

User Guide

Vexira Antivirus for GroupWise





TABLE OF CONTENTS

VEXIRA ANTIVIRUS FOR GROUPWISE	3
Minimal system requirements	3
Additional requirements for Spam filtering and Post Office protection	3
Installation.....	4
Automatic installation.....	4
Manual installation.....	5
Install Internet Agent protection	5
Install spam filter.....	6
Install Post Office filter	6
Program's structure	7
Program's user interface.....	7
Detailed overview	8
General settings.....	8
Internet Agent protection	9
General settings (IA).....	9
Scan parameters	10
On virus found	11
Domains.....	12
Spam filter.....	12
Trusted senders.....	14
Unprotected recipients.....	14
Unfiltered senders.....	14
Unfiltered recipients	14
File filter patterns	14
File filter exceptions	15
Quarantine	15
Post Office protection	17
General settings (PO)	17
Scan parameters	18
Post Offices	18
Scheduler.....	19
Quick scan	20
END USER AGREEMENT	21
CONTACT	23



VEXIRA ANTIVIRUS FOR GROUPWISE

Nowadays most of the viruses and other harmful programs arrive in e-mail, therefore filtering the e-mail traffic of companies for viruses is crucial to avoid virus infections. The dramatic increase in the number of spam e-mails puts a heavy load on e-mail servers and deleting these e-mails can take a long time therefore every mail filtering product must contain an effective spam filter.

The product can be installed as a module of Vexira Antivirus for NetWare Servers. Integrated into the mail system, the Vexira Antivirus for GroupWise provides continuous protection by filtering the e-mail traffic for viruses and other malicious codes and spam. The Post Office protection module provides off-line virus protection for post offices found in the system.

Features:

- Outstanding performance, guaranteed by virus scanning engine
- Modular architecture for ease of use
- Virus scanning of incoming and outgoing messages and the removal of all viruses
- WormBuster for blocking I-Worms instantly
- Replacement of infected attachments with warning attachments
- White list (permissive list)
- Advanced notification and log system: a notification can be sent to the administrator and/or the sender of the message.
- Automatic program and virus database update via FTP
- Traditional, easy-to-use Novell user interface
- Easy integration with the GroupWise system
- Statistical spam filtering with many evaluation methods

Minimal system requirements

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

- Vexira Antivirus for NetWare Servers 2.2.9-X.X.X version
- Novell NetWare Server 4.11 + latest Support Pack
- Novell GroupWise 5x
- Intel Pentium (or compatible) at 200 MHz
- 64 MB of RAM
- 40 MB of free hard disk space

Additional requirements for Spam filtering and Post Office protection

- For Spam filtering: Novell NetWare Server 5.1 + **SP4** or Novell NetWare Server 6 + **SP1**
- For Post Office filtering: Novell NetWare Server 5.1 + **SP8** or Novell NetWare Server 6 + **SP5** and minimum Novell GroupWise version 6.5
- +64 MB of RAM
- +40 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).

Important!
Vexira Antivirus for GroupWise can only be used if Vexira Antivirus for NetWare Servers program is installed and activated!

Automatic installation

The following package is available:

`gwise-<product version>-<poa module version>-<language>.exe`

Example:

`gwise-2.2.08-1.0.05-en.exe`

Important!
If the server protection is functioning, it protects the executable files against writing by default. This can be a problem during the automatic installation so you are recommended to release write protection until the installation process has finished. The simplest way to do this is to stop the server protection while installing. After successful installation it will be restarted automatically.

- After the welcome panel and accepting the license agreement, you can set the target folder that you want to install the product to. The product can only be installed into such a folder that has the Vexira Antivirus for NetWare Servers program's modules installed before.
- 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 *Internet Agent protection* is essential to install, the others are 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).

Internet Agent protection

- *Create domain*: If it is checked, the program tries to find the GroupWise's **domain** folder (this is the same as the one that was set when the mail server has been installed) on the selected volume. If it couldn't find the folder automatically, you have to specify it manually. After setting this parameter, the program performs the actions detailed in the *Install Internet Agent protection* and *Install Spam filter* sections.

- *Start protection*: If it is checked, the Internet Agent protection will be started automatically on the server after the installation.

- *Modify autoexec.ncf*: If it is checked, the necessary modification will be performed in the **autoexec.ncf** file (consult the *Install Internet Agent protection* section for more).

