NORMAN

Norman Virus Control for Workstations

Version 5.0

User's Guide

Limited warranty

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

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

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

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

This warranty expires 30 days after purchase.

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

The Norman logo is a registered trademark of Norman ASA.

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

NVC documentation and software are

Copyright © 1996-2000 Norman ASA.

All rights reserved.

November 2000

Norman Offices

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

Denmark
Norman Ibas A/S
Nordre Strandvej 119 A, DK-3150 Hellebæk, **Denmark**
Tel. +45 7022 3400 Fax: +45 7022 3401
E-mail: info@normanibas.dk Web: http://www.norman.com

Norman Ibas OY
Läkkisepäntie 11, 00620 Helsinki, **Finland**.
Tel: +358 9 2727 210 Fax: +358 9 2727 2121
E-mail: norman@norman-ibas.fi Web: http://www.norman-ibas.fi

Norman Data Defense Systems GmbH
Kieler Str. 15, D-42697 Solingen, **Germany**.
Tel: +49 212 267 180 Fax: +49 212 267 1815
E-mail: norman@norman.de Web: http://www.norman.de

Norman/SHARK BV
Postbus 159, 2130 AD, Hoofddorp, **The Netherlands**.
Tel: +31 23 563 3960 Fax: +31 23 561 3165
E-mail: sales@norman.nl Web: http://www.norman.nl

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

Norman Data Defense Systems AG
Postfach CH-4015, Basel, **Switzerland**.
Tel: +41 61 487 2500 Fax: +41 61 487 2501
E-mail: norman@norman.ch Web: http://www.norman.ch

Norman Data Defense Systems (UK) Ltd
Lawn Farm, Oakhill Road
Woodhill, Milton Keynes, Bucks MK5 6AH, **United Kingdom**.
Tel: +44 1908 520 900 Fax: +44 1908 520 909
E-mail: norman@normanuk.com Web: http://www.normanuk.com

Norman Data Defense Systems Inc.
9302 Lee Highway, Suite 950A, Fairfax, VA 22031, **USA**
Tel: +1 703 267 6109, Fax: +1 703 934 6367
E-mail: norman@norman.com Web: http://www.norman.com

Conventions

We use the following conventions throughout this manual:

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

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

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

[Ctrl]

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

Start|Run

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

Important notes appear in boxes like the one below:

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

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

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

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

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

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

System requirements

Norman Virus Control (NVC) v5.0 can run on any machine that runs any national language version of Windows 95 / 98 / Me, Windows NT 4 (SP 5), and Windows 2000.

Who should read this manual?
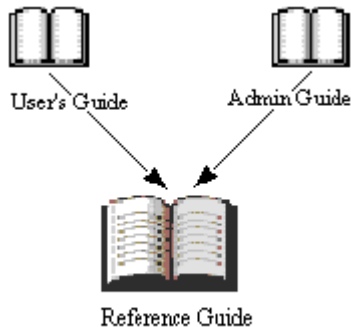
This manual is primarily aimed at end-users who want a brief introduction to NVC's basic functionality without getting too technical. All main functions are outlined, including the installation procedure.

Other NVC manuals

In addition to this manual, the *Administrator's Guide* covers topics that are particularly useful for those responsible for network installations. Finally, the *Reference Guide* provides detailed information on all functions found in NVC, and this manual is useful for administrators as well as single-users.

About this version

NVC v5.0 is currently available in English only. Other language versions will follow shortly. Check Norman's web sites for details, or contact your local dealer for more information about language versions.

The list in the "About" box provides all the necessary contact information about Norman's subsidiaries and distributors.

Prerequisites

To take full advantage of all the functions in NVC, you should have some experience with the Windows 32-bit platform and applications that run on this platform.

NVC is designed to work with the operating system at all levels, and you will find that basic Windows functionality is reflected in the program.

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

Installing NVC

Note:	The NVC CD is equipped with an autorun program that is launched when the CD is inserted. If you have turned the autorun function *off*, you must select `setup.exe` under the appropriate language folder. The structure is `D:\NVC5\<Language>\setup.exe.`

1. Close all Windows applications.

2. Insert the CD and select language and installation type from the menu. Installation type can be single-user or network installation. Refer to the *Administrators's Guide* for instructions on how to install NVC in a network.

3. Follow the instructions on the screen.

The setup program uninstalls possible older NVC versions found during installation.

By default, setup installs NVC to `c:\Norman` with the following subdirectories:

- ...\download
  where NVC updates are placed after downloads.

