

User Guide

**Vexira Antivirus 2006 for NetWare  
Servers**





## TABLE OF CONTENTS

<b>HARMFUL MALWARES</b> .....	<b>3</b>
<b>About computer viruses</b> .....	<b>3</b>
<b>Virus infection symptoms</b> .....	<b>4</b>
<b>Keep computer virus free</b> .....	<b>4</b>
<b>The scan engine</b> .....	<b>5</b>
<b>VEXIRA ANTIVIRUS 2006 FOR NETWARE SERVERS</b> .....	<b>6</b>
<b>Minimal system requirements</b> .....	<b>6</b>
<b>Installation</b> .....	<b>7</b>
Automatic installation.....	7
Manual installation.....	7
<b>Program's structure</b> .....	<b>8</b>
Scanning possibilities .....	8
Protection units.....	9
Program's user interface.....	9
Using lists .....	9
Specifying dates .....	10
<b>Detailed overview</b> .....	<b>10</b>
Engine options.....	10
Searching/killing mode.....	11
Scan threads.....	12
Stop the engine.....	12
Start the engine .....	12
Domain management .....	13
Message redirection .....	14
Place of event.....	15
Type of event.....	16
Messages' recipients .....	17
Type of message .....	18
Global options.....	18
Quarantine .....	19
Information.....	19
Runtime options.....	19
Registration.....	20
<b>UPDATE MANAGER</b> .....	<b>21</b>
<b>Settings</b> .....	<b>21</b>
<b>Module versions</b> .....	<b>22</b>
<b>Manual update</b> .....	<b>22</b>
<b>Information</b> .....	<b>23</b>
<b>END USER AGREEMENT</b> .....	<b>24</b>
<b>CONTACT</b> .....	<b>26</b>



## HARMFUL MALWARES

### *About computer viruses...*

Spreading of the malware programs and increasing of the infections can be important security questions for any computer user. In the following lines you can find a summary review of the malicious programs, their operation and spreading.

Generally, the 'virus' expression means a computer program which endanger the data stored on the computer and/or the system's operation. Similar to a biological virus, the computer variant is also able to multiply itself and usually attaches to an executable file to be spread. When they are isolated (for example in an archived file) and they can't operate you can feel secure, they are harmless in such a case. But if they escape from the archives and become active they can be dangerous and perform considerable devastation in computer systems.

The malicious programs named 'viruses' in everyday language can be divided into groups by their activity and spreading methods.

There are so-called *boot viruses* which spelt the greatest danger among viruses till the middle of nineties. They try to infect the computer's boot sector which control the boot processes. These viruses can be activated at computer's boot time and although they are disappearing, it is worth mentioning them.

The majority of today's known viruses is put among *program viruses*. But surveying their rate in all the known active viruses, this leading role can't be stated. These viruses infect the DOS' .com, .exe, the Windows' NewEXE and the Windows95/NT's portable .exe formats. The program viruses' greater part insert their own code at the end of the program files and modify those to be started automatically when the host program is executed.

The *macro viruses* have appeared for just some years, but better and better invade our privacy. Their main target to infect Microsoft Office package's documents in which macros can be used. These documents are sent in e-mails frequently so the spreading of this kind of viruses is growing.

That viruses belong to the *script viruses* - as their name shows - are not spreading in binary code form but in source codes. For this reason anybody can modify easily the collected virus making a new variant of the original malware.

One of the viruses' subtype is the so-called worm viruses (worms). Several of them spreading in e-mail and try to exploit the possibilities of computer networks spreading from machine to machine using falsified sender address. Besides the waste of time spent on "handling" these e-mails, the worms can overload computer systems.

As the Internet became more popular, the number of e-mail viruses started to grow slowly and they are the top of the viruses at present. They spreading themselves in e-mails, sometimes in more hundred instances utilized the mailer programs or mailer servers. These infected mails can be recognized by their attachment which is the virus itself. The life cycle of the today's viruses accelerated. A typical mail virus is spreading fast after it is released, but practically it disappears in a short time thanks to the frequently updated virus databases.

*Trojan programs* also belong to the computer malwares. These are not able to spread without help and they always have some kind of hidden harmful routine to exploit the system vulnerabilities. As they can't spread themselves, you can get them in e-mails or by downloading the Internet. Based on their functionality there are different trojan programs.

The *backdoors viruses* opens a backdoor on the attacked computer providing clear way into the system. The *dialer programs* change the dial-up Internet connection. They connect to a remote Internet provider instead of the local one increasing the user's telephone bill.

The *password stealing programs* try to collect the user's encoded files and the passwords found in the



memory and send them in a specified e-mail address.

You can see that the protection is reasonable for the viruses' wide incidence and their various form. The justification of antivirus applications is not a question for today in the area of computer security.

### ***Virus infection symptoms***

Infection symptoms strongly depend on the propagated virus' properties. The following list contains some common symptoms you can experience:

- Different problems on the computer (for example: file copy problems)
- The computer often stops or restarts itself.
- Getting messages from your mail partners that they are receiving infected mails from you.
- The computer running slower than usual.
- Less free memory is available than before.
- Menu items, functions or whole applications disappear.
- Program's opening takes longer than before while configuration was unchanged.
- The size of the files increased seemingly without any reason.
- Some viruses simply display a message box to inform the infection.
- The date of the files changed.
- Unable to access drives.
- Strange graphical forms are displayed on the screen.

### ***Keep computer virus free***

Several viruses begin harmful activities in the world a day to start their attacks against the users and antivirus solutions with renewed effort. Because of the fast spreading the viruses are able to infect the unsuspecting users' computer in a short time.

If users devote their energies to prevention too they get back their efforts repelling a serious virus attack. Keep in mind, observing security requirements you can avoid data losing or other serious problems. Some tips how you can keep your computer infection-free:

- Make virus scanning on data that get into system from external device.
- Use resident virus protection.
- Update the antivirus software's virus database as frequently as it is possible.
- Files attached to e-mails must be handled as potential contingency.
- Set user accounts using various authority levels.
- Importance of shared directory handling! Make access rights and permissions for different users.
- Use only official applications.
- Use firewall against outside intrusions.
- Get files from reliable source.
- Protect your own password information.
- Scan the whole system for viruses if infection symptoms are experienced.
- Do not make available your computer stored important data for anybody.

Users can defend themselves against viruses using reliable and up-to-date antivirus applications.



## ***The scan engine***

The scan engine has an outstanding performance and is built in all of our products. The engine also uses heuristic analysis to detect harmful programs. Thanks to its platform- and operating system independent scanning methods it effectively scans for all known viruses, worms, trojans, scripts, macro viruses and other harmful codes on any system even in compressed files. To improve the scanning of these files, the engine uses emulation techniques.