- *X-Spam-Flag support*: Enables IA-side *Junk Mail* handling. To use this function, other settings are needed which are detailed in the [Spam filter](#) section.

Post Offices protection

- *Certify application to access post offices*: If it is checked, the program creates the activation key needed for the Post Office filter (consult the *Install Post Office filter* section for more).



Vexira Antivirus for GroupWise

- *Start module*: If it is checked, the Post Office filter will be started automatically on the server after the installation.
- *Modify autoexec.ncf*: If it is checked, the necessary modification will be performed in the `autoexec.ncf` file (consult the *Install Post Office filter* section for more).

GroupWise settings

- *Start module*: If it is checked, the GroupWise protection module will be started automatically on the server after the installation.
- After these settings the installation process will be started and the selected actions will be performed.

Manual installation

The following package is available:

`gwise-<product version>-<poa module version>-<language>.zip`

Example:

`gwise-2.2.08-1.0.05-en.zip`

Install Internet Agent protection

Copy `VAGWIA.NLM`, `VAGWISE.SET`, `VANOTIFY.NLM` and `VAGWSET.NLM` files into the directory of `VAGUARD.NLM` and `VBENGINE.NLM`.

Create a `VAGWIA` communication directory inside the GroupWise Internet Agent's domain-directory (`... \WPGATE \GWIA`). In this directory (`VAGWIA`) create the `QUARANT`, `TEMP`, `SEND`, `RECEIVE`, `RESULT` subdirectories. This is needed because messages are moved to these directories for virus scanning from GroupWise's same folders.

Set GroupWise Internet Agent to use the communication directory with the help of NetWare Administrator or ConsoleOne programs (find the *Advanced* button on *Server Directories* setting panel of GWIA properties). You should modify the SMTP Service Queues Directory field in the appeared window to the communication directory (`... \WPGATE \GWIA \VAGWIA`). By specifying the SMTP Service Queues Directory, GWIA will not forward messages through the SMTP channel unless the SMTP Service Queues Directory field is deleted or the `VAGWIA.NLM` is loaded.

Attention!

By specifying the SMTP Service Queues Directory, GWIA will not forward messages through the SMTP channel if the `VAGWIA.NLM` is loaded or the SMTP Service Queues Directory field is deleted!

Modify the `VAGWISE.SET` file as required with the help of `VAGWSET.NLM`'s menu system. Don't forget to set GroupWise Internet Agent's work directory, and the quarantine and work directory.

Attention!

Using `VANOTIFY.NLM` you can apply new settings without restarting the protection system.

To activate the GroupWise protection, load the `VAGWIA` program (`load vagwia`). If these steps have been performed in order, mail flow will be recovered in the SMTP channel. From now on, `VAGWIA.NLM` will "help" in forwarding mail while it scans mails according to its settings.

If you want the GroupWise protection module to be started automatically together with the server then you should insert the next line into the `SYS:SYSTEM/AUTOEXEC.NCF` file:

```
load vagwia.nlm
```



Install spam filter

After you have installed the Vexira Antivirus for NetWare Servers and the Vexira Antivirus for GroupWise you, have to copy the `SPAME.NLM` module and the `VEXIRA.SDB` spam database into the installation directory (for example: `SYS:/SYSTEM/VEXIRA`).

To finish spam filter installation create a directory into the communication directory (`...\WPGATE\GWIA\VAGWIA` as suggested) for quarantined spam mails named `SPAMQUAR`.

To control spam filter, find the *Spam filter* menu between the *Internet Agent protection* settings.

Important!
Using spam filter results performance impact to the server. Starting or stopping of the program may take several minutes!

Install Post Office filter

Copy the `VAPOSCAN.NLM` file into the installation directory (for example: `SYS:/SYSTEM/VEXIRA`).

To activate Post Office module, you need to generate an identifier key that allows the Post Office scanner to access mails stored in the post offices. Key generation must be done on a Windows client before the first run of POA scanner. Run the `vapotapp.exe` file (it also needs the `gwtapp.dll`) found in the package to generate. If existed key is found, you will be warned about overwriting.

You need to enter the following path to generate the key:

- GroupWise domain database file path on the Novell server (`wpdomain.db`)
- Vexira Antivirus for GroupWise configuration file path (`vagwise.set`)

After key generation, the GroupWise internal communication mechanism replicates the key to the other agents. It can take some minutes according to the network communication speed.

