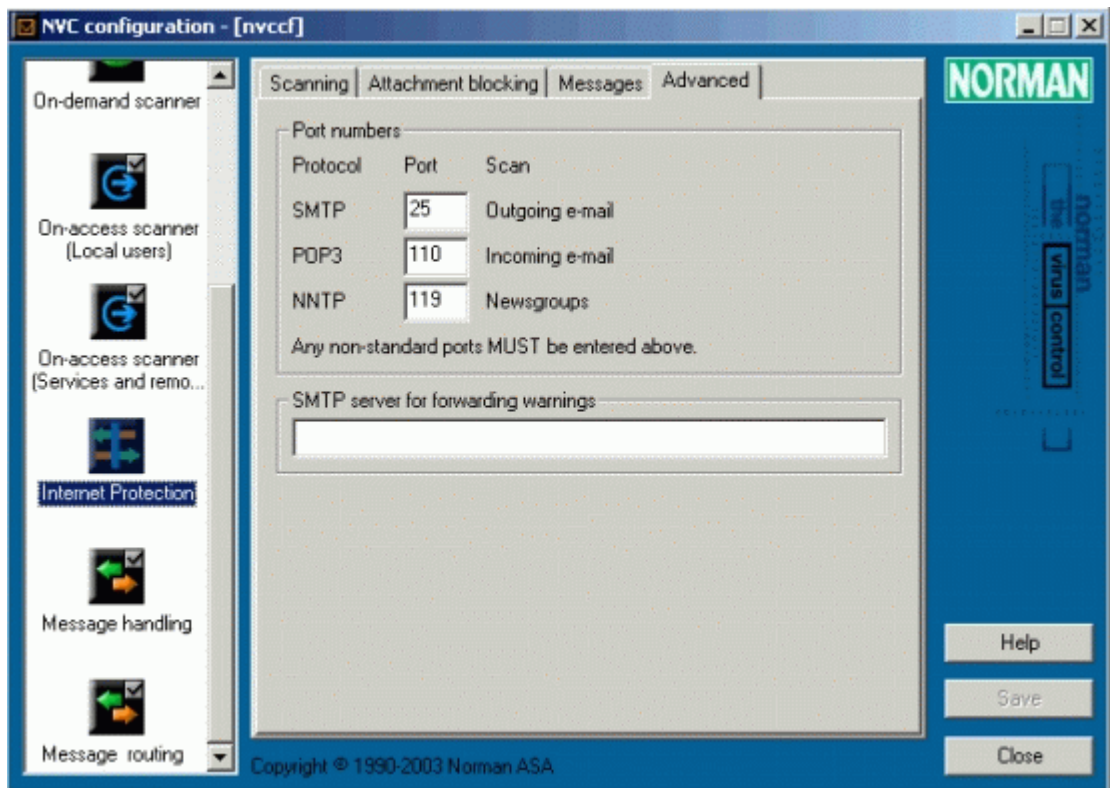
You can send copies of NVC's warning messages on virus infections to the sender and/or recipient of the infected mail. The message reports which action NVC has taken, the attachment file name, and current status (for example **deleted**).

If you consider to select **Mail message to remote sender**, you should bear in mind that many of the new viruses spoof e-mail addresses. Thus a warning message never reaches the sender, and the only effect may be increased network traffic.

You cannot change the text in the warning messages.

## Advanced

Among the numerous protocols for communication between computers, there are some that are vital for Internet use. For standardization reasons, protocols have pre-assigned port numbers.



### Port numbers

In the “Scanning” dialog you selected which Internet traffic you wanted to scan. This dialog identifies the protocols needed for sending and receiving e-mails, for example, and the corresponding port number on the PC, according to the industry standard.

You may have assigned different port numbers to one or more of the supported protocols listed here. If that is the case, you must enter the **actual** port number for the affected protocol(s).

The protocols below are those supported presently. The list is likely to be updated whenever it’s necessary.

These are the complete names of the abbreviated names. The port numbers and functions are already specified in the dialog:

- **SMTP** (port 25) is short for *Simple Mail Transport Protocol*
- **POP** (port 110) is short for *Post Office Protocol*
- **NNTP** (port 119) is short for *Network News Transfer Protocol*

### SMTP server for forwarding messages

This field is only relevant if you selected to send warning message to remote sender (see page 64).

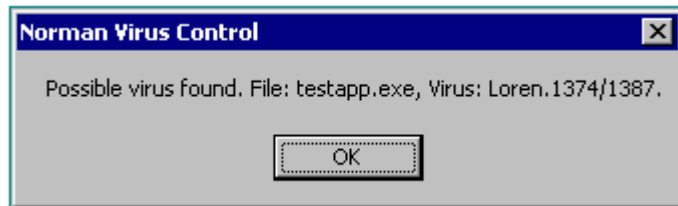
Enter the server for outgoing mail as it is specified in your configuration, for example in the mail account config.

# 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.

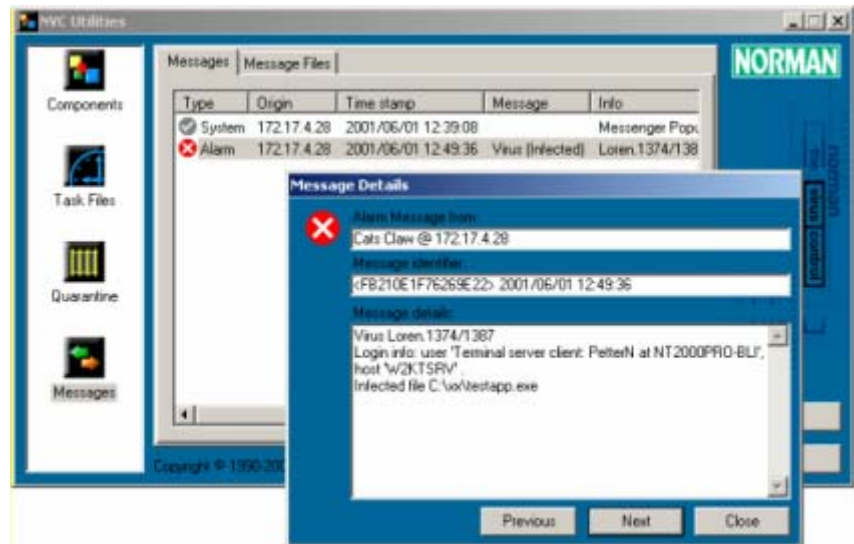
During on-access scanning for Terminal server client sessions, NVC will always use the 'Services and remote users' (or server) configuration. This means that no virus alert dialog box will appear on the Terminal server when a virus is found. On the Terminal server client's machine however, a message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

---

# Messages and logging

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

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.