Main features:

- Heuristic analysis
- High-speed scanning
- Processor/PC emulation technologies if it is possible
- 99% of the scan engine is platform independent (the remaining 1% is the platform dependent parts' implementation)
- Flexible virus database architecture: any new file types can be built into the database
- Usage of independent scanning technologies
- Daily virus database updates
- Processor-/platform-independent virus database and scan engine technology
- Operating system independent file type recongizer and parser
- Native scanning in .tar, .gz, .bzip2, .zip, .rar, .arj, .ace, .chm, TNEF, ms cab archives and in install shield cab files
- Native scanning in files compressed with diet, upx, aspack, pecomact and fsg (other .exe packed files extracted with emulation technology)
- Scanning in embedded archives to any level (depends on system resources)
- Scanning for viruses, worms, trojans and other harmful codes
- Detecting and removing spywares and adwares
- Information about IWORMs that can be removed by deleting the whole mail
- Scanning in many executable files
- Scanning in Microsoft Word, Excel, PowerPoint, Access and Project files
- Scanning in embedded OLE objects
- Scanning in the new Office 2003 XML format
- Scanning in HTML, Java script, ActiveX and Visual Basic Script (VBS) files
- Scanning in other scripting language files, like Unix / Linux shell scripts
- Scanning in Windows Help files (HLP)
- Scanning in LNK and PIF files
- Built-in MIME parser for scanning e-mails, mailboxes and MHT files
- Supporting the following encoding methods: BinHex 4.0, Base64, Quoted-printable, UUEncode
- Native scanning in Outlook Express mailboxes



# VEXIRA ANTIVIRUS 2006 FOR NETWARE SERVERS

In a network environment, the protection of servers is crucial as most of the data used for our everyday work is stored and transferred by servers. Therefore the effective protection of these servers does not only secure the stored data, but provides a secondary defense line for clients connected to them.

Vexira Antivirus 2006 for NetWare Servers provides resident protection for data, systems and therefore for the everyday work, optimized to the increased data traffic of servers. The easy-to-use, traditional NetWare-based user interface, the clear settings and continuous updates ensure, that the protection of the company's NetWare servers operate automatically and effectively.

Main features:

- Effective resident protection against viruses for servers
- Separate protection areas to handle servers' storage disks or their smaller areas individually
- Intelligent file protection, extended write protection to prevent infections
- Manual and scheduled virus scans
- Automatic updates
- Intelligent quarantine for storing infected files
- Incremental virus database update

### ***Minimal system requirements***

The following system components must be available to execute the program:

- Novell NetWare Server 4.11 + latest Support Pack
- Intel Pentium (or compatible) at 200 MHz
- 64 MB of RAM
- 30 MB of free hard disk space



## Installation

The product is available in a self-extracting install package (.exe), and in a .zip file. Use the self-extracting version to install the antivirus system automatically or you have to install it manually (.zip version needed).

### Automatic installation

The following package is available:

`nwguard-<product version>-<engine version>-<language>.exe`

Example:

`nwguard-2.2.08-4.2.13-en.exe`

- After the welcome panel and accepting the license agreement, you can set the target folder that you want to install the product to.
- After setting the target folder, the panel displays the version numbers of the modules to be installed so you can check them.
- On the next panel, you can select the components you want to install. The main component is essential to install, the Update Manager is optional.
- After clicking on the **[Next>]** button, you can set actions which will be executed automatically at the final phase of the installation process.

**Important!**

If one of the actions can't be executed, it must be performed after the installation manually based on the description of the *Manual installation* section.

Actions that you can select here are the same as the ones you would have to do in the course of manual installation steps (consult the *Manual installation* section for more).

#### **Vexira Antivirus 2006 for NetWare Servers**

- *Start protection*: If it is checked, the antivirus protection will be started automatically after the installation.

- *Modify autoexec.ncf*: If it is checked, the necessary modification will be performed in the `autoexec.ncf` file (consult the *Manual installation* section for more).

- *Registration*: If it is checked, the registration data can be entered during the installation.

#### **Vexira Antivirus Update Manager**

- *Start module*: If it is checked, the Update Manager module will be started after installation.

- If you have selected the *Registration* action before, you have to enter the valid registration data in the following panel.
- After these settings the installation process will be started and the selected actions will be performed.

### Manual installation

The following package is available:

`nwguard-<product version>-<engine version>-<language>.zip`

Example:

`nwguard-2.2.08-4.2.13-en.zip`

The product can be run on Novell NetWare servers and must be placed on the server's SYS: volume in a subdirectory so that it can be launched from console. The installation should be performed in domain administrator security context.

Steps when installing the product for the first time:



- Log on to a workstation using a domain administrator account. Create a subdirectory named **vexira** in the **SYS:\SYSTEM** directory for the program. The configuration file, log file and the **QUAR** (quarantine) and **TEMP** (folder of temporary files) directories will be created here automatically. Add this new directory to the **search path** list by using the **search add sys:system/vexira** command.
- Copy the program's files (**VAGUARD.NLM**, **VBENGINE.NLM**, **VEXIRA.INI** and the virus database (the **DATABASE** directory and its content)). Also copy the **VAUPDATE.NLM** and **VAUPDASC.NLM** files for automatic updating.
- Insert the **search add 1 sys:system/vexira** line into **SYS:SYSTEM/AUTOEXEC.NCF** file. If you want the protection to be started automatically together with the server then you should insert the next line, too: **load vaguard.nlm**. The **SYS:SYSTEM/AUTOEXEC.NCF** file can be modified with any editor from a workstation or with **INSTALL.NLM** from the server (NCF files options/ Edit **AUTOEXEC.NCF** file).
- Create a new user with system administrator security context in Novell NetWare's system administration program (NetWare Administrator or ConsoleOne) exclusively for virus protection. Recommended user name: **vexira**. This user should be added to the program's special user group.
- Launch the program on the server with the **load vaguard** command and perform the program's configuration.

If everything is all right, the modules will be loaded and two new entries will be displayed in the console screen's list (VAGuard Screen and VAGuard Console).

### Program's structure

Vexira Antivirus 2006 for NetWare Servers is a general Novell NetWare loadable module (NLM) that should be run on the server. After it having been loaded, it checks the server's every operation and scans every file before performing an operation on them.

If it finds a virus in the scanned file, it initiates the actions specified in the settings. It can deny the operation, put the infected file into the quarantine, disinfect the virus, and send a message to the users concerned, domain administrators or any other users. It puts all information gathered during its operation into a log file.