- `...\msg`
  where all files from the messaging module(s) are located.

- `...\nvc\bin`
  where the program files, like EXEs, DLLs, device drivers, and help files reside.

- `...\nvc\config`
  where NVC stores the different configuration files.

- `...\nvc\nse`
  where the scanning engine and definition files are located.

- `...\nvc\qarantin`
  where quarantined files are placed.

- `...\nvc\tasks`
  where potential task files are stored.

- `...\nvc\info`
  where release notes in web browser format are placed.

NVC overview

Most components can be configured to suit your needs. This manual will not describe all configuration options in detail, but merely point out that they exist and where to find them. For a detailed description about all configuration options, see the *Reference Guide*.

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*. For the sake of simplicity, we often use the term *virus* as a collective description of unwanted code. The most common types of malware are viruses, worms, and trojans. 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 on 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 settings are configurable, so that you can set up NVC to suit your needs.

What's new in NVC v5?

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

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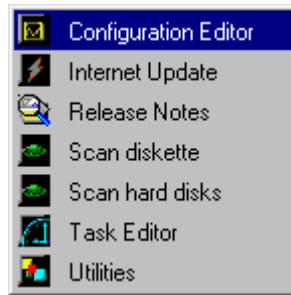- Ease of use
- Invisibility

NVC v5.0 user interface is made up from four main groups:
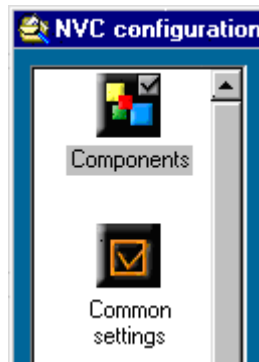
- Configuration editor

- Task editor
- Utilities
- Internet Update

Groups, modules, and components

When we talk about a NVC **group**, we are referring to a larger entity that holds modules and components. The configurable items under **Norman** on the Start|Programs menu are defined as groups:

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

And finally, the modules contain **components**, that often are a set of configuration options. You can view this list from **NVC configuration|Components|Install**:
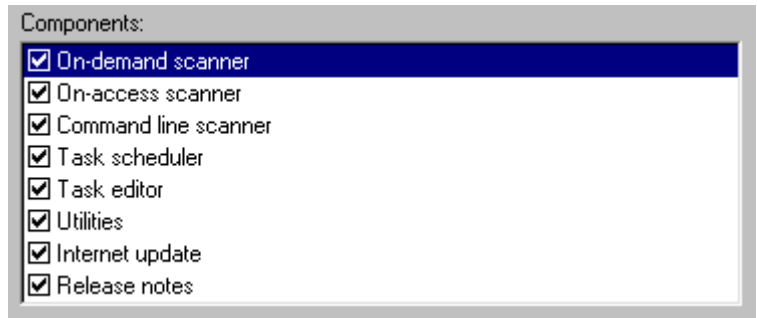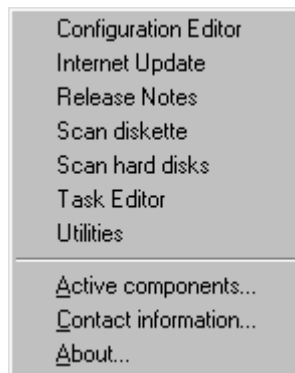
Shortcut to NVC modules and scanning

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

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 all NVC modules, as well as some typical scanning tasks. You can click on either mouse button to display this menu. In addition to easy access to the NVC modules and scanning options, you can read the release notes for the current version, view active components, display a list of Norman offices with street, web, and e-mail addresses. The "About" option displays information about the current scanner engine, including signature date and number of viruses for the virus definition files.