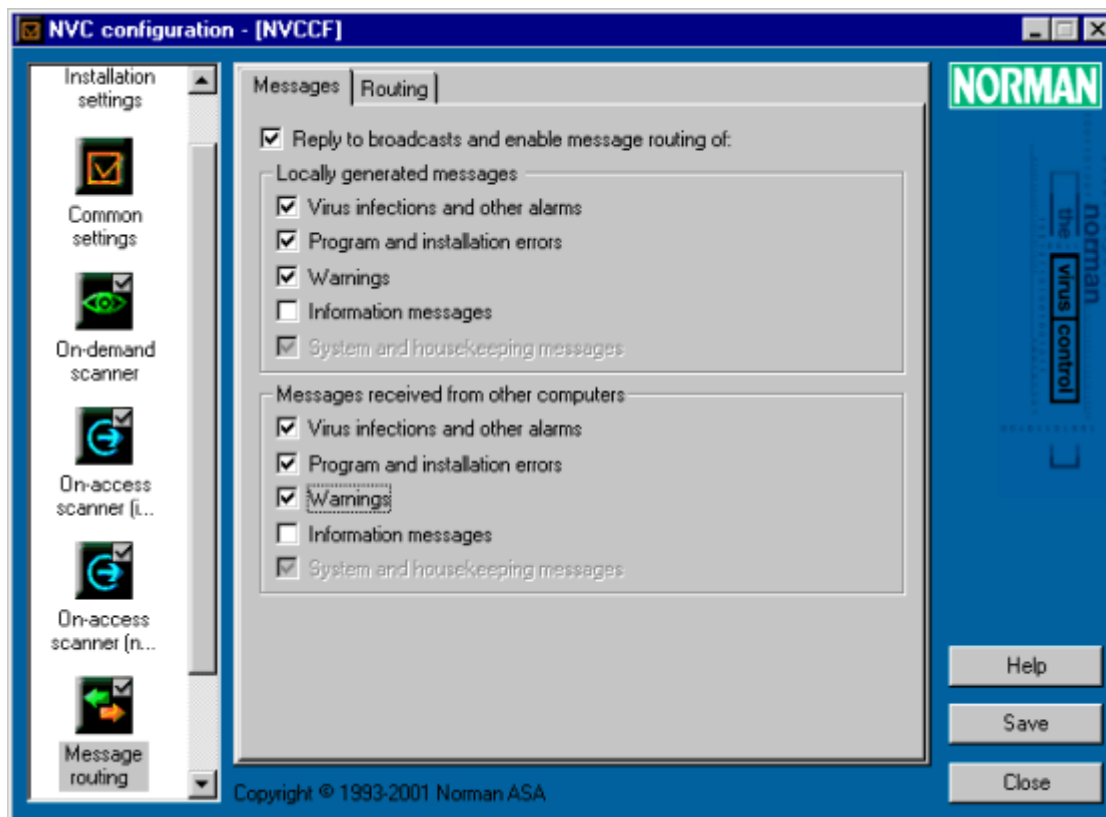
You should use the messaging tool to determine which incidents you wish to be warned about.

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 93). 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. You should consider very carefully before selecting this option. The reason is that *a lot* of information messages of a general nature are being generated.

☒ **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 IP address or machine 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

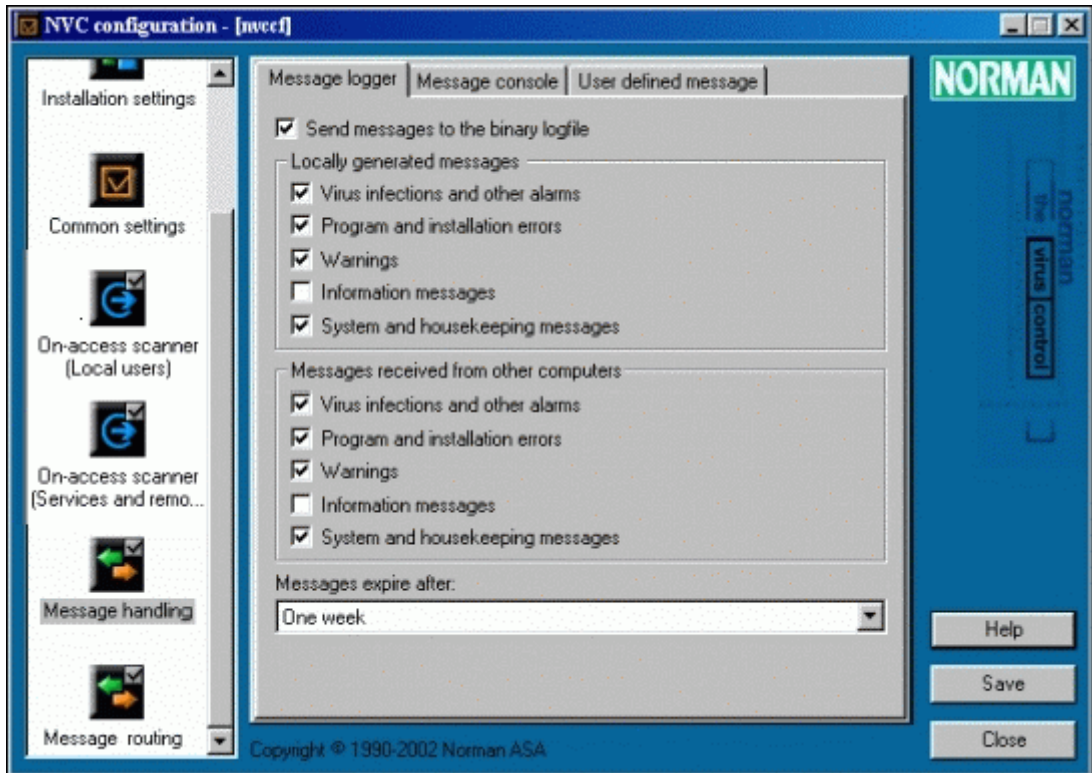
Message handling selects messages to a log file, displays messages on a message console, and decides what should go into the Event Log in Windows NT/2000. Therefore there are three tabs with identical options in this dialog. The selections you make decide which entries that appear in the NVC log file, 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 binary log file is encrypted and can only be viewed from the Utilities module (the Messages component). See page 93. Textual log files are also created, with the same criteria as the binary log file. All log files (textual as well as binary) are stored in the MSG directory in the directory where NVC is installed, normally `c:\norman\msg`.

### 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.

☐ **Information messages**

Create message of an informative nature. You should consider very carefully before selecting this option. The reason is that *a lot* of information messages of a general nature are being generated.

☒ **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 73.

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 89).

## User-defined message

When the On-access scanner detects an infection, the text you enter in this field will appear on the workstations. This message may contain exact instructions or reference to the company’s strategy for correct behavior when malware is at large in the network.

This message is also attached to messages broadcasted via NVC’s internal broadcasting system.

Make sure that the broadcast and routing options are enabled in the module **Message routing** (page 70). Also refer to the *Administrator’s Guide* for more information on how NVC handles messages and alarms.

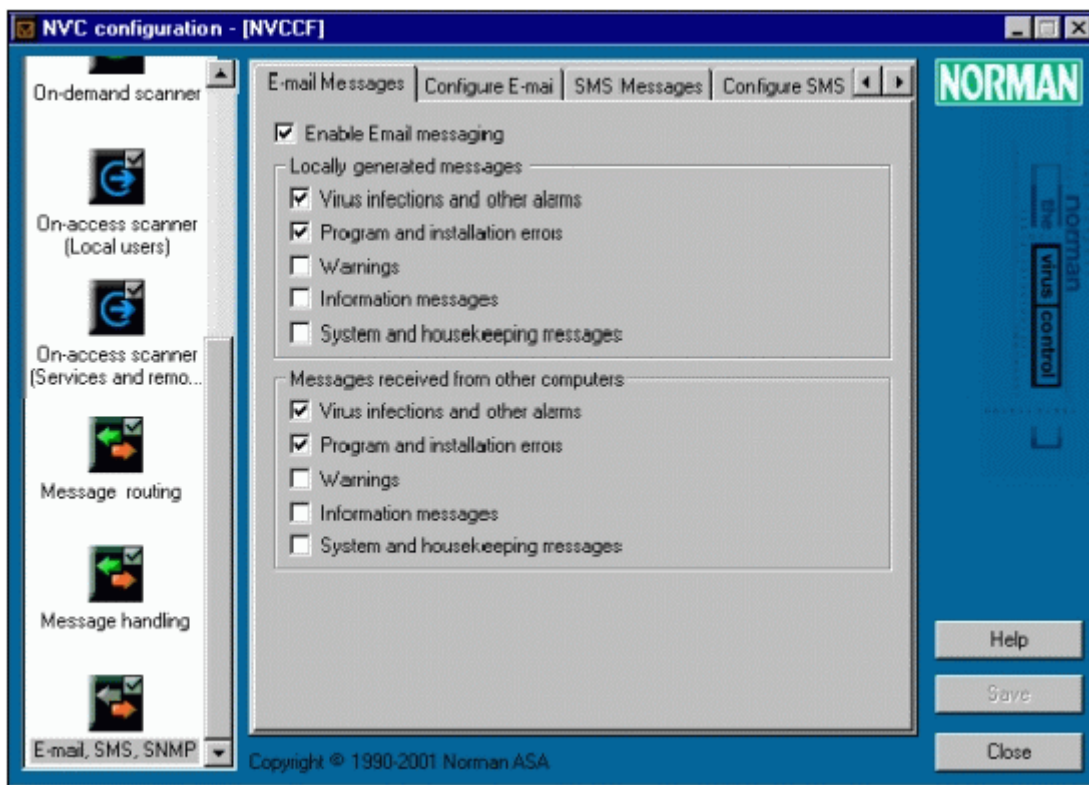
## E-mail, SMS, SNMP

This module provides the option of sending e-mails or SMS messages about selected events on standalone PCs as well as networked machines. For networks with SNMP, NVC can be configured to send SNMP traps.