It is possible to define a file access rights system above Novell NetWare's possibilities. Writing of specified network directories or files can be banned easily this way preventing virus infection too.

### Scanning possibilities

Vexira Antivirus 2006 for NetWare Servers scans files in two ways. On the one hand it monitors every file operation on the server, in other words, it checks every incoming request and only allows access to virus-free files. On the other hand full virus scans can be requested, at a given time, for a specific protection area which can either be scheduled or can be launched manually from the console.

- On access scan  
In case of on access scan, the program automatically scans a file for viruses when its reading is requested. The types of files, which should be scanned, can be set in every domain. There are two lists for this purpose; the first of this contains file-masks of what should be scanned whilst the other contains excluded file-masks.
- Periodical scan  
In case of a periodical scan every file in the domain will be scanned. The periodical scan can be started manually or automatically at times specified for each domain.



- Write protection of files  
The program is able to provide write protection for files by complementing the Novell NetWare network file access protection system. Write protection is users independent in other words it applies to all users. In every domain it can be set whether write protection is enabled or disabled similarly, the mask for files that should be protected or should be excluded can also be set for each domain.

## Protection units

Similarly to the Novell NetWare security context system, the scanning and protection options for Vexira Antivirus 2006 for NetWare Servers can be set individually in every domain. One subdirectory structure of the server belongs to each of the protection units. If this subdirectory does not contain further protection units, the unit will be applied to all subdirectories and files in that directory. If the subdirectory contains further protection units, the upper unit will not be applied to its subdirectories. That is to say a file only belongs to one protection unit and the same settings are applied to every file inside a protection unit.

## Program's user interface

The functions and settings of the product can be accessed through Novell NetWare's regular menu system. After having started the program its functions and settings can be accessed through menus.

### *Using menus*

- Cursor keys - Movement between menu items
- **Enter** key - Selection of the menu item
- **ESC** key - Exiting a sub-menu item or the program
- **F1** key - Displays program help

In the program the basic unit for configuration is the list. Items in the list can be modified, deleted, added or an item can be configured in more detail with the help of the following keys:

### *Using lists*

- Cursor keys, **PgDn**, **PgUp** - Movement between list items
- **Enter** key - Selection of one or more list entries
- **F5** key - Highlighting entries or disabling highlight
- **Delete** key - Removal of an entry
- **Insert** key - Adding a new entry
- **F3** key - Renaming an entry

When specifying the date worksheet the required dates should be marked with a \* (star) in the table which appears.



## Specifying dates

- Cursor moving keys, with which you can move in the sheet
- It is possible to select an interval by pressing **F5** key
- By pressing **Ins** or the star (\*) key the actual date or interval can be selected
- By pressing **Delete** or **Space** key the actual date or interval can be deselected
- By pressing **Enter** key the selection of the actual date or interval can be inverted

## Detailed overview

The product can be launched by the **VAGUARD.NLM**. The program creates two screens:

- VAGuard Screen - The programs operations and logged events can be monitored here.
- VAGuard Console – The program can be configured here, individual options can be set here and periodical scans can be launched from here manually.

### Note!

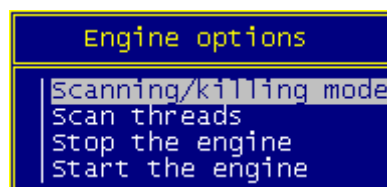
If you leave or exit the screens, the protection will also be terminated. After exiting, scans and periodical scans will not be executed!



Main menu

A more detailed insight of the program can be gained by going through the menu items.

## Engine options



Engine options



## Searching/killing mode

```
Scanning/killing mode
Scan packed/MIME files: Enabled
Temporary directory: SYS:\SYSTEM\vbuster_ ...
Scan: strict
virus killing: Disabled
Non-killable viruses: Keep file
In case of protection error: Access enabled
General heuristics: Normal
suspicious programs: Keep file
```

Scanning/killing mode

### Scan packed/MIME files

If it is activated, the program will perform a virus scan on compressed files.

### Temporary directory

During scanning the program temporarily places the content of a compressed and MIME files into the specified directory.

### Scan

Scan method can be set under this point:

- Strict: Optimized scanning method searches for viruses in those parts of a file where they are likely to be found.
- Fast: Optimized scanning method will only scans for viruses in those parts of a file, where they are likely to be found. This scanning method is the one recommended in most cases.
- Full: Scans the whole file, even places where under normal circumstance viruses are not found, thereby increasing the chance of false alarms. This method is very time-consuming.

### Virus killing

The program will remove the virus from the infected file, if possible, if this option is enabled.

### Non-killable viruses

Some viruses cannot be removed even if they are recognized. The action, which will be performed when such a virus is found can be set here:

- Rename file: renames the infected file.
- File to quarantine: moves the infected file to the quarantine directory.
- Keep file: does nothing with the infected file.
- Delete file: deletes the infected file.

### In case of protection error

It can be set whether the program should prohibit an access request in case of file access error or not.

### General heuristics

Heuristic scan mode can be enabled or disabled and its sensitivity can be set here. During the heuristic analysis, the software tries to detect codes and programs, which have virus-like characteristics but are not registered in the virus database. If such a *suspicious* file is found, the user is notified.



The following levels of heuristic analysis are available:

- *Disabled*  
No heuristic analysis.
- *Normal*  
The depth of the analysis is limited, the possibility of false positives is low, but the chance of detecting unknown viruses is not too high.
- *Strong*  
The chance of detecting unknown viruses is higher, but there is a higher possibility of false positives.

## Suspicious programs

The action set here will be performed when a program file is considered suspicious during the heuristic scan:

- Rename file: renames the infected file.
- File to quarantine: moves the infected file to the quarantine directory.
- Keep file: does nothing with the infected file.
- Delete file: deletes the infected file.

## *Scan threads*

The number of parallel scanning threads can be set here.

```
Scan threads
Total number of scanner threads: 16
(Max.: 16, min.: 2!)
Reserved for on-access scan: 13
(Max.: total-1, min.: 1!)
```

*Scan threads*

### ! Note!

The value must be between 2 and 16. The new value will be applied when the scan engine is restarted!

The program operates with four threads by default. Two threads are always kept for receiving incoming requests, for on-access scan. Increasing the number of threads can reduce system performance although more files can be scanned this way.

## *Stop the engine*

It is seldom that we only want to stop the scan engine independently from the rest of the program, however, it can be rather useful during program update as like this the engine can be changed on the fly.

### ! Note!

By stopping the scan engine, the defense still remains active, but no scans can be performed. This can result in the inaccessibility of certain files!