Start the `VAPOSCAN.NLM` then configure the Post Office filter with the help of `VAGWSET.NLM`.

To run Post Office protection, run the `VAPOSCAN` program (`load vaposcan`).

If you want the Post office protection module to be started automatically together with the server then you should insert the next line into the `SYS:SYSTEM/AUTOEXEC.NCF` file:

```
load vaposcan.nlm
```



Program's structure

The Vexira Antivirus for GroupWise cooperates with Vexira Antivirus for NetWare Servers. Proper functioning can only be guaranteed if Vexira Antivirus for NetWare Servers is installed and activated.

Attention!

VAGWIA.NLM needs **VBENGINE.NLM** to scan letters and forwards its log entries to **VAGUARD.NLM** so always unload **VAGWIA.NLM** before unloading Vexira Antivirus for NetWare Servers!

If the content of **VAGWISE.SET** is modified while running **VAGWIA.NLM**, the **VAGWIA.NLM** can be warned by loading **VANOTIFY.NLM** then the **VAGWIA.NLM** will reload settings.

Program's user interface

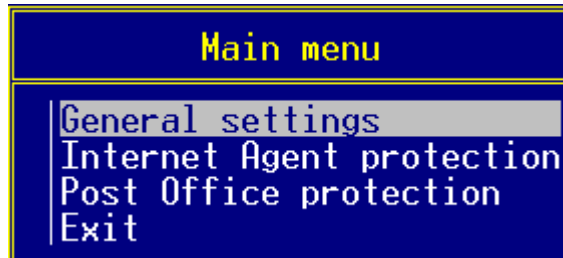
The program's settings can be managed through NetWare's **NWSNUT.NLM** menu system. The following keys are available to navigate in the menu system:

- Cursor keys, **PgDn**, **PgUp** - Movement among individual menu items.
- **Enter** key - Selecting a menu item.
- **ESC** key - Existing a menu item or the program.
- **F1** key - Displays help.
- **Delete** key - Deleting entry.
- **Insert** key - Inserting key.



Detailed overview

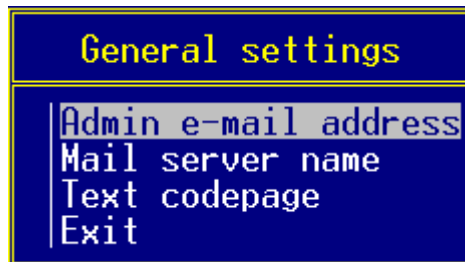
The program's settings can be found in the `VAGWISE.SET` file. The settings can be modified with the help of `VAGWSET.NLM`'s menu system. The menu system's structure:



Main menu

Settings of Internet Agent and Post Office protection could be found in two separated menu item. Options found in the *General settings* are used both IA and PO protection modules. The following lines provides you detailed information about configuration of the anti-virus system.

General settings



General settings

Options found in this menu are common options for the Internet Agent and Post Office protection:

Admin e-mail address

The notification mail will be forwarded to the specified address.

Mail server name

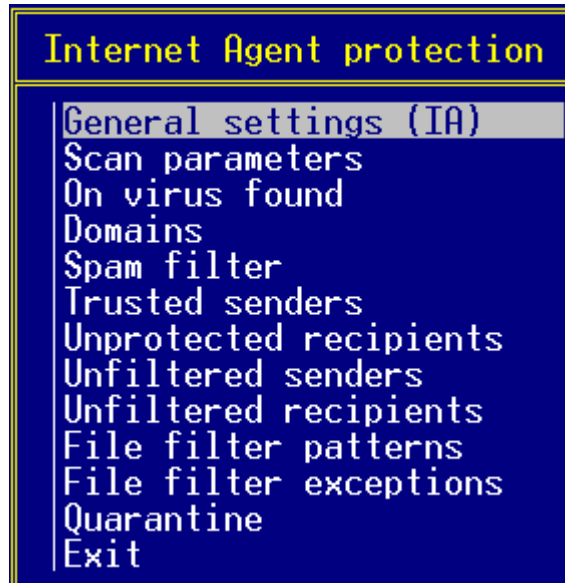
SMTP server's name or IP address needed for mail delivery to the recipient.

Text codepage

The code page of texts connected to event notification can be set here.