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

The configuration editor

The configuration editor is the first group in the Norman program group. You can configure the different functions in NVC from one central point — the Configuration editor. Like all other NVC groups, click on the Norman icon in the system tray and select from the menu. Alternatively, select *Start|Programs|Norman Virus Control|Configuration editor*:
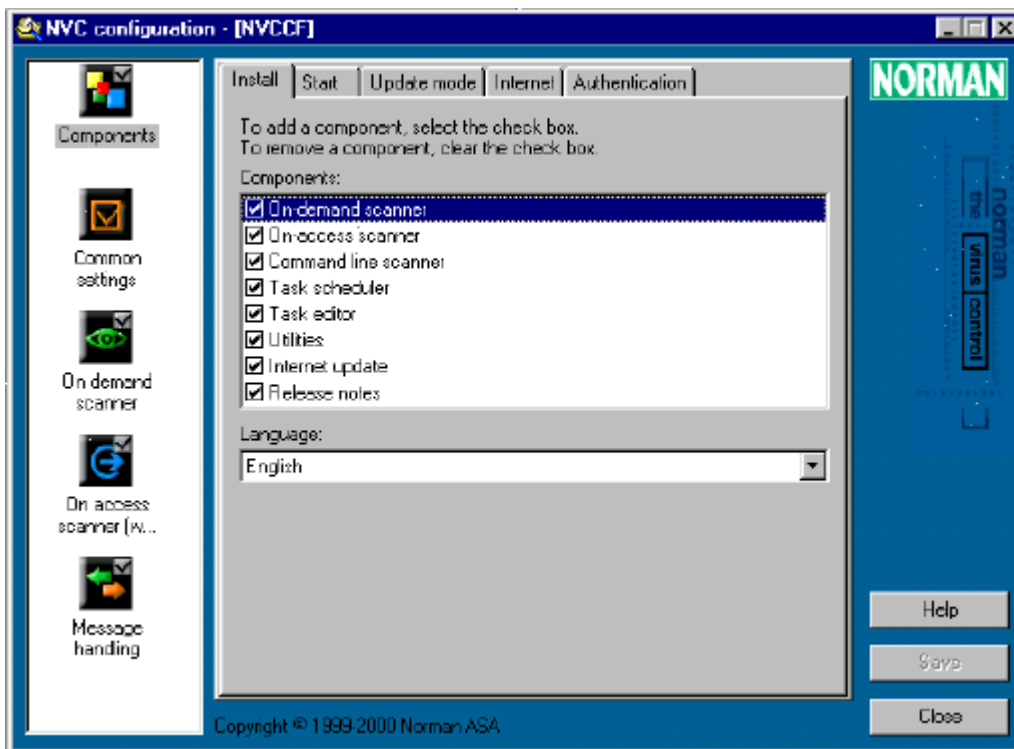
Components

The Components module is made up from six tabs:

Install, where you can view, install, or remove available components,

Start, where you can select which components should start automatically,

Update mode, where you decide how to update NVC: from CD-ROM, Internet, or from LAN/WAN,

Internet, where you may have to enter information if you intend to update NVC and you're protected by a firewall.

LAN/WAN, where you specify where software, configuration, and task file updates are placed.

Authentication, where your customer authentication code appears or should be entered.

Common settings

The settings in this module affect the behavior of the On-demand and On-access scanner (see below). If you select *Default values* for the scanners, NVC will use the settings in this dialog box. Vice versa, the selections you make for the On-demand and On-access scanner overrule the settings in the Common settings module. There are three tabs in the Common settings module:

Scanning, where you select what NVC should scan for, as well as what NVC should ignore,

Exclude list, where you can enter file names, directories, or entire drives that you wish to exclude from scanning,

Quarantine, where you can activate an area to quarantine infected files. You can also choose between a number of options for the quarantine area.

The On-demand scanner
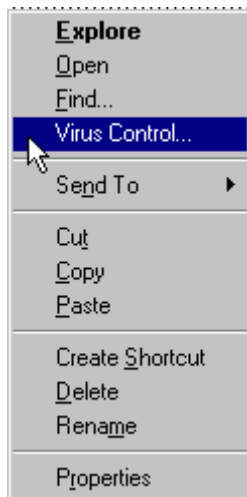
The purpose of the On-demand scanner, or the Right-click scanner, is to make periodic inspections of selected areas on your system. The scanner has its own entry on the Windows menu that pops up when you place the cursor on file system objects such as disks, directories, and files, and click on the right mouse button. The On-demand scanner can detect and remove all types of viruses automatically, except for boot sector viruses on hard drives.

The On-demand scanner will use the settings you specify in the Common settings module and in the On-demand scanner module:

Scanning, where you can select if the On-demand scanner should use default values or if you want to change them.

The On-access scanner

On-access scanning involves constant monitoring of the file system. 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. The On-access module has two tabs:

Scanning, which is divided into three different sections where you can select *scanning strategy*, *files to exclude*, and *how to handle files that cannot be scanned*.

Cleaning, where you determine how infected files should be handled. You can deny access to the file, remove the virus, or prompt for user action.