## *Start the engine*

Starting the engine and loading the actual VDB with the set scan number.



## Note!

Always check if the proper VBENGINE.NLM and virus database files are available in the search path. VBENGINE.NLM will only be launched if it exists and if the version of the virus database and VBENGINE.NLM is proper!

## Domain management

All protection units (domains) are listed in the "Domain entries list" window. Units can be created, deleted or renamed in this list.

The / (root) protection unit cannot be deleted or renamed. If a unit is renamed (**F3** key), all entries connected to it will be renamed as the new domain. If a unit is deleted (**Delete** key), entries will be deleted and if any messaging system would be terminated this way, the program will warn the user. If a periodical scan is running on the unit, which is renamed or deleted, the scan stops immediately. If a new unit is created, it will inherit all characteristics of the unit, which has been selected when having pressed the **Insert** key.

## Note!

The protection unit is inactive while configuring it. Do not leave the configuration window open!

The following modifications can be made inside a protection unit settings:

```
SYSTEM
Domain path: SYS:SYSTEM
On-access scan: Enabled
Virus found action: Access denied
Periodic scan: (time table)
Files to be scanned: (list)
Exceptions: (list)
Write protection of files: Enabled
Write protected files: (list)
Exceptions: (list)
```

Domain's settings

### Domain path

Every protection unit has a subdirectory. This subdirectory can be set here. The full path must be set in **volume name:path** form. When specifying a path, directories can be divided either by the "/" or "\" sign.

### On-access scan

On-access scan of files stored on the server can be enabled or disabled. The program scans files on access if this option is enabled.

### Virus found action

If on-access scan is enabled, the action, which will be performed when a virus is found during an on-access scan, can be set here:

- File to quarantine: the infected file will be moved to the directory set in Global options/Virus collector.
- Access denied: denies access to infected files.

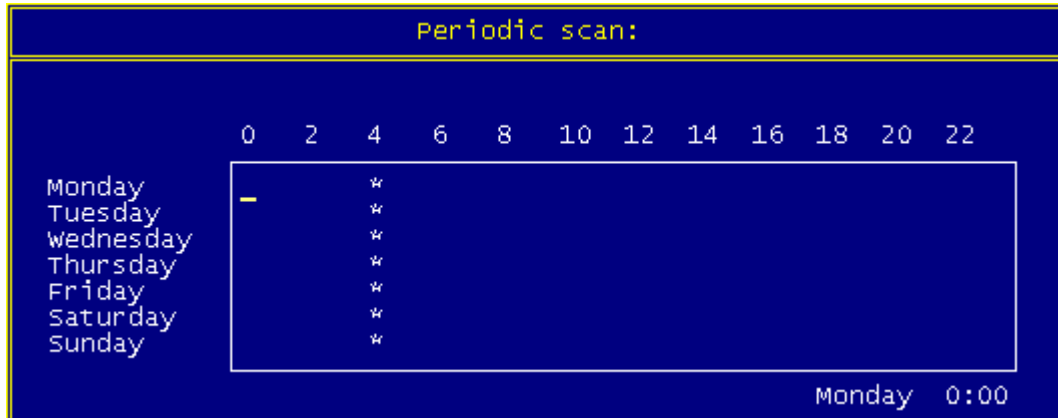


## Vexira Antivirus 2006 for NetWare Servers

- No action: does nothing with the infected file.
- Delete file: deletes the infected file.

### Periodic scan

Periodic scans can be set in 30 minute long intervals in this window so that the program would perform scans weekly in the given domain's directories at given times. If the program detects that it has to perform a scan in the interval when it is started it will perform the scan immediately.



*Periodic scanning*

### Files to be scanned

The masks of files, which should be scanned when accessed, can be selected here (e.g: `*.com`, `*.exe`, `*.doc`).

### Exceptions

The masks of files, which should not be scanned when accessed, can be selected here (e.g: `command.com`).

### Write protection of files

The write protection can be enabled or disabled here. This protection is not applied to special users.

### Write protected files

The masks of files, which are protected can be selected here.

### Exceptions

The masks of files that should not be write-protected can be selected here.

### **Note!**

If the configuration file (`VEXIRA.CFG`) does not exist in Vexira Antivirus 2006 for NetWare Servers' directory, the entries of protection units will be created, with default settings, when the program is started. According to these entries on-access scan is performed on all executable files that are stored on the server. Periodical scan is performed every day at 4:00 am all executable files each on domain. Write protection is only applied to files under `SYS:LOGIN`, `SYS:PUBLIC` and `SYS:SYSTEM` by default.

## Message redirection

The program displays the name of the redirection entry in this menu. Redirection entries can be created, deleted or renamed in this list. The options of a unit can be accessed by selecting the unit.

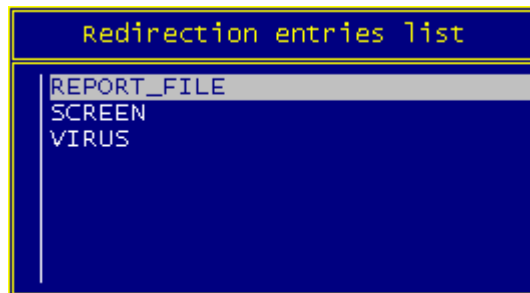
### **Note!**

The unit will remain inactive during configuration!



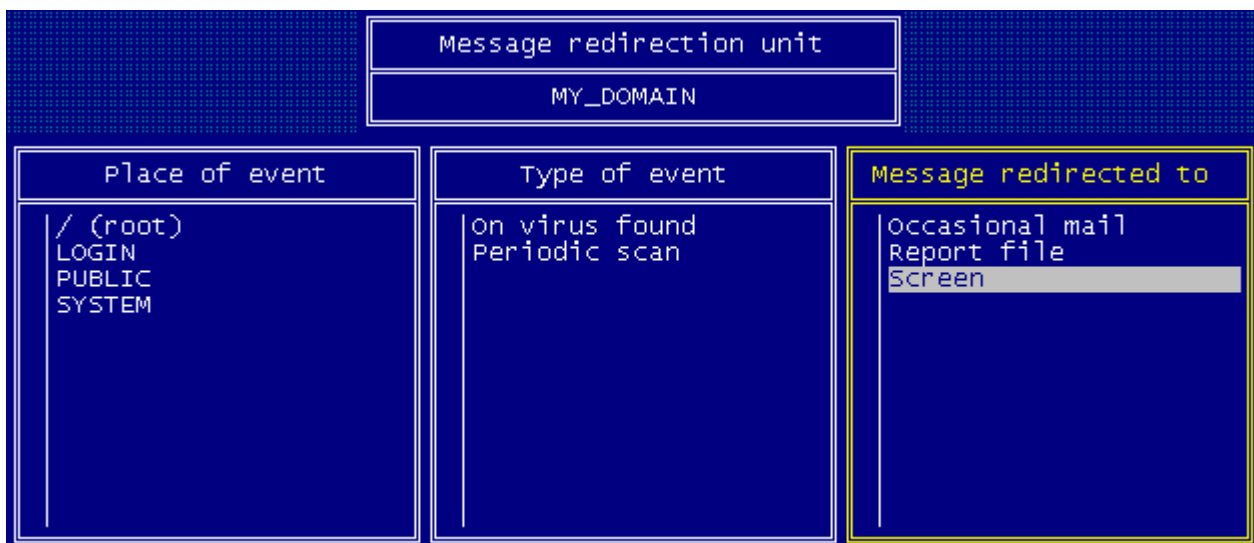
During redirection configuration you have to specify where the messages should be forwarded which were created at a given location as a consequence of a given event. Three units are present in the program by default:

