

# User Guide

## **Vexira Antivirus Scanner**

for Windows/Linux/OpenBSD/FreeBSD/Solaris/AIX





## TABLE OF CONTENTS

<b>VEXIRA ANTIVIRUS SCANNER .....</b>	<b>3</b>
<b>System requirements .....</b>	<b>3</b>
<b>Functionality .....</b>	<b>5</b>
Options .....	5
Some examples .....	11
<b>Scheduled launching (only on Linux/Unix systems).....</b>	<b>13</b>
<b>Returned values.....</b>	<b>13</b>
<b>The configuration file .....</b>	<b>14</b>
<b>Virus database updating.....</b>	<b>15</b>
<b>END USER AGREEMENT .....</b>	<b>16</b>
<b>CONTACT .....</b>	<b>18</b>



## VEXIRA ANTIVIRUS SCANNER

The Vexira Antivirus Scanner programs have been drawn together in this manual, as they are similar and have same functionality. The differences in the operation of the programs will be indicated. The task of the Vexira Antivirus Scanner programs is to find virus infections on the data storage systems and other areas and if possible remove them. The program provides the opportunity for performing regular scans on the data storage devices. The program can be run from the command line and its operation can be adjusted with aid of parameters. An automatic protection can be achieved, to a certain degree, by using the parameters.

Main features of the product:

- Operating in interactive and automatic modes
- Heuristics scanning levels
- Multi-thread scanning
- Enable/disable boot scanning
- Option's values can be stored in configuration file
- Command line quarantine handling
- Incremental virus database update

## System requirements

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

General requirements

-----

x86, amd64, ia64 processor at 200 MHz minimum  
64 MB of RAM  
40 MB of free hard disk space

Supported platforms

-----

WINDOWS: 95/98/Me/NT4/NT4s/2000/2000s/XP/XP-x64/2003s/2003s-x64

LINUX GLIBC 2.2.5, kernel 2.2.x (i386, amd64)

FREEBSD 4.9, 5.4, 6.0 (i386) and 6.0 (amd64)

OPENBSD 3.4, 3.6 (i386)

SOLARIS 9 / SunOs 5.9 (sparc)  
UltraSparc IIe at 500 MHz  
128 MB memory

AIX 4.3, 5.2 (powerpc)  
Maintenance level 10  
Power3 - II (G3)  
256 MB memory

Package naming

-----



# Vexira Antivirus Scanner

vascan-<productversion>-<platform>[version].tar.gz



## Functionality

The Vexira Antivirus Scanner applications act as command line scanners, they scans the system for viruses by options specified in the command line or in the configuration file. It is possible to store the general settings in a configuration file so only your extra settings should be specified in the command line when required. The multi-thread operation provides faster scanning using parallel processing.

The modules of the Vexira Antivirus Scanner program can be found in a simple archived file, you have to unpack them before use. The package contains the following modules:

**vascan.exe | vascan**

Main executable file (on Windows | Unix systems)

**vbeng\*.dll | libvbengine.so**

Scan engine module (on Windows | Unix systems) on the other systems the main executable file

includes this module.

**vascan.ini**

Configuration file

**vdb/**

Folder storing the virus database files

**docs/<lang>/**

Contains:

- Description of the program  
(in text and man page (Unix) format)
- End user license agreement

Use the vascan.exe or vascan file to launch scanning, the settings can be specified in the program's configuration file or by command line options.

### Important!

The presence of previous version(s) of Vexira Antivirus products in the system can have an effect on the scanner so you should uninstall it/them if there is any problem with the product!

If the location of the configuration file is not specified in the command line, then the program is searching for it automatically and tries loading it from the current directory or the program's home directory (where the executed main program file is found). If the configuration file is not found only the command line options will be applied.

You will not be able to launch the program if the required settings are not specified either in the configuration file or in the command line.

Before scanning you are required to set the quarantine directory (-y option), the temporary directory (-t option) and also recommended the location of virus database (-d option).