## Messages for E-mail, SMS, and SNMP

You can filter the events that trigger an e-mail, a message, or a SNMP trap in exactly the same way as you select relevant events

for **Message routing** and **Message handling**, and from the same set of options:



As for the other messaging modules, you must distinguish between **locally** generated messages and messages **received** from other machines.

### Default values

Default values for local messages and messages received from other machines are:

#### ☒ **Virus infections and other alarms**

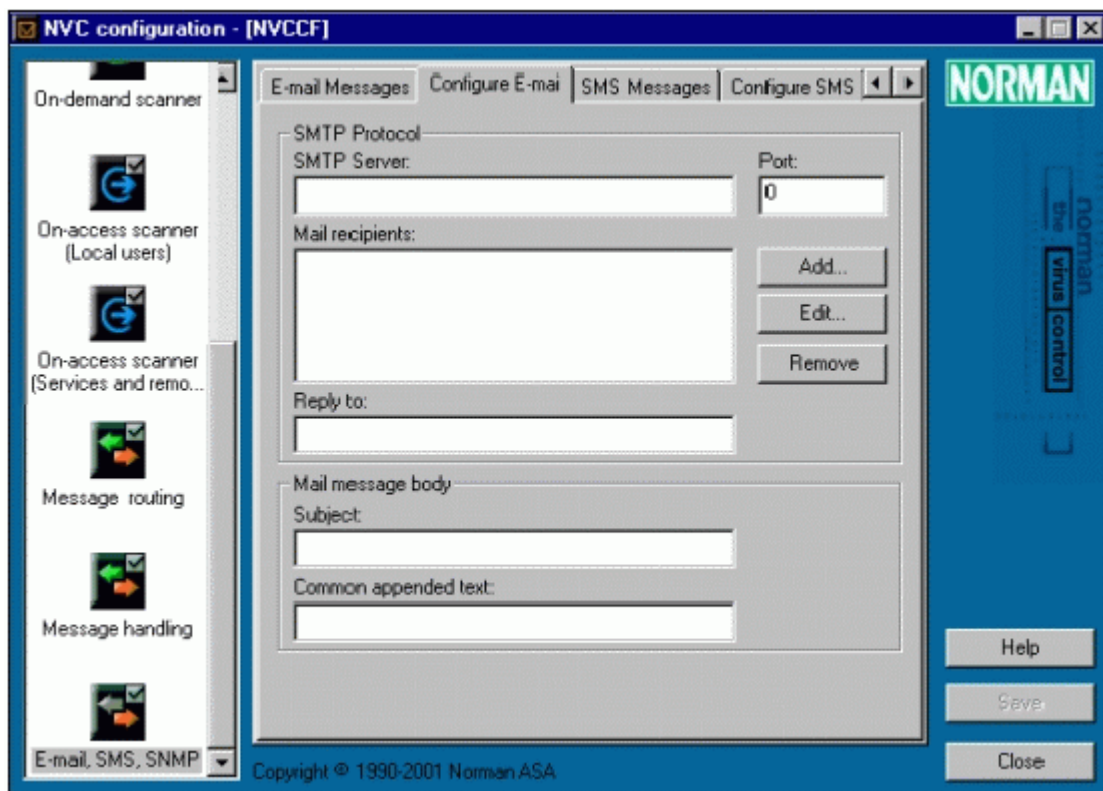
Forward message on virus detection or if other harmful code is found.

☒ **Program and installation errors**

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

For SMS messages, only the first option is the default value.

## Configure E-mail messages



These fields must be completed in the *SMTP Protocol* section of the dialog:

### SMTP Server

The server name or the IP address for the e-mail server which can receive the SMTP message.

**Port**

The default SMTP port is '25', which is the correct value unless you explicitly have selected another port.

**Mail recipients**

Enter the e-mail addresses to those who should receive the mail.

- Click on the **Add** button to enter the e-mail address for a mail recipient.
- Select an address from the list and click on **Edit** to change an existing address.
- Select an address from the list and click on **Remove** to delete an existing address.

**Reply to**

Enter the e-mail address to whom a recipient can reply to, for example the system administrator.

In the section *Mail message body*, you can specify:

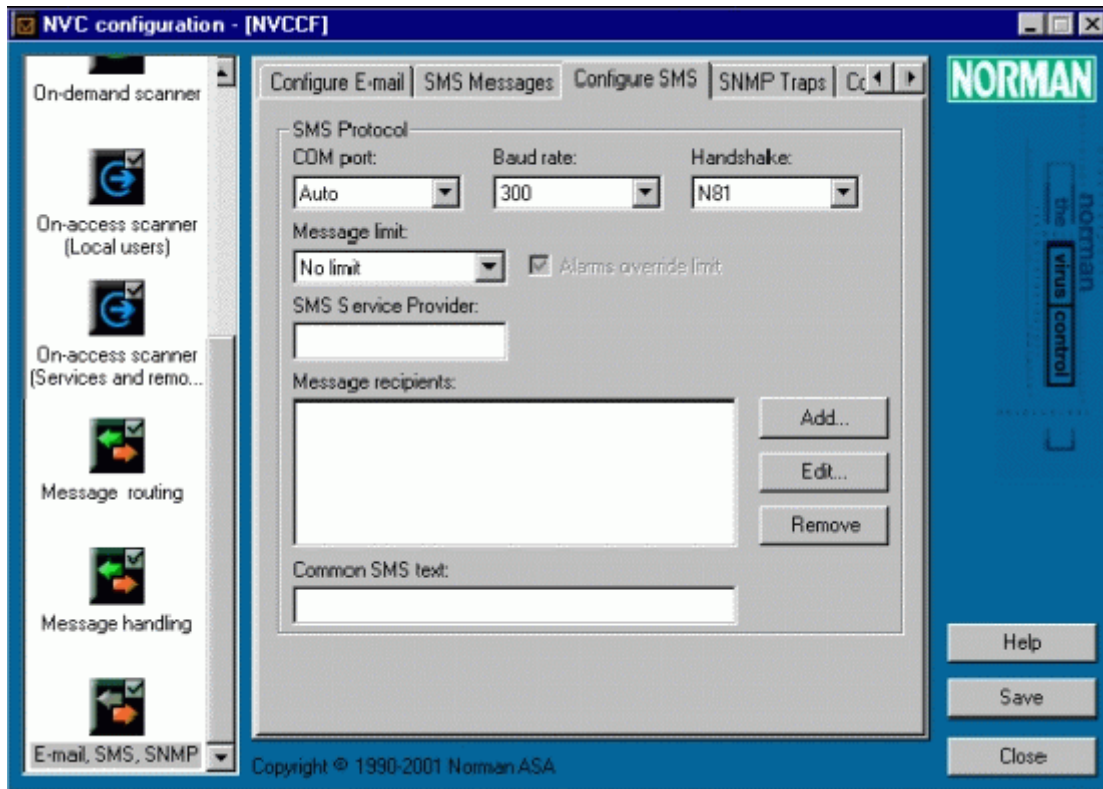
**Subject**

The title of the mail, for example "Message from NVC". It might be a good idea to reflect the event that triggered the mail, if you selected one alternative only, for example **Virus infections and other alarms**.