- Report file - A log file, in which all events are stored that occurred during the system's operation.
- Screen - The program's screen messages.
- Virus - A unit, which contains several addresses and is activated when a virus is found.



*Redirection entries*

When configuring a Message redirection unit, you have to specify the following data: Where was the message to be forwarded created, what was it triggered by and where should it be forwarded to.



*Message unit panel*

### *Place of event*

The message redirection unit's place of creation contains the following settings:

#### General

Describes the place of creation of those messages, which cannot be connected to any protection units. If a message control unit contains the "general" place of creation description, than the unit was created inside Vexira Antivirus 2006 for NetWare Servers, which means that it can forward messages that cannot be connected to any protection units.



### Domain name

If a domain's name can be found in a message control unit's place of creation field, the unit will be applied to messages created in the given protection unit. When creating a new protection unit, it will inherit the characteristics of the unit, which has been selected when pressing the **Insert** key. These settings can be modified.

### *Type of event*

The message control unit classifies events into four main groups:

### File protection

Describes events made by Vexira Antivirus 2006 for NetWare Servers' file protection system. If enabled, the message control unit will forward messages, which have been created when performing an illegal writing process in any domain included in the place of creation list.

### Information

Describes events, which has been caused by Vexira Antivirus 2006 for NetWare Servers, but are not connected to the program's scanning or protection system. The message control unit will forward the following messages if enabled:

- Occasional mail has been sent: The program generates a confirmation message when an occasional mail is sent. If the option is enabled, the unit also forwards this message.
- Component: If the option is enabled, messages created by an external component will be registered.
- Engine events: The program generates a message on every event, which occurs connected to the engine.
- File changed: If a virus had been found and the infected file has been moved to a given folder or has been renamed, it sends a message. By logging these, it is possible to recover these files.
- Error: All errors, which occur inside the program generates a message. If the option is enabled, the unit forwards this message it also forwards a message describing the error.
- Error message from engine: The program generates a message on every error, which occurs connected to the engine.
- Configuration has changed: If the option is enabled, messages created when the program's configuration had been modified are forwarded.
- Vexira Antivirus 2006 for NetWare Servers has started: If the option is enabled, the message created on program launch will be forwarded.
- Vexira Antivirus 2006 for NetWare Servers has stopped: If the option is enabled, the message created on program stop will be forwarded.
- Periodic mail has been sent: The program generates a confirmation message when a regular mail is sent. If the option is enabled, the unit also forwards this message.

### Periodic scan

Describes events caused by Vexira Antivirus 2006 for NetWare Servers' periodical scan system. The message control unit will forward the following messages describing the status of periodical scans in the given protection units:

- File to be scanned: The program has arrived at a new file during periodical scan. The message contains the name of the protection unit and the file.
- Scan sub-directory: The program has arrived at a new subdirectory during periodical scan. The message contains the name of the protection unit and the directory.
- Scan started: The program's periodical scan system has initiated a periodical scan on a protection unit. The message contains the name of the protection unit.
- Scan stopped: The program's periodical scan system has finished a periodical scan on a protection unit. The message contains the name of the protection unit.



## Vexira Antivirus 2006 for NetWare Servers

- Scan aborted: The program's periodical scan system has aborted one of the running periodical scans on a protection unit due to user intervention. The message contains the name of the protection unit.

### On virus found

Describes events caused by Vexira Antivirus 2006 for NetWare Servers' virus scanning system. The message control unit will forward a message if a virus is found in the listed protection units regardless of the fact whether it was a periodical or an on-access scan. Depending on the scan result the messages can be the following:

- Suspicious: The virus scanning system has found a suspicious code part indicating the presence of a virus when scanning a file.
- Immuniser: The program has found a file, which has been disinfected by a virus scanner.
- Internet worm (I-Worm): The program found an Internet worm-type malware.
- Mutant: The virus scanning system has found a code part similar to a known virus when scanning a file.
- Sequence: The virus scanning system has found a byte sequence, which can be found in a virus.
- Non-killable: The program has found a file, which has been ruined by a virus so it cannot be disinfected.
- Packed: The program has found a compressed file, which contains a virus.
- Trojan program: The program has found a file, which contains a Trojan program.
- Virus: The virus scanning system has found a virus.

### *Messages' recipients*

The message control unit can send messages to the following recipients:

#### Occasional mail

Sends an occasional mail to recipients given in global options.

#### ErrorLog

Writes the message into Novell NetWare's error log file (`SYS:SYSTEM/SYS$LOG.ERR`).

#### User

If the event, which has caused the message, can be connected to a user, the program sends a broadcast message to the user.

#### Screen

The message will be displayed on the server, on the VAGuard Screen.

#### Console

The message will be displayed on the server, on the System Console screen.

#### Operator

The message will be broadcasted to every operator, which can be given optionally. The message will only be sent to operators, who are logged on to the network when the event occurs. Operators must be added to the operator list before activating the message sending unit.

#### Periodic mail

Sends periodic mail (at given times) to recipients given in global options.

#### Report file

Writes the message into the file, which can be given optionally (the default is `vexira.log`).



## Type of message

The language of the message and the level of details can be given in case of every output. The level of details can be one of the following:

### Short

The message contains only one line. Broadcast messages can only be sent as a short message.