## Options

Options are divided into groups for best lucidity. We were about to using standard tags and the frequently used ones can be specified by short option names as well. The default settings are indicated at the required topics, these functions are activated without specifying any options.

### Information

-----

**-V --version**



# Vexira Antivirus Scanner

Prints the program's version number then exits.

## **-h --help**

Prints the general command line options, their default values and the application's version number.

## **--full-help**

Prints all the command line options, their default values and the application's version number.

## **Registration data**

-----

### **-k --registration-key**

Specifying the registration key based on your license. The program handles the hyphen separated form, too (XXXXX-XXXXX-XXXXX).

### **-u --registered-user**

Specifying the user name based on your license.

Using program without - valid - registration data you have to wait 30 seconds after starting scanner. You have to specify both the registration key and the user name for successfully registration.

## **Operational settings**

-----

### **--terse**

Enables compact log mode.

Compact mode:

```
/mnt/test/eicar.zip//eicar1.com: found: EICAR skipped.
```

Original mode:

```
/mnt/test/eicar.zip//eicar1.com
```

```
    virus found: EICAR_test_file (NOT killable) ... skipped.
```

### **-q --quiet**

Enables the quiet working method. The program displays only the virus incidents on the screen or in the log file and a summarized statistics at the end of the scan.

Duplicate use:

#### **-qq or --quiet --quiet**

This time the program writes out just the virus incidents to the stdout, summarized statistics also skipped.

Triple use:

#### **-qqq or --quiet -quiet --quiet**

Combines the effect of --terse and -qq options.

IMPORTANT! 'quiet' option affects only the stdout, error messages could be returned by stderr.

### **--summary**

Disables displaying summarized statistics tables about the scan.

If -qq or --quiet --quiet options are also specified, it results reversed action: enables the summary display.

### **-o --old**

The program doesn't show warning message if virus database is older than two weeks.

### **-c --config=FILE**

Specifying the used configuration file with its path. If this option is not set, the program is looking for that file (named vascan.ini by default) in the actual folder. If that one doesn't contain the .ini file the program's home directory will also be scanned for it. The configuration file is suitable for storing common settings needed



# Vexira Antivirus Scanner

for a general scanning. These settings can be redefined by command line options if necessary.

Note that the program will try to locate the files and directories that are specified by relative path in the configuration file starting from the actual directory (from which one the program was launched).

## **-E --engine=FILE**

It is possible to set the location of the virus scan engine file to be used. By default, it is used from the program's home folder.

## **--debug=FILE**

If debug file is specified, the program will create it during the scan process to log detailed information about the program operations. It can help you to analyze the scan if necessary.

## **Scan area settings**

-----

## **-Z --skip-archive**

Archived files will not be scanned.  
The archived files are scanned by default.

## **-b --boot**

The program scans the computer's boot sectors as well. Impossible to scan boot sectors separately. This option is working only on Windows system.

## **-M --skip-mail**

MIME of type files will not be scanned.  
The MIME files scanning is included by default.

## **--symlink=ACTION**

Handling symbolic references (this option is working only on unix systems).

Available values (actions):

follow - uses the link name to identify the file  
resolve - uses the file's own name to identify it  
(in such a cases, it scans the referenced file as a regular file)  
skip - ignores symbolic references  
(in such a case it doesn't scan symlinks)

## **-R --skip-subdir[=PATH]**

The program scans each subdirectories recursively by default if a directory is specified as target. If you set this option, you can select directories or directory fragments to exclude from the scan while the other locations will be scanned recursively. If you use this option without parameter (the -R or --skip-subdir alone) then all the subdirectories of the specified target area will be ignored.

## **-f --file=FILE**

Text file containing paths and files (objects) to be scanned. This option's value locates the path of this text file. The objects will be read by lines from the file.