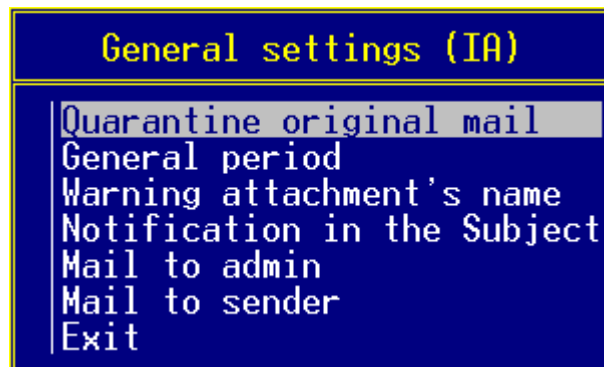
Internet Agent protection



Internet Agent protection

The Internet Agent is responsible for e-mail transmission and makes connection between the Internet and local networks. Detailed information about virus and spam filter could be found hereafter.

General settings (IA)



General settings (IA)

Quarantine original mail

If an e-mail is modified, the original one will be moved to the quarantine.

General Period

Time period setting for those tasks which do not belong to either of domains. The program executes the tasks by the specified interval.

Warning attachment's name

The warning attachment's name, which will be sent with the modified e-mail can be set here.

Notification in the subject



If this option is enabled, the program inserts information in the mail's subject line to inform the user on the results of scanning.

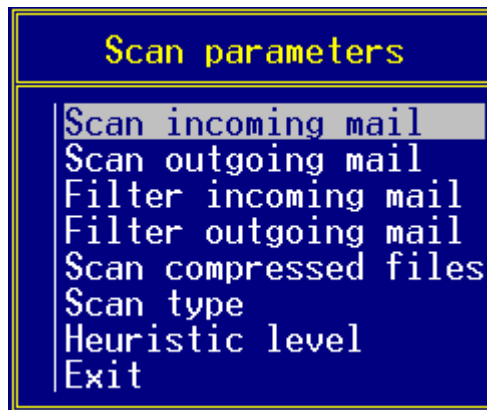
Mail to admin

Enable/disable sending notification mail to the administrator on incidents.

Mail to sender

Enable/disable sending notification mail to the user on incidents.

Scan parameters



Scan parameters

Scan incoming mail

Scanning of incoming mail can be enabled or disabled.

Scan outgoing mail

Scanning of outgoing mail can be enabled or disabled.

Filter incoming mail

If the incoming e-mail has an attachment, which matches any of the patterns set in file filter patterns, the program will remove it if this option is enabled.

Filter outgoing mail

If the outgoing e-mail has an attachment, which matches any of the patterns set in file filter patterns, the program will remove it if this option is enabled.

Scan compressed files

The scanning of compressed attachments can be enabled or disabled.

Scan type

The virus scanning engine is able to scan for and detect viruses according to the set methods/levels. It is possible to choose the needed scanning method in the components in the software. The following levels are available:

- **Fast**
Scans only 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).



Vexira Antivirus for GroupWise

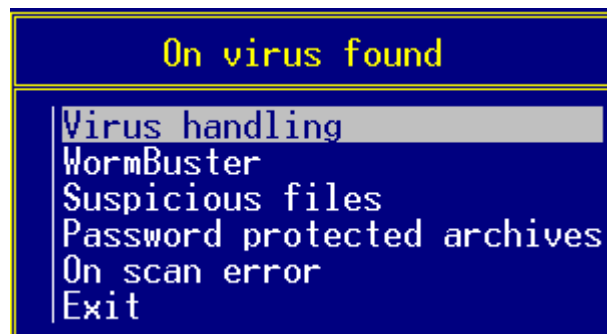
- **Strict**
Optimized scanning method, which detects all viruses registered in the virus database and scans those parts of the file, which are most likely to contain a virus.
- **Full**
Detects all viruses registered in the virus database and scans the whole file, even those parts, where viruses are not likely to be found.

Heuristic level

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:

- **Off**
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.

On virus found



Actions in case of virus found

Virus handling

The action, which will be performed on the infected file can be set here. The infected file can be deleted, disinfected or you can also delete the whole mail, if you want.

WormBuster

If you enable this function then the mails infected by I-Worm-type will be blocked without notification.

Suspicious files

The action, which will be performed on files that are considered suspicious by the heuristic scan can be set here.