### Normal

The message contains all information on the event except for:

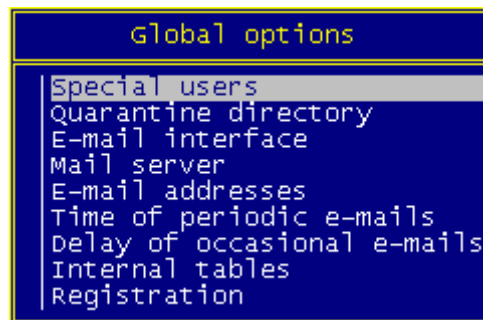
- If the event can be connected to a file, its path is displayed in a shortened form.
- The date of the event is not included.
- Does not contain the physical base address connected to the event.

### Detailed

The message contains information on the event including.

## Global options

The programs general settings can be found in the Global options menu.



*Global options*

### Special users

The list of users, who can write or read protected files, can be specified here. These users can perform disinfection while Vexira Antivirus 2006 for NetWare Servers is running. In this case, users using the server, do not have to log out from the network.

### Quarantine directory

If a virus is found and it must be moved according to the program's settings, the infected file will be moved to this directory.

### E-mail interface

The e-mail interface, which is used when sending periodical or single messages, can be set here.

- None: The program does not send mails.
- Socket: E-mails are forwarded with the aid of a socket.

### Mail server

You can specify the domain name of IP address of the SMTP server used for message forwarding

### E-mail addresses

The following users will receive the message, which can be a periodical or an occasional e-mail.



## Time of periodic e-mails

The times, when periodical messages are sent can be given in this table in 30 minute intervals weekly.

## Delay of occasional e-mails

If the appropriate delay is set, than it is here that it can be specified that the sending of an occasional e-mail should be delayed for a certain time.

## Internal tables

The size of Vexira Antivirus 2006 for NetWare Servers' internal tables can be set here. The size of tables is given in bytes. The size of the following tables can be set:

- On-access file cache size: The program places the names of the files, which were considered virus-free during the on-access scan in this table. In case of repeated access the file will not be scanned if its name is in this table. In case of writing, the file's name will be automatically removed from the table. If you do not want to use this option, set the size of file cache to 0.
- Redirection table: The size for storing message control units can be set here.
- Domain table: The size for storing protection units can be set here.

## **Quarantine**

The task of the quarantine is to store infected or suspicious files and handle them according to the settings.

If you select a quarantined item you will get some information on the selected file in a new window and you can choose from the actions performed on the file by using the *Quarantine actions* menu item.

- Keep: The program keeps the file as it is.
- Save as: The program saves the file coded, so it can be sent for analysis.
- Delete: The program deletes the selected file permanently.
- Rescan: The program performs a scan on the file and removes the virus from it if it is possible.
- Restore: The program restores the file to its original location if the given path exists and if a file with the same name does not exist at the said location.

The selected action will be performed after closing the window!

## **Information**

In this menu you can request information on units known by the program.

### About

The addresses and phone numbers connected to the program's distribution and support and version numbers are displayed here. The status of the scan engine can be checked here (loaded or unloaded).

## **Runtime options**

The following options are displayed:

- Start scanning: Displays the list of domains, where a scan can be performed (no scans are running, the domain entry is valid). After having selected the domain(s), a scan will be initiated.
- Stop scanning: Displays the list of domains, where a scan is running or a periodical scan is due to start. In the second case, the domain's name is in a bracket. After having selected the



## Vexira Antivirus 2006 for NetWare Servers

domain(s), scans will be stopped.

- Report file listing: Displays the name of log files, which can be displayed. If a file is selected, its content will be displayed. If the display is at the end of the file, it will switch to tracking mode so that new entries will be displayed automatically.

### Registration

You will only be able to launch the product if you have a user name and a valid registration key for the program.

Vexira Antivirus 2006 for NetWare Servers becomes fully functional after it has been registered. If your registration expired, you should renew it to be authorized to use the latest program versions (the virus database updating is allowed without any restriction). Your actual program version can be used for unlimited time but you are not allowed to update the program-files after registration have expired.

```
Registration
Registered: 8
User: TEST
Key: WEW43-TG64G-TTR6B
Registration will expire soon: 2005. 2. 4.
```

*Registration windows*

### Registration process

During the registration process the user will receive a registration key for the name and number of server users given by the said user. The name and the registration key can be entered after selecting the *Global Options/Registration* menu item. A window will appear in which information can be found on the registration status, the number of server user as well as the number of users registered.

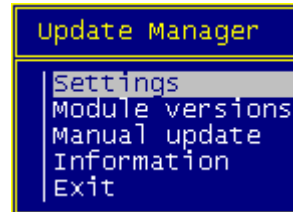
#### ! Note!

Please take care of the little and capital letters when you are entering the registration data!



## UPDATE MANAGER

Novell-based Vexira Antivirus products can be updated easily with the help of *Update Manager*. In order to install the updater, from the installation CD, copy the **VAUPDATE.NLM**, **VAUPDASC.NLM** files and the **VEXIRA.INI** file if this does not already exist into Vexira Antivirus 2006 for NetWare Servers directory. The update can be started with the **load vaupdate** command. The following options are listed in the console window:

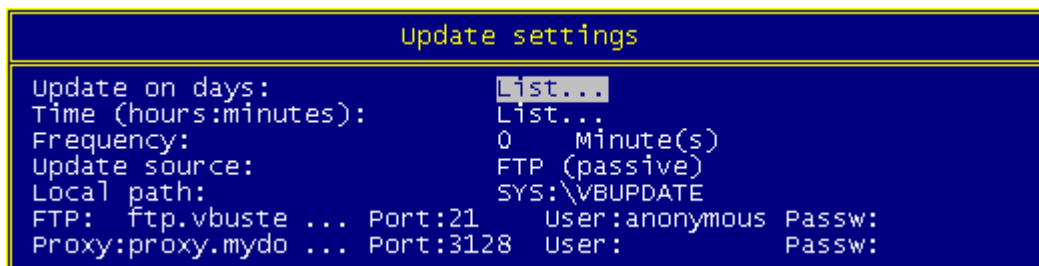


*Main menu*

! The product uses incremental virus database update mechanism to keep the virus database up-to-date. The advantage of this method is that the program doesn't need to download the whole virus database file every time (its size is several MBs) but usually only a small additional database package including the virus signatures processed and released recently. Using this mechanism, the download time is decreased to a minimal level so we can release additional virus database packages several times a day to improve the defence. Users can obtain protection against new malware without spending long time and generating considerable network load for the update. The protection is available almost immediately after the signatures of the newly discovered viruses have been processed in our virus lab.

## Settings

The general settings that will affect both the automatic and the manual updates can be viewed here.