Special parameter: '-' hyphen ('--file=-'): this time the scanner reads the names of the files or directories to scan from STDIN (only in automatic mode).

**This option can't be used for scanning quarantine items and boot sectors!**

## **Scanned file types**

-----

By default only file types matching any item of the scan engine internal pattern list (default extensions) will be scanned during the virus scan. These are the following:

Program files: \*.exe|\*.com|\*.ov?|\*.sys|  
\*.386|\*.bin|\*.dll|\*.drv|\*.lnk|\*.ocx|\*.prg|



```
*.scr|*.vxd|*.crt|*.prc|*.xml|*.swf
Script files: *.bat|*.ht*|*.js|*.jse|*.vbs|
*.ini|*.csc|*.hlp|*.shs|*.pif|*.ade|*.adp|
*.bas|*.chm|*.cmd|*.cpl|*.inf|*.ins|*.isp|
*.zl*|*.mde|*.msc|*.msi|*.msp|*.mst|*.pcd|
*.reg|*.scr|*.sct|*.url|*.vb|*.vbe|*.ws*|
*.ans|*.tmp|*.mpp|*.mpt|*.
Document files: *.do?|*.rtf|*.wiz|*.eml
Chart files: *.xl?
Access files: *.mdb
Presentation files: *.ppt|*.pot
Compressed files:*.arj|*.a??|*.zip|*.rar|
*.cab|*.gz|*.bz2|*.tgz|*.tar|*.dbx
```

The default pattern values can be altered with the following options:

## **--all-files**

Switches off the pattern matching at all so all file types will be scanned.

## **-p --pattern=PATTERN**

The program scans only that files which match the specified PATTERN.

## **--include=PATTERN**

Adds PATTERN to the default configuration.

## **--exclude=PATTERN**

Excludes PATTERN from the default configuration. This option takes precedence over the above options.

## **-m --match-in-archive**

Pattern-matching inside the archives is enabled by default if you use the built in patterns of the scan engine for scanning (using '--include' and/or '--exclude'). In every other cases it is disabled (using '--pattern' or '--all-files'). This option changes the default value.

## Relations:

- '--all-files', '--pattern', '--include' could not be used at the same time
- If you don't specify either of the above options, the program will scan the files with the default extensions

## PATTERN syntax:

Several patterns can be specified in the pattern option separated by pipe (|). The pattern can contain ? and \* meta-characters (the ? (question mark) is considered as an optional character, the \* (star) is considered as an optional character chain). The program is also able to handle character-classes for more restriction. Character-classes must be specified between brackets (e.g. [abc]). The exclamation mark '!' means negation if it is placed straight after the initial bracket '['. The '-' sign placed between two characters means a character range. If you want the '-' or '!' signs to be a considerable character, you should place it straight before the ending bracket ']'. The program does not make a distinction between small and capital letters.

The '\*' and '?' meta-characters do not match directory separator characters in pathnames. The special '\*\*' sequence can be used to match any arbitrary characters including directory separators. For example:

```
'Program Files\**\*.exe' - each .exe file will be matched in the Program Files
directory and its subdirectories
```

## **Important!**

PATTERN is matched against file's basename (filename without path) if PATTERN itself does not contain directory separator characters or '\*\*' sequences, otherwise full path to the file shall be used. The separator character is '/' on Unix and GNU/Linux, and '\' on Windows that is the same as you can use to convert meta characters to



# Vexira Antivirus Scanner

literals. The application usually consider '\' as directory separator. It should be used duplicated if special characters follow it. These characters are: | \* ? [ ] .

## Scanning methods and actions in case of virus incidents

**-e --heuristics = ( o | off | n | normal | h | high )**

Heuristics level setting. Default: normal level.

o / off - heuristics off

n / normal - normal level

h / high - high level

**-s --scanning = ( q | quick | s | strict | f | full )**

Scanning method setting. Default: regular level.

q / quick - Only scans those parts of the file, which are most likely to contain a virus and does not detect viruses, which can only be detected by using a major amount of system resources (e.g. Excel FORMULA viruses).

s / strict - Optimized scanning method, which detects all viruses registered in the virus database and scans those parts of the file, which are most likely to contain a virus.

f / full - Detects all viruses registered in the virus database and scans the whole file, even those parts, where viruses are not likely to be found.