**Common appended text**

Enter the text you wish to include as the default footnote text in the mail.

## Configure SMS messages



Complete the following fields:

### COM port

Specify the SMS com port by choosing from the list in the pull-down menu. This is the port you specified when you set up your cellular phone as a modem with the driver supplied by the manufacturer. If you don't know the port number, select 'Auto' and let the program identify the correct port.

### Baud rate

The baud rate specifies the serial communication parameters that apply to the GSM modem. If you don't know the baud rate, please refer to the technical documentation for your modem. NVC supports the Extended Hayes command set for SMS -

“ETSI GSM 07.07”, and through testing found that the recommended modem is Falcom GSM Modem (for details, see: [www.falcom.de](http://www.falcom.de).)

### **Handshake**

The most common format for serial communication is **N81**. Click on the pull-down menu for more options.

### **Message limit**

You limit the number of messages you can send within a certain period of time. If you don’t want the ‘No limit’ default, select from the pull-down menu:

1/15 denotes one message per 15 minutes

1/hour denotes one message per hour, etc.

Note that if you select 1/15, for example, *all* messages beyond the first one within the time span of 15 minutes are lost.

### ☒ **Alarms override limit**

If you select a limit, i.e. any option except ‘No limit’, this option is by default *on*. This is to ensure that you don’t miss important messages (alarms) because less critical messages have used the specified quota. If you only specified ‘Virus infections and other alarms’ and the override option is on, there is no limit for alarms.

### **SMS Service Provider**

Enter the telephone number of your SMS service provider.

### **Message recipients**

Enter the telephone numbers for all recipients of the SMS messages.

- Click on the **Add** button to enter the phone number for a message recipient.
- Select an entry from the list and click on **Edit** to change an existing recipient.
- Select an entry from the list and click on **Remove** to delete an existing number.

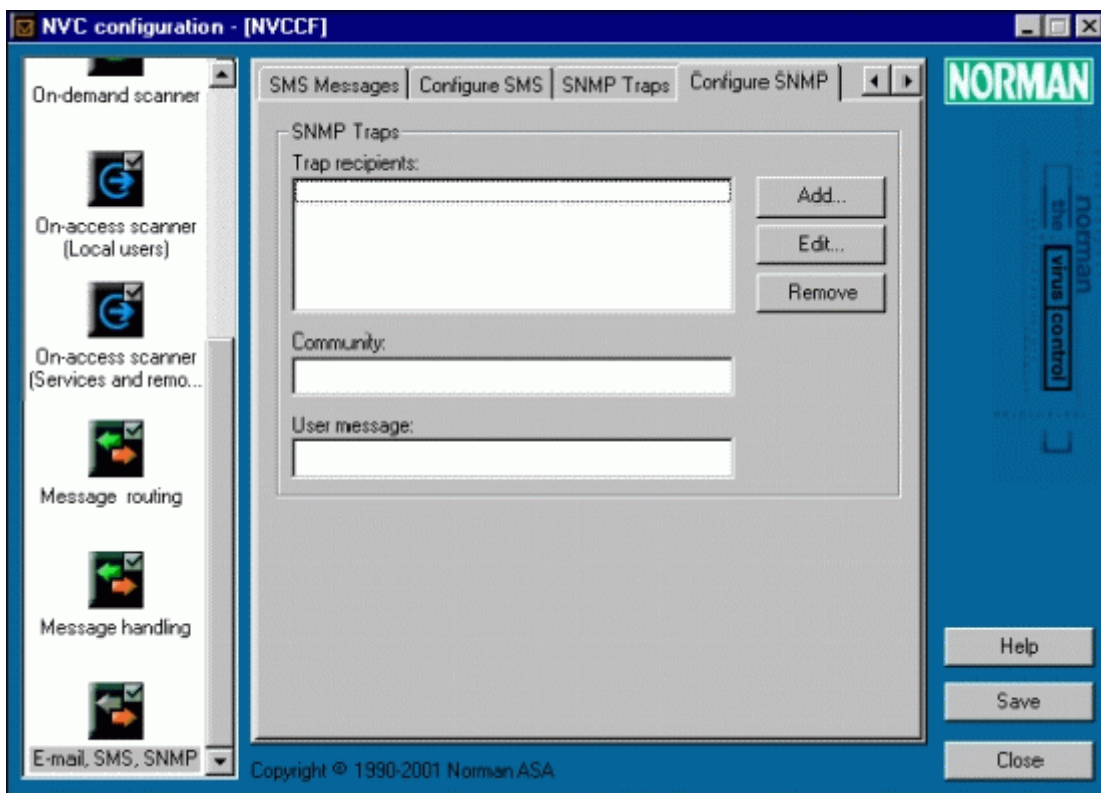
### **Common SMS text**

What the message is about, and that appears whenever a message is sent. It might be a good idea to reflect the event that triggered



the message, if you selected one alternative only, for example **Virus infections and other alarms**. This message can be “Call SysAdm”, for example. Note that the maximum length of the message is 12 characters.

## Configure SNMP



Complete these fields to enable SNMP traps:

### Trap recipients

Enter the machine name or the IP address for the recipient(s).

- Click on the **Add** button to enter the name or address for a SNMP recipient.
- Select an entry from the list and click on **Edit** to change an existing address.

- Select an entry from the list and click on **Remove** to delete an existing address.

**Note:** Recipients should have Norman's MIB installed to make sure that the trap is decoded correctly.

### **Community**

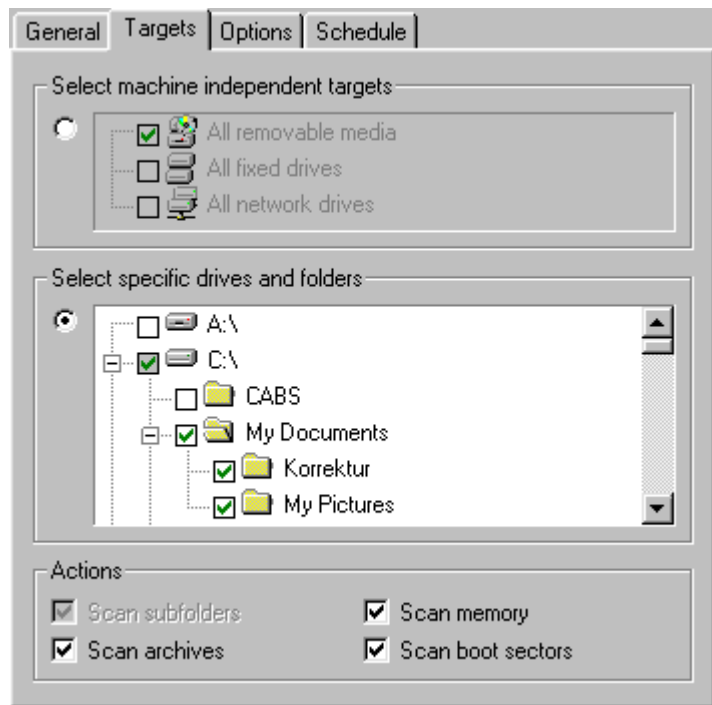
Each SNMP managed object, like a trap, belongs to a community. The authentication is based on plain text community name, which you must enter here. "Public" is frequently used as community name.

### **User message**

This field is for a common, user configurable text, for example "Something went wrong with..."

# 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 89).

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 89.