*Update settings*

### Update on days

It is through this option that the days on which the program should perform the updates can be set. New days can be added with the aid of the **Insert** key and days already on the list can be removed through the use of the **Delete** key.

### Time

This list contains the times when the program should perform the updates. The times must be given in hh:mm format (for example 22:30 stands for half past ten p.m.). The specified value is only valid, if 0 (zero) value is given in the next menu item (*Frequency*).



## Frequency

The frequency of updates can be set here in minutes. The program will perform an update in every x minutes if this option is set.

## Update source

The type of the source from where the program will execute the update can be specified here. It can either be a local, a passive or active FTP path or a Proxy FTP.

## Local path

It is here that you can enter the server path where the installation kits can be found.

## FTP/Port/User name/Password

This is where you can enter the details of the FTP server. We suggest using the default setting; [upd.vexira.com/pub2006](http://upd.vexira.com/pub2006) for sever name, using of port 21 and *anonymous* as user name with no password.

## Proxy/Port/User name/Password

These fields have to be completed if the FTP update is carried out through a proxy server. As default we suggested using the port 3128.

## **Module versions**

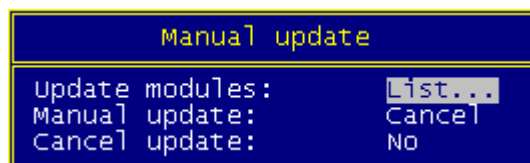
The module versions of the program and the dates they were created are displayed here. It also here that you can set as to which modules should be updated.

Under the name of the installed products we can see the modules belonging to it as well as the module version number and the date it was created.

On the field next to the product name it can be set whether or not the modules of the program should be updated.

## **Manual update**

Manual updates can be initiated in this window:



*Manual update*

## Update modules

This list contains all modules that will be updated during the update process. The modules listed here are those that were selected for updating in the Module versions window.

## Manual update

Choosing the Start option in this window will start the update process. It is very important, that the process will only be started, if no other tasks are running.

## Cancel update

It is with the aid of this option that a running update process can be cancelled.



## ***Information***

This menu contains the address of the Central Command, Inc.



## END USER AGREEMENT

IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS DO NOT INSTALL OR USE THE VEXIRA ANTIVIRUS SOFTWARE (referred to hereafter as the "Software"). BY CLICKING "YES", "I ACCEPT", "I AGREE", "OK", "CONTINUE", "NEXT" OR BY INSTALLING OR USING THE SOFTWARE IN ANY WAY, YOU ARE INDICATING YOUR COMPLETE UNDERSTANDING AND ACCEPTANCE OF THE TERMS AND CONDITIONS OF THIS END USER SOFTWARE LICENSE AGREEMENT (referred to hereafter as the "License"). IF YOU DO NOT ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE, THEN CENTRAL COMMAND, INC. IS UNWILLING TO LICENSE THE SOFTWARE TO YOU. YOU MAY, WITHIN THIRTY (30) DAYS OF YOUR INITIAL PURCHASE OF A COPY OF THE SOFTWARE, RETURN THE ENTIRE COPY OF THE SOFTWARE (INCLUDING ALL COMPUTER MEDIA, PACKAGING AND DOCUMENTATION) WITH PROOF OF PURCHASE EITHER TO CENTRAL COMMAND, INC. DIRECTLY AT ITS CUSTOMER SERVICE DEPARTMENT OR TO THE RETAILER FROM WHICH YOU PURCHASED THE SOFTWARE, FOR A FULL REFUND OF THE AMOUNT INDICATED BY YOUR SALES RECEIPT OR PROOF OF PURCHASE FOR THE SOFTWARE.

IF YOU ARE INSTALLING THE SOFTWARE ON A COMPUTER THAT IS NOT OWNED BY YOU, YOU ARE BOUND TO THE TERMS AND CONDITIONS OF THIS LICENSE BOTH IN YOUR INDIVIDUAL CAPACITY AND AS AN AGENT OF THE OWNER OF THE COMPUTER, AND YOUR ACTIONS WILL BIND THE OWNER OF THE COMPUTER. YOU REPRESENT AND WARRANT TO CENTRAL COMMAND, INC. THAT YOU HAVE BOTH THE CAPACITY AND AUTHORITY TO ENTER INTO THIS LICENSE ON YOUR OWN BEHALF AS WELL AS ON BEHALF OF THE OWNER OF THE COMPUTER ON WHICH YOU ARE INSTALLING THE SOFTWARE. FOR PURPOSES OF THIS LICENSE, THE "OWNER" OF A COMPUTER IS THE INDIVIDUAL OR ENTITY THAT HAS LEGAL TITLE TO THE COMPUTER OR THAT HAS THE POSSESSORY INTEREST IN THE COMPUTER IF IT IS LEASED OR LOANED BY THE ACTUAL TITLE OWNER.

This End User License Agreement ("License") is a legal agreement between you (either an individual, agent of the owner, or a single entity end user) and Central Command, Inc. for use of the Central Command, Inc. software product identified above (i.e. Vexira Antivirus), which includes computer software and may include associated media, printed materials, and "online" or electronic documentation (collectively referred to as the "Software"), all of which are protected by U. S. copyright laws and international treaty protection. By installing, copying, or otherwise using the Software, you agree to be bound by the terms of this License. If you do not agree to the terms of this License, do not install or use the Software.

The Software and the name "Vexira Antivirus" is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The Software is licensed, not sold. If you agree to be bound by all of the terms of this License, you will only own the media on which the Software has been provided and not the Software itself.

**THIRTY DAY MONEY BACK GUARANTEE:** If you are the original licensee of this copy of the Software and are dissatisfied for any reason with it within the first thirty (30) days after your purchase or delivery date, you may return the complete product, together with your original proof of purchase to Central Command, Inc. or the retailer from which you purchased the Software, for a refund of the amount indicated by your original proof of purchase. If this purchase was completed using electronic delivery you are required to complete a Letter of Destruction (referred to hereafter as an "LOD") and return it within thirty (30) days after your purchase date to receive a refund. Central Command, Inc. uses the postmark or fax date of the completed and returned LOD to determine compliance. You can receive a LOD by contacting your electronic retailer from which you purchased the software or directly from Central Command, Inc. via e-mail at [service@centralcommand.com](mailto:service@centralcommand.com), postal mail at P.O. Box 468, Medina, Ohio, 44256, or fax at +1 330-722-6517. For assistance you may also contact Central Command, Inc. by calling +1 330-723-2062 and requesting Customer Service.

**GRANT OF LICENSE:** Central Command, Inc. hereby grants you and only you a non-exclusive license to use the Software subject to and upon all of the terms and conditions set forth in this License.

