

# User Guide

## **VEXIRA FOR SAMBA SERVERS**

1.2





## TABLE OF CONTENTS

INTRODUCTION .....	3
<b>VEXIRA ANTIVIRUS FOR SAMBA SERVERS .....</b>	<b>4</b>
System requirements .....	4
Minimal required Linux distributions .....	4
Supported Samba versions .....	4
Installation, uninstallation .....	5
Operation.....	5
<b>Configuration settings .....</b>	<b>6</b>
General settings.....	6
Notification .....	7
Available tokens for messages .....	8
Registration data.....	8
Including external configuration file .....	8
<b>VEXIRA SCAN DAEMON .....</b>	<b>9</b>
Executable files .....	9
Database update.....	9
Configuration files.....	10
<b>END USER AGREEMENT .....</b>	<b>17</b>
<b>CONTACT .....</b>	<b>19</b>



## INTRODUCTION

The package includes the Vexira Antivirus for Samba Servers and the Vexira Antivirus ScanDaemon daemon programs.

The name structure of the package:

```
vasambashield-<vasambashield-version>-<vascand-version>-<opsystem>.tgz
```

e.g.: vasambashield-1.2.0-1.2.0-linux-i386.tgz

The 'vainst-pkg.pl' is the main install script file, run it to install both the vasambashield and vascand packages.

Available install script parameters:

```
--no-update
```

The installer doesn't install the vascand.

The installer tries to install the vascand package first. If the installer finds an installed instance of the vascand in the system and its version is less than the current version, it removes the older one and installs the new one (if it is not disabled by the --no-update parameter). After vascand has been installed successfully, the script also installs or updates the vasambashield.



## VEXIRA ANTIVIRUS FOR SAMBA SERVERS

The program ensures comprehensive virus protection for Samba file servers running on Linux or Solaris operating system. The on access protection keeps the computer virus free. It works totally transparent mode, scans the files in the background, users don't perceive its operation.

The program is divided into two modules:

- shield module, which performs the scanning functions
- vfsemu module, which is an interface for the different Samba version

### **System requirements**

Supported operating systems:

- Linux i386/amd64
- Solaris 9 (sparc), 10 (i386)

Requirements for all the supported platforms:

- 256 MB free memory
- 100 MB free hard disk space
- wget (for update)
- perl5 (for update)
- Vexira Antivirus ScanDaemon

Requirements by platforms:

- Intel Pentium (or compatible) processor at 300 MHz (Linux, Solaris 10)
- Ultra Sparc IIe processor at 500 MHz (Solaris 9)
- Minimal required for Linux: GLIBC 2.2.5, kernel 2.2.1

### **Minimal required Linux distributions**

SuSE 8.0  
RedHat 7.3  
Debian 3.0 (woody)  
Mandrake 9.0  
Slackware 8.1

### **Supported Samba versions**

Samba 2.2.1 - 3.4.0

Remark:

Those Samba versions that are newer than the mentioned above may be supported if their VFS module interface is compatible with the earlier versions. The 2.2.1-2.2.3 versions are only supported if the Samba daemon's binary was built with exported symbols. 3.0 alpha XY versions are not supported.



## Installation, uninstallation

The program is available in a tgz package:

Unpacking:

```
tar -xzvf vasambashield-<version>-<platform>.tgz
```

```
Installation: vasambashield-install.pl
```

```
Uninstallation: vasambashield-uninstall.pl
```

## Operation

To activate the virus protection, the user has to modify the Samba's configuration file.

Setting of the various versions is differ:

**In case of 2.x.y Samba version:**

```
vfs object = <vfs module's name with path>  
(specify absolute path)
```

**In case of 3.x.y Samba version:**

```
vfs objects = <vfs module's name with path>  
or  
vfs objects = <vfs module's name>
```

If this option already has parameter in the configuration file then the required line must be inserted to the previous ones.

The options above can be specified generally for all the shares (the option and its parameter must be placed in the [global] section) or for certain shares (the option and its value must be placed into the required share(s)).

Examples:

```
vfs object = /usr/lib/samba/vfs/vasambavfsemu.so
```

```
or
```

```
vfs objects = vasambavfsemu
```

The program scans for viruses only on that connection that have been established after the configuration file's modification, the previous ones will not be concerned.



## Configuration settings

The configuration file is located on the `/etc/vasambashield/general.conf` path.

Settings in the `[general]` section

### General settings

#### **registration-username**

Enter user name.

#### **registration-key**

Enter registration key.

#### **scanaddress**

Scan daemon's network address.

There are two supported socket types: unix socket and internet socket.

unix socket syntax: `unix:<path>`

internet socket syntax: `inet:<hostname or ip address>:<port>`

Example: `scanaddress= unix:/var/run/vascand`

#### **engine\_path**

#### **vdb\_file**

These options need to be set when we use direct connect to the virus scan engine (without using `scandaemon`) - this is the default setting. The `engine_path` option has to point to the virus scan engine file, the `vdb_file` option to the virus database file.