**--thread=NUM**

Maximum number of program threads. This option's value is 1 by default. The multi-thread applications result in better performance, but this strongly depends on the system settings.

**--timeout=NUM**

Timeout limit of the scanning threads (seconds). Scanning will be cancelled if all the threads or just one of them exceed this limit - depending on the '-timeout-abort' option - and have no activity over the specified time-interval. You should increase this limit in case of large archives or strongly loaded system.

**--timeout-abort**

A '-timeout-abort' option affects the abort mechanism. If this option is set the program will be aborted immediately in case of first timeout.

This function is disabled by default that means the program runs until at least one thread ends within the specified limit.

The default --thread setting allows only one thread to be run so if it exceeds the timeout the program will be aborted.

**-a --action=ACTION**

Setting this option the program can be run in automatic mode so the specified action(s) will be performed without user interaction on virus incidents. If the action option is used repeatedly in the command line (separated by commas (,)), the actions will be considered and performed by their order. The first specified action has the highest priority and so on. If the first action can't be performed the following one will be tried. If the action (-a or --action) is not specified at all, the user is asked to choose an action in case of any incidents (interactive mode). Meaning of the available actions.

k - virus killing from the file (kill)

s - ignores the infected object (skip)

r - renaming the file (rename)

q - moving to quarantine (quarantine)

d - irreversible deleting (delete)

**--remove-macro**

Automatically deletes all the macros from the Microsoft Office documents without any confirmation.

**--sfx**



## Vexira Antivirus Scanner

Enables SFX (self extractor) recognition (it may result in scanner performance decrease (about 30% slower scanning)).

### **--archive-max-size=NUM**

Default value: 0 (in such a case, the program is using the virus scan engine's default value).

If this file size limit is exceeded during the decompression of an archive, the program stops this action and also the scan of the file and returns exploit virus found. (Option's value is in MByte).

### **--archive-max-ratio=NUM**

Default value: 0 (in such a case, the program is using the virus scan engine's default value).

Example value: 50

If the size of the decompressed file is 50 times (or more) greater than the compressed file's, the program will return exploit virus found.

Other explanation (option's value in percent):  $1/n*100$ , where n is the value.

In the example:  $1/50*100 = 2\%$  so if the compression ratio is better than 2% the program will return exploit virus found.

### **-G --greyware**

If you use this option, the program will detect the applications marked as greyware in the database and perform the specified action on them.

Greyware cannot be clearly categorized as malicious or not malicious application because it strongly depends on its use. Generally this kind of software is not harmful program in case it is installed by the user's consent and approval. But it can happen, that this program is installed in the background without the user's permission and in this case it can be used for malicious activity (for example an ftp server program or a remote access application).

So, in case of greyware, we cannot declare the application as malicious or not malicious based on the name or files of the program, it depends on the method of its installation.

## **Quarantine handling**

-----  
The following options can accept one or more KEY(s) or KEY:FILE argument(s), the actions will be performed only on these specified files. If KEY is not specified, the selected action is performed on each file found in quarantine. KEYS belonging to items can be displayed by listing (--list) the contents of the quarantine directory.

### **--status = ( all | clean | deleted | infected | suspicious )**

Using this option you can limit/change the default range of quarantine items to be processed. Select the desired value to process only items being in the specified infection status. The 'all' means that the specified action will be applied to all the items.

This option's default value depends on the specified quarantine option:

--list: 'all'

--restore: 'clean'

--delete: 'infected'

--saveas: 'all'

### **-l --list[=KEY]**

Prints the quarantined files with their KEYS, infection status (see the --status option), original location, file size and date of last modification. Use KEY argument to print only the requested items.