**APPLICATION SOFTWARE:** You may install and use only one copy of the Software, and only on a single computer terminal.

**NETWORK USE:** You may also store or install a copy of the Software on a storage device, such as a network server, which is used only to install or run the Software on your other computers over an internal network; however, you must purchase and dedicate a separate license for each separate computer terminal on which the Software is installed or run from the storage device. A license for the Software may not be shared or used concurrently on different computers or computer terminals. You are required to purchase a license pack or multi-use license if you require multiple licenses for use on multiple computers or computer terminals.

If you purchase a License Pack and you have acquired this License for multiple licenses of the Software, you may make the number of additional copies of the computer software portion of the Software specified above as "Licensed copies." You are also entitled to make a corresponding number of secondary copies for use on a single home computer as specified above in the section entitled "Application Software".

If you purchase a License for the Software to be used to virus scan electronic messages or you install the Software in such a way to virus scan electronic messages you are required to purchase a license for each domain name and each sub domain name that is virus scanned. If your total electronic mail addresses exceed 6000 you are required to purchase a special Internet



## Vexira Antivirus 2006 for NetWare Servers

Service Provider (ISP) License for use of the Software.

**TERM OF LICENSE:** The License granted hereunder shall commence on the date that you install, copy or otherwise first use the Software. You may terminate this License at any time. This License shall terminate automatically (and you shall have no right to use the Software) upon your breach of any term of this License. Upon termination, you must destroy the Software and all copies, if any, you made pursuant to this License.

**UPGRADES:** If the Software is labeled as an upgrade, you must be properly licensed to use a product identified by Central Command, Inc. as being eligible for the upgrade in order to use the Software. A copy of the Software labeled as an upgrade replaces and/or supplements the product that formed the basis for your eligibility for the upgrade. You may use the resulting upgraded product only in accordance with the terms of this License. If the Software is an upgrade of a component of a package of software programs that you licensed as a single product, the Software may be used and transferred only as part of that single product package and may not be separated for use on more than one computer.

**COPYRIGHT:** All right, title and interest in and to the Software and the name "Vexira Antivirus" and "Vexira" and all copyright rights in and to the Software (including but not limited to any images, photographs, animations, video, audio, music, text, and "applets" incorporated into the Software), the accompanying printed materials, and any copies of the Software are owned by Central Command, Inc. and/or its suppliers. The Software is protected by copyright laws and international treaty provisions. Therefore, you must treat the Software and the term "Vexira Antivirus" or "Vexira" like any other copyrighted material except that you may install the Software on a single computer provided you keep the original solely for backup or archival purposes. You may not copy the printed materials accompanying the Software. You may not use the name "Vexira Antivirus" or "Vexira" or any similar name except when referring to the Software. You must produce and include all copyright notices in their original form for all copies created irrespective of the media or form in which the Software exists. You may not sub-license, rent, sell, or lease the Software. You may not reverse engineer, recompile, disassemble, create derivative works, modify, translate, or make any attempt to discover the source code for the Software or any part thereof. Except as expressly permitted by applicable law, you may not remove from the Software, or alter, any of the trademarks, trade names, logos, patent or copyright notices or other proprietary rights notices or markings, or add any other notices or markings to the Software.

**LIMITED WARRANTY:** Central Command, Inc. warrants that the media on which the Software is distributed is free from defects for a period of thirty (30) days from your date of receipt or purchase date of the Software. Your sole remedy for a breach of this warranty will be that Central Command, Inc. at its option, may replace the defective media upon receipt of the damaged media, or refund the money you paid for the Software. Central Command, Inc. does not warrant that the Software will be uninterrupted or error free or that the errors will be corrected. Central Command, Inc. does not warrant that the Software will meet your requirements. CENTRAL COMMAND, INC. HEREBY DISCLAIMS ALL OTHER WARRANTIES FOR THE SOFTWARE, WHETHER EXPRESSED OR IMPLIED. THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESSED OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

**DISCLAIMER OF DAMAGES:** Anyone installing, using, testing, or evaluating the Software bears all risk to the quality and performance of the Software. In no event shall Central Command, Inc. be liable for any damages of any kind, including, without limitation, direct, indirect, exemplary, special, consequential or incidental damages of any kind (including without limitation lost profits or damage to other systems) arising out of the use, performance, or delivery of the Software, even if Central Command, Inc. has been advised of the existence or possibility of such damages. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN NO CASE SHALL CENTRAL COMMAND, INC.'S LIABILITY EXCEED THE PURCHASE PRICE PAID BY YOU FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept or use, evaluate, or test the Software.

**IMPORTANT NOTICE TO USERS:** THE SOFTWARE IS NOT FAULT-TOLERANT AND IS NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. THIS SOFTWARE IS NOT FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, OR COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY OR PROPERTY DAMAGE.

**GOVERNMENT RESTRICTED RIGHTS/RESTRICTED RIGHTS LEGEND:** Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c)(1) and (2) of Commercial Computer Software-Restricted Rights clause at 48 CFR 52.227-19, as applicable. Contact Central Command, Inc., at P.O. Box 468, Medina Ohio 44258-0468.

**GENERAL:** This License is deemed delivered in, and will be governed by, the laws of the State of Ohio, in the United States of America. This License may only be modified by a license addendum, which must accompany this License or by a written document which has been signed by both you and Central Command, Inc. This License has been written in the English language only and is not to be translated or interpreted in any other language. Prices, costs and fees for use of the Software are subject to change without notice to you. In the event of invalidity of any provision of this License, the invalidity shall not affect the validity of the remaining portions of this License. Vexira, Vexira logo, Central Command, Central Command's logo, EVRT, Emergency Virus Response Team, Without us, there's no defense, are trademarks of Central Command, Inc. Microsoft,



## Vexira Antivirus 2006 for NetWare Servers

Windows, Excel, Word, the Windows logo, Windows NT, Windows 2000 are registered trademarks of Microsoft Corporation. All other trademarks or tradenames are the property of their respective owners.

### CONTACT

This manual provides comprehensive information on operational of our virus protection product. If you have any additional questions about it or would like to share your experience or proposals with us do not hesitate to contact us! Turn to us with confidence, your demands and remarks will be respected.

Address Central Command, Inc.  
Medina, Ohio 44258,  
P. O. Box 468.  
United States

Phone (+1) 330 723 2062  
Fax (+1) 330 722 6517  
Web [www.centralcommand.com](http://www.centralcommand.com)  
E-mail [sales@centralcommand.com](mailto:sales@centralcommand.com)  
[support@centralcommand.com](mailto:support@centralcommand.com)