Message handling
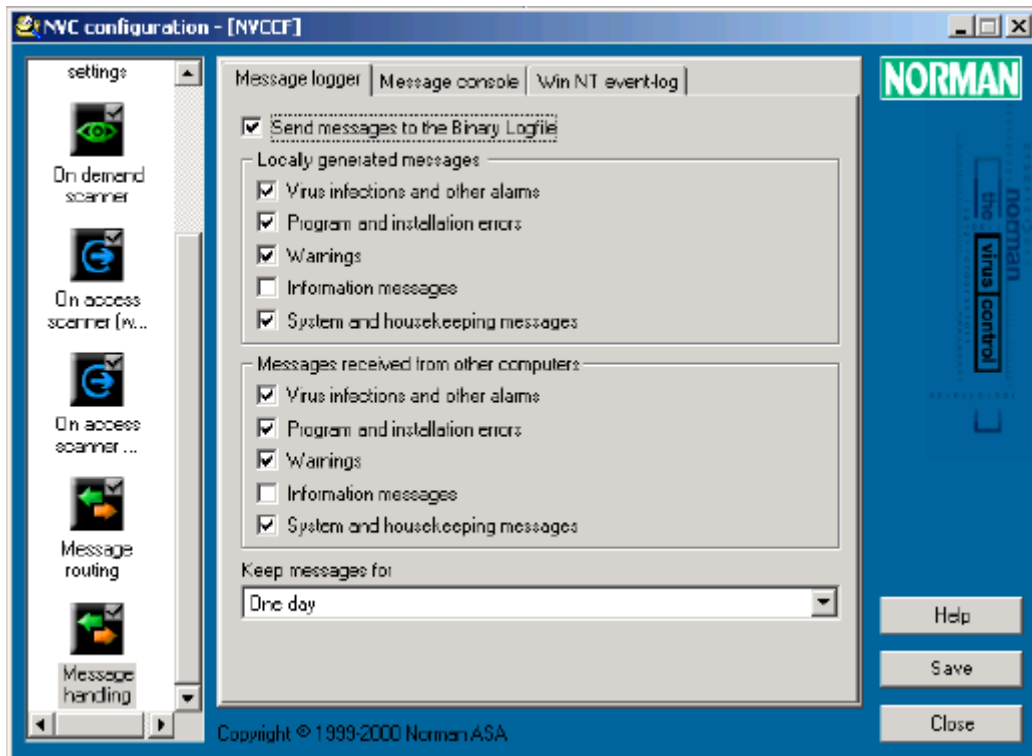
Message handling is the input module for generating a log file, displaying messages on the message console, and what should go into the Event Log in Windows NT/2000. Therefore there are three tabs with identical options in this dialog. Each tab has two sections, one for *local* incidents and one for incidents received from *other computers*. The selections you make decide what type of incidents are kept in the log file or the Event Log, or displayed on the message console.

The task editor
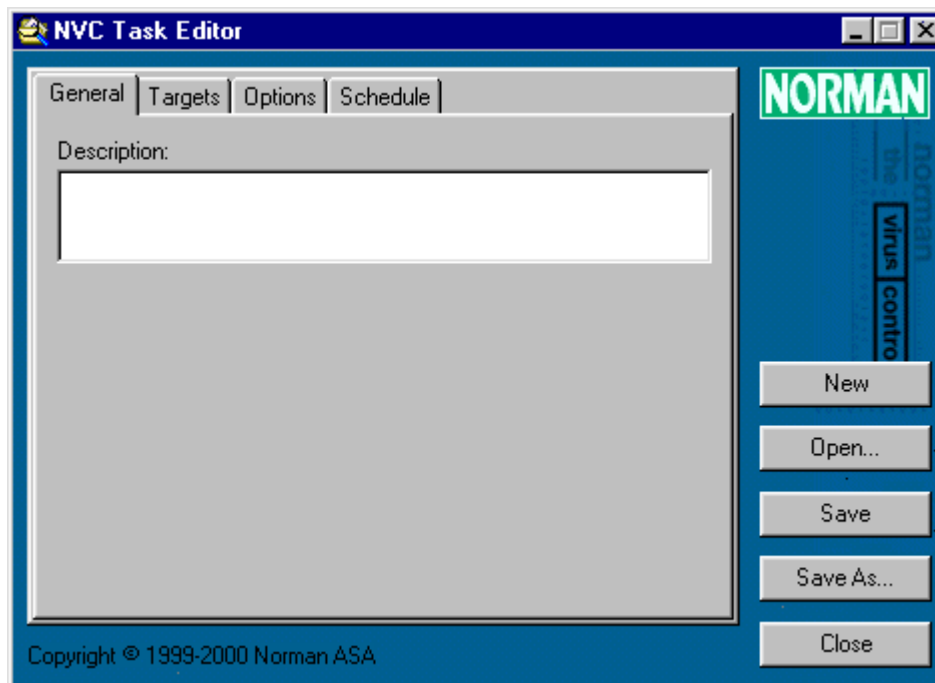
You can create a task file for scans that you wish to perform on a regular basis, or special scans that you intend to run in certain situations. For example, if you download files from the Internet to designated areas, you can create a task file that scans these areas only and run the task manually after 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 20).