Example: `engine_path=/usr/lib/libvbengine.so`

`vdb_file=/var/lib/vexira/vdb.xml`

#### **killable\_action**

If the virus is killable one of the following actions can be performed.

Available values:

`delete` - deleting file

`kill` - killing virus

`rename` - renaming file

`skip` - ignore incident

Default: `kill`

#### **non\_killable\_action**

If the virus is non-killable one of the following actions can be performed.

Available values:

`delete` - deleting file

`rename` - renaming file

`skip` - ignore incident

Default: `skip`

#### **suspicious\_action**

In case of suspicious file is found, one of the following actions can be performed.

Available values:

`delete` - deleting file

`rename` - renaming file

`skip` - ignore incident

Default: `skip`

#### **scan\_method**

Specifying scanning method.

Available values: `strict/fast/full`

Default: `strict`



## **heuristic\_level**

Specifying the level of the heuristics scanning.

Available values:

normal - normal level

off - heuristics off

high - high level

Default: normal

## **access\_on\_error**

Allow or deny access to the file if error(s) occurred during the scan.

Values: allow/deny

## **log\_level**

Log level setting.

Available values:

EMERG or 0

ALERT or 1

CRIT or 2

ERR or 3

WARNING or 4

NOTICE or 5

INFO or 6

DEBUG or 7

DEBUG0 or 7

DEBUG1 or 8

DEBUG2 or 9

DEBUG3 or 10

DEBUG4 or 11

DEBUG5 or 12

DEBUG6 or 13

DEBUG7 or 14

DEBUG8 or 15

Default: INFO

## **file\_log**

Using log-file (yes/no).

Default: yes

## **log\_path**

Location of the log file. This file stores the log events created during the program's operation.

Default: /var/log/vasambashield/general.log

## **virus\_log\_path**

Location of the virus-log file. This file stores the log events created during virus scanning.

Default: /var/log/vasambashield/VirusScan.log

## **samba\_log**

Using Samba log-system (yes/no).

Default: yes

## **syslog**

Using syslog (yes/no).

Default: no

## **Notification**

**message\_sender = Samba Shield**

Message sender's name.



## **message\_virus\_killed = "Message"**

Sent message in case of virus found and killed. It must be specified between quotes, you can use tokens in the text.

## **message\_access\_denied = "Message"**

Sent message in case of virus found but any error occurred. It must be specified between quotes, you can use tokens in the text.

The following settings must be specified to display the messages in case:

- using nt based Windows: running Messenger service
- Windows 9x: installed network message sender application (e.g. Winpopup)

## **Available tokens for messages**

### **%virus%**

Last found virus name.

### **%file%**

The scanned file's name.

### **%version%**

SambaShield version number.

## **Registration data**

### **registration-username**

Enter user name.

### **registration-key**

Enter registration key.

## **Including external configuration file**

It is possible to include external configuration files into the main configuration file. These linked files will be processed as a part of the main configuration file.

The architecture of external configuration files must be the same as the original, use the @ sign to specify external link to a file in the main configuration file.

Example:

### **@messages.conf**

The default configuration file includes external file, too, linking messages sent in case of virus incident. It is practical to change the language of warning messages easily and quickly.



## VEXIRA SCAN DAEMON

The Vexira Antivirus ScanDaemon (hereinafter called scandaeomon) provides an interface for the remote client program to utilize the full functionality of the virus scan engine through unix or internet socket. The package also includes a command line scanner client program (vascan).

To establish the connection between the scandaeomon and its client(s) you have to set a common communication address. Use the 'address' option in the configuration file of the scandaeomon to set this address.

When the client is started, it tries to connect to the scan daemon and if it fails it displays an error message.

### *Executable files*

#### Parameters of the scandaeomon

-----

##### **vascand [options]**

Scan daemon binary file. Possible options:

-n, --nodaemon - no daemon mode (run in the console where started)  
-v, --version - display the version of vascand and exit  
-b, --build - display the version and build of vascand and exit  
-c FILE, --config=FILE - read configuration from FILE  
-p FILE, --pid\_file=FILE - save the pid to FILE  
-d FILE, --vdb\_file=FILE - virus database descriptor file  
-a ADDR, --address=ADDR - connect to ADDR  
-k SEC, --conn\_timeout=SEC - connection timeout in seconds  
-r SEC, --read\_timeout=SEC - read timeout in seconds  
-w SEC, --write\_timeout=SEC - write timeout in seconds

#### Parameters of Scan daemon init script (found in the /etc directory)

-----

##### **vascand [options]**

start - start scan daemon  
stop - stop scan daemon  
restart - restart scan daemon  
cfgreload - reload configuration file  
vdbreload - reload virus database

#### Command line scanner client

-----

##### **vascan [options]**

The available options are described below where the configuration file is detailed (vascan.ini).