Password protected archives

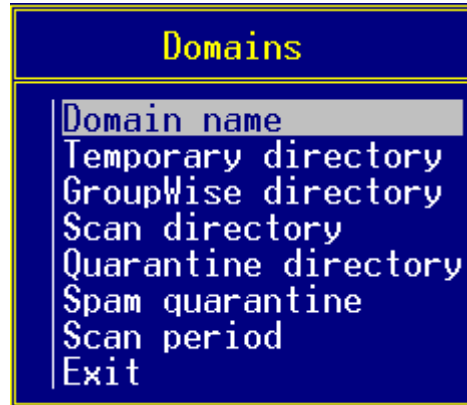
If a compressed file is fail to scan because it is protected by password then the program will block it if this option is enabled.

On scan error



If any errors occur during scanning the certain mail can be blocked if this option is enabled.

Domains



Domain settings

Domain name

The protection area's name can be specified here.

Temporary directory (e.g. `... \WPGATE\GWIA\VAGWIA\TEMP`)

Temporary files will get into this directory.

GroupWise directory (e.g. `... \WPGATE\GWIA`)

The GroupWise Internet Agent's work directory can be specified here. GroupWise's **SEND**, **RECEIVE**, **RESULT** directories can be found here.

Scan directory (e.g. `... \WPGATE\GWIA\VAGWIA`)

The GroupWise's work directory for SMTP scan can be specified here (**SEND**, **RECEIVE**, **RESULT**, quarantine and temporary directories must be created manually in this directory).

Quarantine directory (e.g. `... \WPGATE\GWIA\VAGWIA\QUAR`)

Specify a directory, into which the modified mail's original instances will be placed.

Spam quarantine (e.g. `... \WPGATE\GWIA\VAGWIA\SPAMQUAR`)

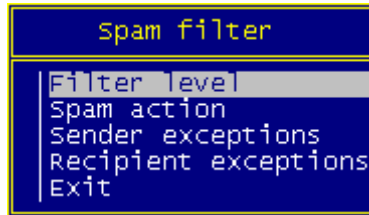
Quarantine directory for that mails' original instances marked as spam by the active spam filter.

Scan period

A scan period can be set inside the current protection area.

Spam filter

Vexira Antivirus for GroupWise made for mailing systems to protect them against virus attacks and now it is provided with spam filtering as well to protect you and your computer against unsolicited mails.



Spam filter settings

Filter level

You can enable or disable the activity of the Spam filter and set its sensibility.

If you select the No filter item, the Spam filter will be disabled. If the other settings are used, the Spam filter will be activated and its sensibility depends on your selection.

Spam action

The following options can be performed on the mails which are declared as spam by the filter:

- None: the mail is forwarded without any interaction and you can have the mail copied into the quarantine directory.
- Mark mail:
 - Subject change
You can change the content of the *Subject* field of the mail in the appeared window. You are allowed to specify the new content and use the `%Subject%` token representing the content of the original *Subject* field of the mail.
 - Insert X-Spam-Flag
Yes: the "X-Spam-Flag: Yes" field will be inserted in the e-mail's header. The GWIA will identify e-mails which will be forwarded to the *Junk Mail* folder with this flag.
 - Quarantine copy
Yes: Besides executing one of the above options, the original copy of the e-mail which has been marked as spam will be moved to the quarantine.
- Blocking: the mail will not be forwarded to the recipient(s), it will be deleted. But you can have the mail copied into the quarantine directory, as well.
- To quarantine: the mail will not be forwarded to the recipient(s), it is moved to the quarantine directory.

Keep in mind, if spam mail is detected, log message is got into the `VEXIRA.LOG` file without exception. You can set the quarantine directory in the *Domains* menu item. It is recommended to use the `SPAMQUAR` directory which having been created in the course of installation.

Other Junk Mail folder settings

If you would like to forward e-mails, which have been marked as spam to the *Junk Mail* folder, and you have selected the option to insert the *X-Spam-Flag*, please check the following settings:

- Select the GWIA object in the ConsoleOne system administration program (usually it is called GWIA).
- After right-clicking on the object, select the *Properties* option from the displayed list.
- Click on the *SMTP/MIME* tab and select *Junk Mail* from the list.
- A dialog will be displayed where the *Flag any messages that contain x-spam-flag: yes or...* option must be checked..