## 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:

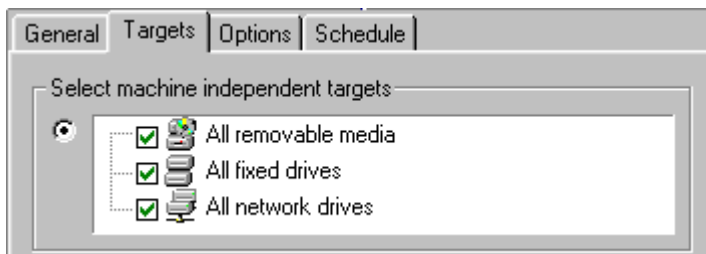
1. Click on the radio button ☐ to activate the section you wish to select from.

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.

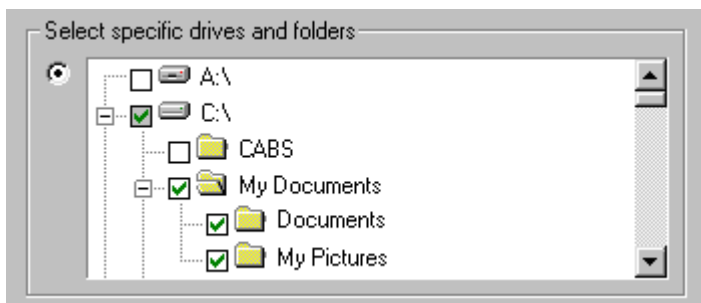
#### ☒ **All fixed drives**

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. The following formats are currently supported: ZIP, ARJ, RAR, ACE, ARC, GZIP, TAR and BZIP2.

☒ **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:

#### ☐ **Automatic: 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.

#### ☐ **Automatic: 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.

#### ☒ **Automatic: 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.

#### ☐ **Manual start: Normal window**

Instructs NVC to run in an open window during scanning. When you schedule a scan with this 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.

**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 - waiting for restart*, *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.



You can run task files from the command line. This process involves starting the on-demand scanner and run a specific task from the command line hidden for the user.

⇒ See 'Running task files from the command line' on page 102.

### 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**

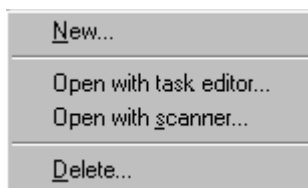
Displays at which day, month, and time the task file will run next. If the task is not scheduled, this field is empty.

**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 33), files that qualify for quarantine will appear as a list in this dialog box. These files are either infected, have an unknown format, or are blocked by Norman Internet Protection (NIP). Please refer to 'Attachment blocking' on page 60.

### Fields in the Quarantine dialog box

#### **Quarantined file**

Displays path (if applicable) and file name of the quarantined file. In some situations a path cannot be displayed, for example for e-mail attachments which always are checked in a temporary area on disk.

#### **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. For e-mail attachments, only a file name appears and you must use the **Save As** option.

#### **Save As**

Save the file with the name and location you wish.

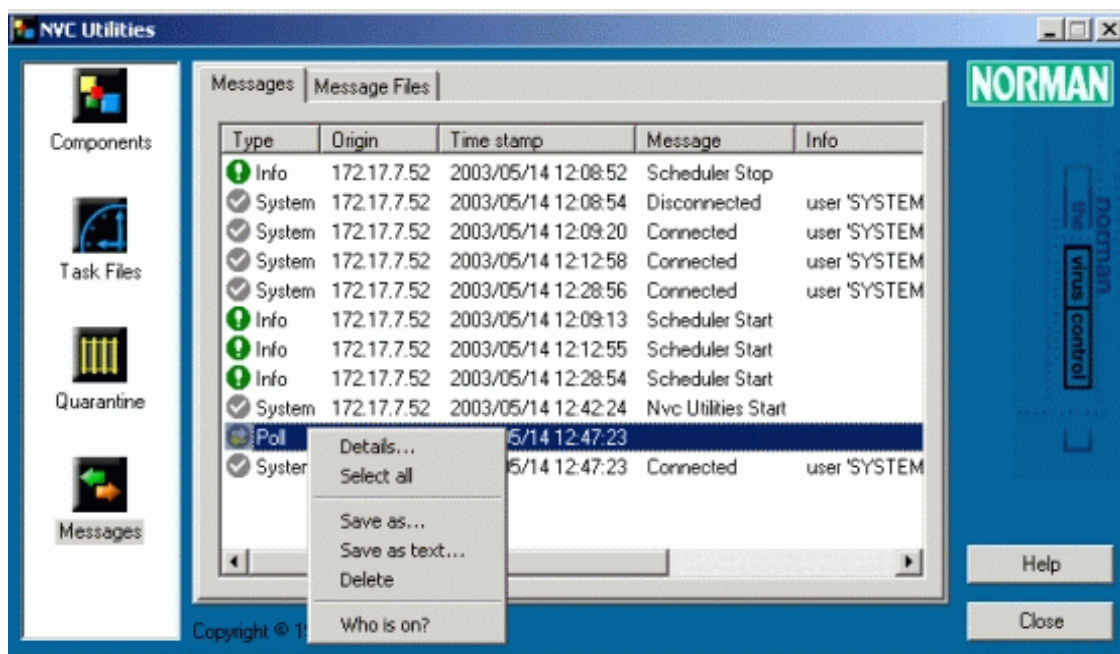
#### **Delete**

Deletes the file altogether.

# Messages

## Messages tab

If you have enabled the message service (see ‘Message logger’ on page 73), 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 messages/entries 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.

**Save as text**

Saves the selected entries to a text file with whatever name you like.

**Delete**

Deletes the entry.

**Who is on?**

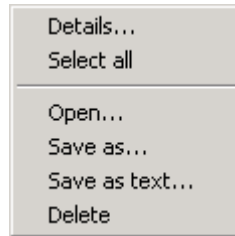
Broadcasts the message.

## **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, **Internet** tab. If you select **On direct access at specified times** and then click the **Specify** button, you can enter the intervals when you check for updates:



**Note:** These options are also discussed in the section ‘Internet’ on page 27.

The option **On-demand only (start manually)** 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 (wait for 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 **On direct access at specified times**. This allows you to plan when NIU should run and possibly integrate NVC updates with other planned tasks. See top of this page.

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 proxy server settings on page 30.

## 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. As the name suggests, it is busier in a network than on a stand-alone computer, and therefore discussed more exhaustively in the *Administrator’s Guide*.

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. Note that the collaboration between Zanda and NIU is particularly important during updates: An update is *not* completed until Zanda has unpacked and installed the new files.

The agent is always running.

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

- Handle NVC updates.
- Ensures that modules start as they are configured to do.
- 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 22.

- Features its own scheduler.

Please refer to the *Administrator's Guide* for more details about the agent.