### *Database update*

You can update the virus database manually or automatically by the updater script found in the package.

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.

### Automatic update

-----

We create a script to automate the update process, it is in the /usr/bin directory (vas\_vdbupdate.sh).

Execute it, it is going to download the virus database, copies it into the correct directory and activates it. Updating will only be performed, if the database available on the server is newer than one on your computer. Otherwise the database will be left unchanged.

To execute the script, you should enter the vas\_vdbupdate.sh command. It is possible to use parameters, too:

```
-f, --ftp          uses FTP update source
-h, --http,       uses HTTP update source
-v, --verbose,    verbose mode
--help,          displays help
```

### Example:

```
vas_vdbupdate.sh -v --http
```

It downloads the database from the HTTP source and the progress bar will be displayed.

To run the script, you need wget program! By the help of cron, you can schedule the script executing to be performed by half an hours. Register into /etc/crontab:

```
0,30 * * * * root /usr/bin/vas_vdbupdate.sh
```

### Manual update

-----

Our virus database-set consist of several files, you need to update all the files from our FTP server from the following folder and copy them to the virus database folder (/var/lib/vexira):

```
upd.vexira.com/pub12/vexira/vdb12/
```

You can activate the new database by the "vascand vdbreload" command.

## Configuration files

### ----- Configuration file of Scan daemon (vascand.conf) -----

The configuration file stores the settings in hierarchical structure. The storing mechanism based on the encapsulation concept which means that user has to specify the storing path (section) for each coherent setting group step by step.

The path (section) must be specified between square brackets in the configuration file:

```
[General]
```



## VEXIRA for Samba Servers

Enter comments by using semicolon (;) before the comment text. The characters entered after semicolon will not be interpreted by the parser.

The configuration file ('vascand.conf') can be found in the /etc/vexira directory by default.

Options to be set in the [General] section:

**address=unix:/var/run/vascand**

Address to listen on.

Two socket types are supported: unix socket and internet socket.

unix socket syntax: unix:<path>

internet socket syntax: inet:<hostname or ip address>:<port>

Default: unix:/var/run/vascand

**vdb\_file=/var/lib/vexira/vdb.xml**

Path to virus database descriptor file.

Default: /var/lib/vexira/vdb.xml

**pid\_file=/var/run/vascand.pid**

Path to pid file.

Default: /var/run/vascand.pid

**conn\_timeout=1**

**read\_timeout=180**

**write\_timeout=1**

Socket timeout in seconds.

conn\_timeout: connection accept timeout

read\_timeout: socket reading timeout

write\_timeout: socket writing timeout

Default value is 1 to all options.

-----  
**Configuration file of the command line scanner (vascan.ini)**  
-----

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.

The configuration file (vascan.ini) can be found in the /etc/vascan directory by default.

**Connection**  
-----

**--attach**

Scan daemon's network address.

There are two supported socket types: unix socket and internet socket.

unix socket syntax: unix:<path>

internet socket syntax: inet:<hostname or ip address>:<port>

Example: attach= unix:/var/run/vascand

**--engine**

**--vdb**



## VEXIRA for Samba Servers

These options need to be set if we would like to connect directly to the virus scan engine (without using scandamon). The engine option has to point to the virus scan engine file, the vdb option to the virus database file.

Example: engine=/usr/lib/libvbengine.so  
vdb=/var/lib/vexira/vdb.xml

### Information

-----

#### **-V --version**

Prints the version number of the program, scan engine and vdb.

#### **-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 (XXXXXX-XXXXXX-XXXXXX).

#### **-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

-----

#### **-T --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.
```

#### **-TT --terse --terse**

Only found information will be logged.

#### **-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.

#### **-qqqq or --quiet --quiet -quiet --quiet**

If there is no need to notify the user (there was no malware found during the scan), entries will not be created into the log file.



## **--summary**

Disables displaying summarized statistics tables about the scan.  
If `-qq` or `--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 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).

## **--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.

### **-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).

## **Scanned file types**

-----



## **--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 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 = ( fa | fast | s | strict | fu | full )**

Scanning method setting. Default: regular level.



## VEXIRA for Samba Servers

fa / fast - 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.

fu / 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)

d - irreversible deleting (delete)

### **--remove-macro**

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

### **-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.

## **File- and directory references**

-----



## VEXIRA for Samba Servers

### **-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.

### **--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).



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



## VEXIRA for Samba Servers

**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 <http://www.centralcommand.com>  
Support <http://www.centralcommand.com>  
E-mail [sales@centralcommand.com](mailto:sales@centralcommand.com)  
support@centralcommand.com