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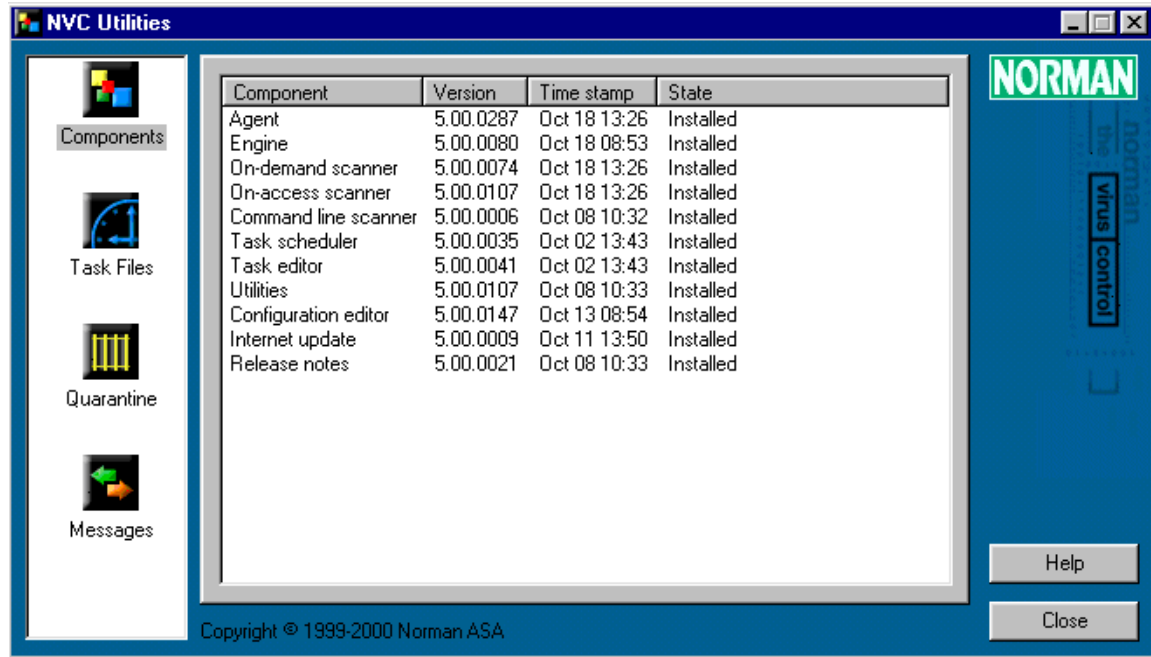
NVC utilities is a tool that presents an overview of the current state of affairs for the NVC components on your PC. In addition to viewing key information, you can change certain elements by selecting some of the entries, for example task files. Other functions, like Components, provide information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

In this version the utilities group is made up from four modules:

- Components
- Task files
- Quarantine
- Messages

Norman Internet Update (NIU)
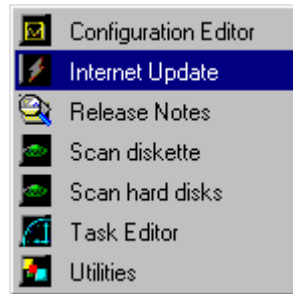
For those who don't update NVC by letting the agent distribute updates in a local network, Norman Internet Update (NIU) is the alternative method. NIU is a program that ensures that you are running the current version of NVC for your platform. Any changes to NVC, such as actual program changes, bug-fixes, 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 server. If date and/or size deviate from the current version, 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.

Other functions

The agent

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

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

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

The agent is always running.

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

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

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.

From the DOS prompt, go to the folder where the command line scanner is located and type:

```
nvc32 /?
```

for a list of available commands. The default location is `...\nvc\bin`.

Index

—R—

remove components 14
Requirements, system v
right-click scanner 16

—S—

schedule a task 18
System requirements v
system tray 13

—T—

Task editor 12
task file 18
Technical support vi
trojan 11

—U—

Universal Time Coordinates 19
update mode 15
Utilities 12

—V—

virus 11

—W—

worm 11

—Z—

Zanda 22