## 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:

```
nvcc [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 103 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.

Note that malicious code such as **trojans**, where the entire file is the malefactor, there is nothing to repair. In such situations the only cure is to *delete* the entire file. That's why we sometimes use the expression "Cleaning by deletion".

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.

## Running task files from the command line

You can start NVCOD from the command line in order to run a task file from this environment.

NVCOD can use an existing task file if you enter the following command:

```
NVCOD @<path to the task file>
```

The function is useful since the task will run hidden from the user, for example as a method of scanning in login scripts.

Example:

You have created a task called `myscan.sdf`. The file is located in the default library `c:\norman\nvc\tasks`. You want to scan the machine with the options specified in the task file rather than scan the entire hard disk using the option **Scan hard disks**.

From the command line, you enter:

---

```
c:\norman\nvc\bin>nvcod.exe @c:\norman\nvc\tasks\myscan.sdf
```

## Command line scanning options

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

```
nvcc /?
```

from the command line to display a list of available options. The following tables chart out the available parameters and their functions.

Param.:	Function:
/- help	Show help.
/?	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.
/B	Do not sound alarm when infections are found (default OFF).
/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 (default OFF).
/BS+	Scan system areas only.
/C:	Scan archive files. /C: 0 no, /C: 1 yes (default in config).
/C	Scan archive files. Same as /C: 1 (default in config).
/CP	Scan compressed program files (default OFF).
/CL:	Repair files and boot sectors: /CL: 0 no, /CL: 1 yes, /CL: 2 also within archives (default in config).

<b>Param.:</b>	<b>Function:</b>
/CL	Repair files and boot sectors. Same as /CL:1 (default in config).
/CZ:	Max archive file size in Kb. Implies /C (default in config).
/CR:	Max archive file recursive depth. Implies /C (default in config).
/FLOPPY	Read NSE files from separate floppy (DOS only).
/H	Show help.
/HUM	Handle uncertified macros (needs NSE\NVCMACRO.CRT from CatsClaw).
/L:	Set logging level: /L:0=no, 1=yes, 2=verbose (default in config).
/LD:	Specify directory for log files (default directory in config).
/LF:	Specify fully qualified log file name (overrides LD: and /LG:). Type in the name immediately after the parameter (no spaces).
/LG:	Specify number of log file generations (default number in config).
/N	Suppress the default memory scan.
/O	Ignore locked files (default OFF).
/Q	Quiet mode, i.e. no screen output at all (default OFF).
/R	Repeat the scan. Useful for checking several floppies (default OFF).
/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. Default when scanning drives.
/SB	Use sandbox. 0=Off, 1=On



Param.:	Function:
/SN	Do not allow user aborts (default OFF).
/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 (default OFF).
/V	Verbose mode (default OFF).
/W:	Wait specified number of milliseconds between each file (default 0).
/YH	Abort when infection found (default OFF).

## 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 `nvcc.exe` is installed, type:

```
nvcc c:\*.exe /s /u /cl /lf:myscan.log
```

This will scan all files with the extension `.exe` on the local `c:` drive including subdirectories. The scanner will not stop if infected files are found, possible infected files are cleaned, and the `myscan.log` will be created in the directory where `nvcc.exe` is installed.

Then type:

```
nvcc *.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.
11	Some files or archives were found corrupted.
10	All files could not be opened for scanning.
9	Scanning aborted by user.
8	Internal error: Scanning aborted.
7	Warning. Some components as Nlog5.dll not found.
6	Disk input/output error.
5	Usage error: Illegal parameter or parameter argument given.
4	The hardware configuration has changed since you installed the scanner.
3	Usage error: The scan began without having any scanning criteria.
2	Virus found active in memory and removed.
1	Virus found and/or repaired. This error code overrides all other error codes except for 2.
0	Everything OK. No virus or other malicious code found.

# Appendix A - Sandbox

## Background

The vision of inventing a method that automatically detects new, unknown viruses is as old as the antivirus industry itself. Throughout the years, the AV business has invested significant resources to come up with a solution which could fulfill this ambitious goal.

At the Virus Bulletin Conference in 2001, Norman produced a fully functional prototype of a scanning engine with sandbox functionality.

## What is a sandbox?

Sandbox is the term that best describes the technique that is used to check if a file is infected by an unknown virus. The name is not randomly picked, because the method allows untrusted, possible viral code to play around on the computer – not in the real computer, but in a simulated and restricted area within the computer. The sandbox is equipped with everything a virus expects to find in a real computer. This is a playground where it is safe to let a virus replicate, but where every step is carefully monitored and logged. The virus is exposing itself in the sandbox, and because its actions have been recorded, the cure for this new perpetrator can be generated automatically.

Today, a new e-mail worm can infect ten thousands of workstations in a matter of seconds. The AV vendors are expected to find the cure, update the virus definition files, and distribute these to its customers immediately. The need for speed is imperative, because the nature of today's malware is such that a "successful" piece of viral code can paralyze networks and cause serious damage to an unlimited number of computers.

## Sandboxing techniques

### *Sandboxing using emulation*

A computer virus is a computer program, defined through its behavior. It will transfer code/data to other computer files. When these other computer file in turn is given control, the virus code is somehow activated, trying to infect other computer files. This process is called replication. For a computer program to be called “viral”, it must be able to perform this task recursively.

Norman’s sandbox is a virtual world where everything is simulated. It is powered by an emulator, and together they let possible virus infected binary executables “run” just as they would do on a real system. When execution stops, the sandbox is analyzed for changes.

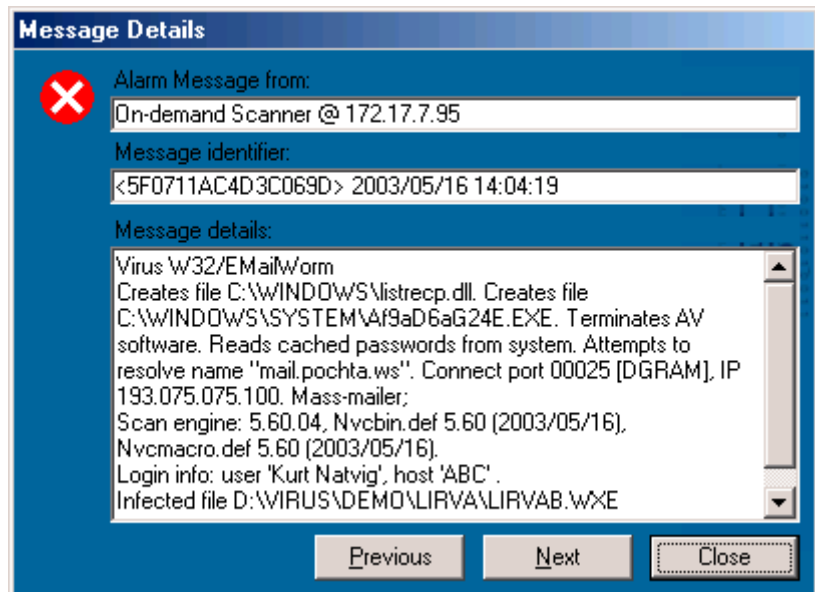
### *Sandboxing using a virtual machine*

It is also possible to build a sandbox by creating a VM (Virtual Machine). The idea is to block all exits, so the executable you are examining cannot escape. However, we don’t consider this solution as safe enough. There will always be “another” exploit of the PC’s processor, some weird interrupt/exception/fault etc. that will allow malicious code to escape a VM, and spread to your real system.

## How does sandboxing affect the user?

The fundamental idea about the sandbox is to offer better protection for the user. A major challenge is to integrate the new technology in the product without slowing down scanning speed. The other capital problem —false alarms—has already been solved. Norman’s sandbox technology is officially introduced with NVC v5.60, even though it has been “covertly” used by the scanning engine for some time. But as of v5.60 the sandbox is visible among the configuration options in certain modules.

If new malicious code is detected, the administrator is notified by a message similar to this:



Considering the advanced technique involved in this process, scanning time increases slightly with the sandbox option on. However, it's a low price for the possible gain of stopping a network worm, for example.

## What to do when the sandbox detects a new virus

First of all you should check that your NVC installation is up-to-date with the latest virus definition files. If NVC is outdated, the sandbox might have found a virus which is *now* entered in the definition files.

If it proves to be a new virus, we would appreciate that you zip the infected file, password-protect the zip file, and send it *analysis@norman.no*. This procedure is also described at our web site.

For more details on Norman's sandbox technology, please refer to previously published white papers on the subject. They are available at Norman's web site:

[http://www.norman.com/documents/nvc5\\_sandbox\\_technology.pdf](http://www.norman.com/documents/nvc5_sandbox_technology.pdf)

[http://www.norman.com/documents/nvc5\\_sandbox\\_technology\\_2002.pdf](http://www.norman.com/documents/nvc5_sandbox_technology_2002.pdf)

# 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](http://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](mailto:documentation@norman.no).