### **--rescan[=KEY]**

Rescans the quarantined files or the specified file (in case of using KEY argument). The --status option is ineffective to the --rescan option.



## **--restore[=KEY[:FILE]]**

Restores all the quarantined items or only the specified ones to their original location cleaned by '--rescan' command. Non-existed directories will not be created, existed files will not be rewritten (except when '--overwrite' option is set).

### **Important!**

This option restores only the cleaned, uninfected files by default, but you can override this operation by using the --status option to specify items with different status. Use this option (--status) if you are sure that the item to be restored is not infected.

## **--delete[=KEY]**

Deletes all the quarantined items or only the specified ones from the quarantine. This option deletes only the infected items, you can override this operation by using --status option.

## **--saveas=KEY:FILE**

Saves the specified quarantined file (KEY) which will be named as you wish in the FILE parameter. The item will be saved encoded so the file will not be equal to the original. This function is useful when you would like to send a file to the Vexira for analysis.

## **-w --overwrite**

Allows rewriting existing files for '--restore' and '--saveas' operations.

## **File- and directory references**

-----

**Non-absolute path name arguments are considered relative to the program's home directory (where the executables are placed).**

## **--log[=FILE]**

Screen output could be saved into a specified log file. If file name is not specified (FILE), the output will be appended to the end of a possibly available log file with the default name (vascan.log).

## **-y --quarantine=DIR**

Specifying the quarantine directory.

## **-t --temp=DIR**

Directory of the temporary files. The TEMP/TMP variable's value is used by default.

## **-d --vdb=DIR**

Specifying the location of the XML descriptor file of the virus database. It is not compulsory to use this option but recommended. If the value of this option is not set, the program will be looking for the virus database in the 'vdb' folder of its home directory.

## **Some examples**

### **vascan.exe c:**

Scans the whole C: drive and asks the user for further action in case of any incidents.

### **vascan.exe --pattern="\*.exe|\*.dll|\*.com" --action=quarantine "C:\Program Files"**

Scans Windows binary files in Program Files directory and the infected files will be quarantined to be available for later scanning.

### **Important!**

File names which contain special characters ('space' in this example) must be specified between quotes (" ") on Windows system!



**vascan --pattern='\*.exe|\*.dll|\*.com' --action=quarantine /mnt/windows/c/**  
Binary files scanning on a mounted Windows partition on Linux. The infected files are to be quarantined automatically.

### Important!

Joker characters have to be protected against shell interpreter on Linux/Unix systems so they have to be enclosed in ' ' (single quote) signs!

**vascan.exe --rescan --action=kill --restore --delete**  
Rescans the quarantine directory's items and try cleaning them. The cleaned items will be restored to their original location with original name. The remaining ones (which can't be disinfected) will be deleted from the quarantine.

**vascan --list --status=suspicious**  
Only the suspicious items will be listed.

**vascan --saveas=0892342:examine.vbq**  
The quarantine item which has key number 0892342 will be copied into the actual directory as name as 'examine.vbq'.

**vascan.exe --file=- --action=kill**  
It reads the names of the files or directories to scan from STDIN (--file), infected files will be cleaned (--action).

**vascan c:\ --skip-subdir="Utils\Arc\*" --terse**  
Scanner will scan the c:\ drive recursively, interactively (action is not specified in the command line) but will not scan any of the directories starting with 'Arc' letters in the 'Utils' folder (--skip-subdir). Compact log is enabled (--terse).

Using short option:

**vascan -b -eh -sf --follow -ak,q /**  
It is scanning for all the files of the system from the root on the highest level, removes the killable viruses and moves the non killable ones into the quarantine. It recognizes that the '--follow' argument is the abbreviation of '--follow-symlink' and several actions are specified in the argument separated by commas.