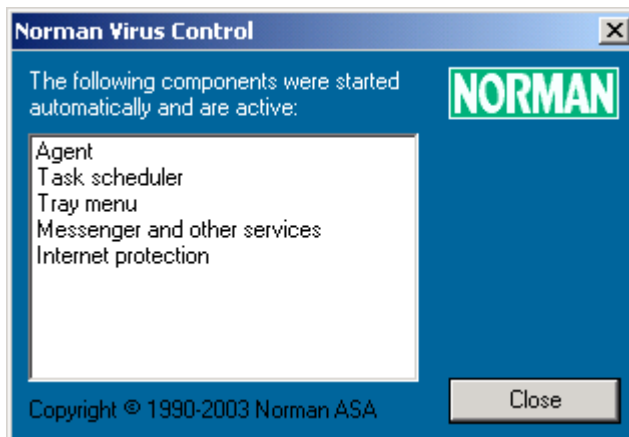
## How do I start NVC?



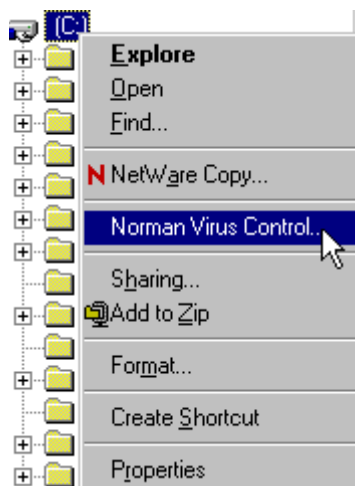
NVC's key components are started automatically when the operating system is loaded. Look for the little green Norman 'N' in the system tray:

## 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. If you stop the on-access scanner, it will not start again in the current session or after rebooting unless you do it manually. You can stop and start the on-access scanner from a separate entry in the menu (system tray), or 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.

### **NVC in addition to other antivirus software**

"After installing NVC in addition to an antivirus solution from another vendor, the computer freezes completely and I receive lots of error messages."

Different antivirus products may "quarrel", as they often want to scan the same files at the same time. This may affect the stability of your PC and create unwanted behaviour

*Recommendation:* You should uninstall other anti virus software before installing NVC.

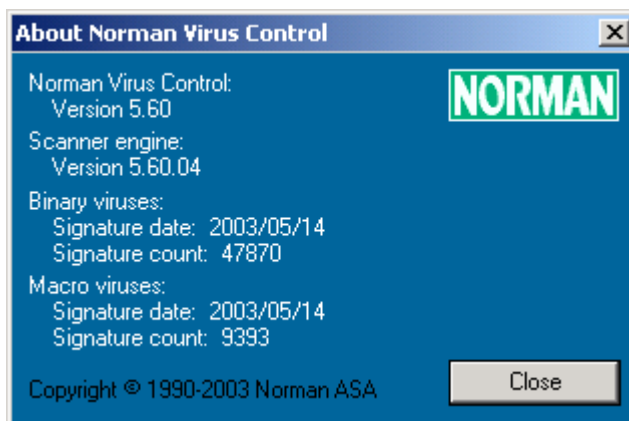
If you experience this problem on Windows NT4, 2000, or XP, you may have to start your PC in safe mode before you can uninstall one of the conflicting antivirus products. To start the PC in safe mode, press F8 during boot, before Windows is loading.

### **NVC5 and version numbers: How can I verify that NVC is up-to-date?**

You can find NVC's version number by choosing **About** from the tray icon menu (N).

Here you will find version numbers for NVC, as well as version numbers for the scanner engine, and the creation date for the virus definition files, for the binary viruses and the macro viruses respectively:





To consider Norman Virus Control as up-to-date, the signature dates for the virus definition files should not be more than 10-12 days older than the current date. In addition, make sure that all available updates to other NVC components are downloaded and installed.

Don't worry if the scanner engine's version number differs from the current version number of NVC. The scanner engine features its own internal version number.



# Index

## —A—

ACE 86  
 Additional path elements 26  
 administrator's rights 18, 49  
 Agent  
   zanda.exe 100  
 Aggressive commercials 37, 48  
 Alarms override limit 80  
 ARC 86  
 ARJ 86  
 At default intervals 23  
 At user-defined intervals 23  
 Attachment blocking  
   Attachment list 62  
   Block all attachments 61  
   Block all attachments listed below 62  
   Block all attachments, except those listed below 62  
   Block any attachment with double extensions 61  
   Block any CLSID extensions 62  
   Security level 63  
   string 63  
 authentication 30  
 Authentication key for installation/update 21  
 Automatic - Hidden until cleaning fails 87  
 Automatic - Minimized until cleaning fails 87  
 Automatic - Minimized until infection found 87

## —B—

Back up files to quarantine before repair 34  
 baud rate 79

Block all attachments 61  
 Block all attachments listed below 62  
 Block all attachments, except those listed below 62  
 Block any CLSID extensions 62  
 block attachments (NIP) 60  
 Block attachments with double extensions 61  
 boot sector virus 35, 50, 102  
 BZIP2 86

## —C—

CLSID extensions 62  
 COM port 79  
 Combining different parameters 105  
 command line scanner 101  
 Common settings  
   Aggressive commercials 37  
   New, unknown viruses 37  
   Security risks 47  
 Community 82  
 Components  
   Internet tab 97  
 Configuration editor 12  
 Conventions iv  
 Create log file 39

## —D—

Daily on dial-up (wait for connection) 29  
 Daily on dial-up connection (wait for connect) 28, 29  
 Daily on direct connection at scheduled time 29  
 default.ndf 56  
 Definition  
   DLL 55  
   news reader 53  
   protocol 53  
   Winsock 53  
 dial-up connection 24  
 Do not use Internet - update from CD 28

double extensions 61  
Dynamic Link Library (DLL) 55

## —E—

e-mail 75  
email worms 37, 60  
E-mail, SMS, SNMP  
    Default values 76  
    Program and installation errors 77  
    Virus infections and other alarms 76  
environment variable 26  
Exclude from scan 38, 48

## —F—

Files of indeterminate format 38  
Files on exclude list 38  
Files on network drives 38  
Floating Point Unit (FPU) 12  
Forward messages 72

## —G—

GSM modem 79  
GZIP 86

## —H—

Handle files that cannot be scanned 49  
Handshake 80  
HTTP proxy 97

## —I—

Incoming e-mail 60  
Information messages  
    Message routing 71  
Install tab  
    Additional messenger protocols 20  
    Authentication key for installation/update 21  
    Command line scanner 19  
    Internet protection 20  
    Internet update 20  
    Language 20

On-access scanner 19  
On-demand scanner 18  
Release notes 20  
Task editor 19  
Task scheduler 19  
Utilities 19

### Internet tab

Daily on dial-up (wait for connection) 29  
Do not use Internet - update from CD 28  
Log on to proxy server 31  
On direct connection at specified times 29  
On-demand only (start manually) 29  
Proxy server 30  
Update distribution server 29  
Use a proxy server 30  
When to look for updates on the Internet 28

### Internet Update 12

Internet update 20  
NIU 96

## —L—

### LAMN/WAN tab

Logon credentials 31

### LAN/WAN

Automatically from server 99

### LAN/WAN tab

At default intervals 23  
At user-defined intervals 23  
Distribution server name 24  
Network type 24  
Never (update from CD or Internet) 22  
Novell NetWare 24  
Share name 24  
Update software from 25  
Update task files from 26  
User-defined paths 25  
Volume name and root directory 24

- 
- Where to look for updates on the LAN/WAN 24
  - Windows NT/2000/XP 24
  - Workgroup or peer-to-peer network 24
  - Linux iv
  - Log file 73
    - generations to keep 40
  - Log file path 39
  - Log on to proxy server 31
  - Logon credentials 31
- M—**
- malware 50
  - Manual start - Normal window 87
  - Maximum size of quarantine (% of partition size) 34
  - Maximum time to keep file in quarantine 33
  - Memory, scanning 86
  - message console 75
  - Message files tab
    - Right-click options 95
  - message limit 80
  - Message logger
    - Information messages 74
    - Locally generated messages 74
    - Messages received from other computers 74
    - Program and installation errors 74
    - Send messages to the binary log file 73
    - System and housekeeping messages 74
    - Virus infections and other alarms 74
    - Warnings 74
  - Message routing
    - Information messages 71
    - Messages received from other computers 71
    - Program and installation errors 71
    - Reply to broadcasts and enable message routing of 70
  - System and housekeeping messages 71
  - Virus infections and other alarms 71
  - Warnings 71
  - Messages
    - Fields in the Messages tab 93
  - Messages tab
    - Info 94
    - Message 94
    - Origin 93
    - Right-click options 94
    - Time stamp 94
    - Type 93
  - Messaging
    - E-mail 69
    - SMS 69
    - SNMP 69
  - Minimized until infection found 87
  - Minimum time to keep file in quarantine 33
  - Move unrepairable files to quarantine 34
  - Multi Media Extensions (MME) 12
- N—**
- network worms 37, 60
  - Never (update from CD or Internet) 22
  - New, unknown viruses using sandbox 37
  - news reader 53
  - Newsgroups 60
  - NIP
    - attachment blocking 60
    - block file types 63
    - block specific attachments 63
    - default.ndf 56
    - Display message for local user 64
    - Mail message to local recipient 64
    - Mail message to remote sender 64
    - POP 66
    - Port numbers 66
    - SMTP server for forwarding messages 66
  - NIP configuration
-

- Incoming e-mail 60
  - Newsgroups 60
  - NNTP 66
  - Outgoing e-mail 59
  - POP 66
  - SMTP 66
  - Use sandbox 60
  - nip.exe 56
  - niphk.dll 55
  - NIU 27
    - Daily on dial-up (wait for connection) 97
    - downloading packets 98
    - On-demand only (start manually) 97
    - packages 98
  - NIUcf 27
  - niucf.exe 98
  - NNTP (Network News Transfer Protocol) 66
  - Norman Internet Update 27
    - Configuration Settings 97
  - Novell NetWare 24
  - NVC components 14
  - NVC group 13
  - NVC modules 13
  - NVC update 21
- O—**
- On demand scanner
    - Exclude from scan 38
    - Scan for 37
  - On direct connection at specified times 29
  - On-access scanner 19, 20
    - Ask user what to do 50
    - Deny access 50
    - Display warning 49
    - Display warning and deny access 49
    - Exclude from scan 48
    - Files of indeterminate format 48
    - Files on exclude list 48
    - Files on network drives 48
  - Handle files that cannot be scanned 49
  - Ignore 49
  - Remove 50
  - Scan files before they are used 46
  - Scan new or changed files 46
  - Strategy 45
  - Use scanning mode for services and remote users only 49
  - Virus removal 50
  - On-access scanner (Local users)
    - Scan files before they are used 46
    - Scan new or changed files 47
    - Strategy 46
  - On-access scanning
    - Aggressive commercials 48
  - on-access scanning
    - Terminal services 67
  - On-demand only (start manually) 29
  - On-demand scanner 18, 21
    - Aggressive commercials 37
    - create log file 39
    - Files of indeterminate format 38
    - Files on exclude list 38
    - Files on network drives 38
    - Log infections and errors only 40
    - New, unknown viruses using sandbox 37
  - Right-click scanner 35
  - Scan archive files by default 41
  - Security risks 37
  - Verbose logging 40
  - OS/2 iv
  - Outgoing e-mail 59
- P—**
- Parameters
    - combining 105
  - password crackers 37, 47
  - permanent connection 24
  - POP (Post Office Protocol) 66
  - port numbers 66
  - Program and installation errors
    - Message routing 71

Protocol  
     NNTP 53  
     POP3 53  
     SMTP 53  
 protocol 53  
 proxy 30  
 Proxy server 30  
 Proxy server logon credentials  
     Domain (for Windows NT chal-  
     lenge/response) 31  
     Password 31  
     User name 31

## —Q—

Quarantine  
     Options 34  
 Quarantine properties 33  
 Quarantine tab  
     Back up files to quarantine before  
     repair 34  
     Move unrepairable files to quaran-  
     tine 34  
 Quarantined files  
     Right-click options 92

## —R—

RAR 86  
 remote administrative tools 37, 47  
 removing viruses 101  
 repairing files 102  
 Reply to broadcasts and enable mes-  
     sage routing of  
     Message routing 70  
 Requirements, system iv  
 Resource usage 87  
 right-click scanner 35  
 rights 18, 49

## —S—

sandbox 37, 60  
 Sandboxing  
     emulation 108  
     virtual machine 108

Scan archive files by default 41  
 Scan files before they are used 46  
 Scan for viruses, trojans, worms, etc 47  
 Scan new or changed files 46, 47  
 Scheduled task 88  
 Security risks 37, 47  
 Select machine independent targets 85  
 Select specific drives and folders 85  
 Send messages to the binary log file 73  
 Send messages to the message console  
     75  
 SMS 69  
 SMS configuration  
     baud rate 79  
     COM port 79  
     Common SMS text 80  
     Community 82  
     Handshake 80  
     Message limit 80  
     Message recipients 80  
 SMS messages 75  
 SMS Service Provider 80  
 SMTP (Simple Mail Transport Proto-  
     col) 66  
 SMTP port 78  
 SMTP Server 77  
 SMTP server for forwarding messages  
     66  
 SNMP 69  
     Trap recipients 81  
 SNMP traps 75  
 Specify paths  
     Additional path elements 26  
     environment variable 26  
     Server name 25  
     Share name 25  
     Update configuration files from 25  
     Volume name and root directory  
     25  
 Start tab  
     On-access scanner 21  
     Task scheduler 21  
 System and housekeeping messages  
     Message routing 71

System requirements iv  
system tray 14

## —T—

TAR 86  
Task editor 12, 19, 83  
    All fixed drives 85  
    All network drives 85  
    All removable media 85  
    Frequency 88  
    General tab 84  
    Hidden until cleaning fails 87  
    Minimized until cleaning fails 87  
    Minimized until infection found  
        87  
    Normal window 87  
    Options tab 87  
    Resource usage 87  
    Scan archives 86  
    Scan boot sectors 86  
    Scan memory 86  
    Scan subfolders 86  
    Scanner window 87  
    Schedule tab 88  
    Scheduled task 88  
    Select machine independent tar-  
        gets 85  
    Select specific drives and folders  
        85  
    Selecting targets 84  
    Start date/time  
        88  
    Targets tab 84  
    Universal Time Coordinates 88  
task file  
    schedule 90  
Task files  
    Last run time 91  
    Next run time 90  
    Right-click options 91  
    Schedule 90  
    Task file 90  
Task scheduler 19, 21

TCP/IP 96, 97  
terminal services 67  
trojans 57

## —U—

Update configuration files from 25  
Update distribution server 29, 30  
Update software from 25  
Use a proxy server 30  
Use sandbox 60  
User-defined paths 25  
UTC 88  
Utilities 12, 19  
    Components 89  
    Components dialog box 89  
    Message files tab 94  
    Messages tab 93  
    Quarantine dialog box 92  
    Task files 90  
Utilities module 89

## —V—

view quarantine 91  
Virtual Machine (VM) 108  
virus definition file 21  
Virus infections and other alarms  
    Message routing 71

## —W—

When to look for updates on the Inter-  
    net 28  
Where to look for updates on the LAN/  
    WAN 24  
Windows NT/2000 terminal services  
    67  
Windows NT/2000/XP network 24  
Winsock 53, 56  
winsock.dll 53  
Workgroup or peer-to-peer network 24

## —Z—

Zanda 100