## Scheduled launching (only on Linux/Unix systems)

Automatic program launching can be realized with the help of 'cron' program. For example if you want the scanner to be launched at 8 pm every evening then register into /etc/crontab:

```
00 20 * * * root <path>vascan<path>vascan.ini
```

## Returned values

Besides the program displays result of scanning on the screen or in log file it is able to inform users about scanning tasks' results by return values. This feature is useful for getting information in case of scanner is run automatically or scheduled.

There are three different basic return values ('A' case):

- 0**  
Suspicious or infected objects were not found.
- 1**  
Suspicious or infected objects were found among target objects.
- 2**  
The specified actions (--action) were performed successfully on the suspicious or infected objects (except if they were "stop" or "skip").

If errors occur during scanning, the program is not able to check or clean some specified objects completely. The return values can change depending on the errors.

Explanation of the return values:

	In the successfully scanned objects		
	no virus found	virus found and not killed	action performed on infected files
'A' case All the specified target objects are scanned successfully	0 (*)	1 (!)	2 (*)
'B' case Failed to scan all the specified target objects	3 (?)	1 (!)	5 (?)
'C' case Failed to scan all the specified target objects because of system errors	6 (?)	1 (!)	8 (?)
'D' case Failed to scan all the specified target objects for lack of file format support	9 (?)	1 (!)	11 (?)



## Legend:

number: the return value itself

(\*): after scanning the scanned path is surely virus free

(!): after scanning the scanned path contains infected files

(?): after scanning the scanned path may contain infected files

## 'B' case:

Some files could not be read because of password protection or they were corrupted or exploit danger. These files may carry malicious codes.

## 'C' case:

System error during scanning (e.g.: access denied, specified path not found).

After it had been repaired you should retry scanning. The cause of the error may be that the specified files do not exist or the program doesn't have permission to access them. High loaded systems could also result the same error codes.

## 'D' case:

Some files were not scanned successfully. Although the virus scan engine recognizes their format your current scan engine version doesn't support them. You need to update your scanner program to analyze these files completely.

Higher error codes mean bad parameter specification generally:

### 255

Invalid command line or configuration file parameters, check them!

### 254

Failed to run scan engine or the specified virus database does not exist!

### 253

Bad (incompatible) virus database. Check its version!

### 252

Failed to start scanning maybe for short system resources!

### 251

Unable to initialize quarantine! Check the value of '--quarantine' parameter!

### 250

Program running aborted by external request. (SIGINT, SIGTERM)

Return value is always 0 if quarantine operations could be performed successfully.

## **The configuration file**

The configuration file is line-oriented for simple handling. Each line contains different settings, the option's name is conform to long option names.

You can use both the one character long- and the more character long options without dash ('-' or '--'). The options' values are similar to the command line options. In case of logical options the presence or the lack of the related option specifies if the function is enabled or disabled similar to the command line specification. Comments can be specified after '#' character in a new line or at the end of an opened line.



## ***Virus database updating***

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 defense. 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.

### **On Windows system**

-----

You can update the virus database manually. Our virus database-set consist of several files. The program stores the database files in the 'vdb' folder. You need to update all the files of the following folder from our FTP server:

`upd.vexira.com/pub2006/vexira/vdb.9/`

Finally replace the old virus database files with the downloaded ones.

### **On Unix systems**

-----

We create a script to automate the update process. Find it in the package named `vdbupdate.sh`.

It is going to download the virus database, copy its files into the correct directory ('vdb' by default). Updating will only be performed, if the database available in the server is newer than one installed on your computer. Otherwise the database will be left unchanged.

Available parameters of the script:

```
-h print list of valid parameters
-v verbose output
-t temporary directory, it must not exist (default $TMPDIR)
-i directory where to put the new virus database file (default $LIBDIR)
-p use HTTP instead of the default FTP
```

To run the script, you need the `wget` and `sed` programs! With the help of `cron`, you can schedule the script execution.



## 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 Scanner

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,



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)