The following settings must also be applied for proper operation:



- On the main page of ConsoleOne, in the left tree, under *GroupWise System* the protection area (domain) or post office must be selected, where the functionality should be activated (if several protection areas are needed, the settings must be applied to all of them).
- After right-clicking on the selected item, choose *GroupWise Utilities\Client Options* in the list and click on the *Environment* button on the displayed dialog.
- On the *General* tab of the displayed dialog, the *Enable Junk Mail Handling* option must be checked in the *Junk Mail Handling* section.
- Select the *Enable Junk Mail using Junk Mail list* option and other options as well if needed. The settings can be locked by clicking on the lock icon on the right side so that the option for the post office or mailbox which belong to the object cannot be modified.

Sender exceptions

Mails sent from that address (domain name) enumerated in this settings are not filtered by the spam filter, these are forwarded to their recipients without any spam checking. You can use the **INSERT** and the **DELETE** keys to add or remove items (address) from the list.

Recipient exceptions

Mails received by that address(es) (domain name(s)) enumerated in this settings are not filtered by the spam filter.

Trusted senders

The program will not scan messages coming from the given addresses. The following rules are applied to the addresses:

- The address is a common e-mail address in which ***** and **?** characters can be used as wild cards, the ***** substitutes an undefined number of characters whilst the **?** only substitutes a single character. The **@** sign can't be substituted!
- If the address begins with **@**, it is applied to all users on the given host.

Unprotected recipients

The program does not scan mail sent to the given addresses.

Unfiltered senders

The filter settings are not applied to messages incoming from the given addresses.

Unfiltered recipients

The filter settings are not applied to messages outgoing to the given addresses.

File filter patterns

Attachments, which match the given file name patterns are removed from messages without scanning (for example: ***.com**, ***.exe**, ***.doc**).

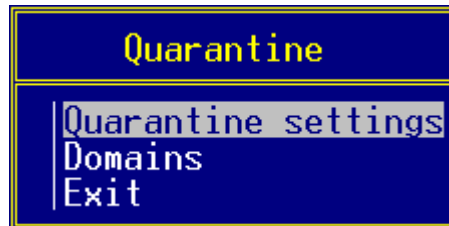


File filter exceptions

That files can be given here to which filter patterns should not be applied (for example: command.com).

Quarantine

You can view the contents of the quarantine folder in this menu and customize the display of the quarantine items with the available options.



Quarantine

Quarantine settings

The following options can be used to customize the list:

- View
Quarantined mails will be displayed in the list according to the selected option:
Sender + subject
Recipient + subject
- Sort by
E-mails will be sorted in the list following these options:
Date
Sender/Recipient
Subject
- Sort order
E-mails will be sorted in the list following the option selected above, in one of the following orders:
Ascending
Descending

Domains

You can select a protection area (domain here) to display a list of items found in its spam or virus quarantine.

The quarantined objects will be displayed in the list (which can take some seconds depending on the length of the list). By pressing **Enter**, details about a specific item in the quarantine can be displayed and the following actions can be performed on the item by pressing **Enter** again:

- *Delete*
- *Forward to admin*
- *Forward to recipient*
- *Skip*

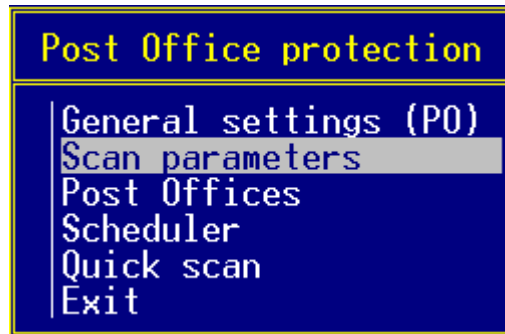


Vexira Antivirus for GroupWise

After selecting an action, the details window can be closed by pressing **ESC**. The action will be performed on the selected item after this. Except for the *Skip* option, every action will delete the item from the quarantine.



Post Office protection



Post Office protection

The Post Office protection module allows off-line virus scanning of Post offices storing users' mailbox. The system scans for viruses according to the settings at the scheduled dates. The off-line virus scan provides more security for the mail-database preventing virus spreading and blocking infected mails that have managed to get in the system.

Important!
If the folder to be scanned contains more than 5000 items, it can't be opened to check because of the limit of IMAP protocol!

General settings (PO)

General settings of Post Office module:

Mail to Admin

Entering this option you will get a list including system events. If the event(s) found in the list occurs, the program will send a message to the system administrator.

Handling the list:

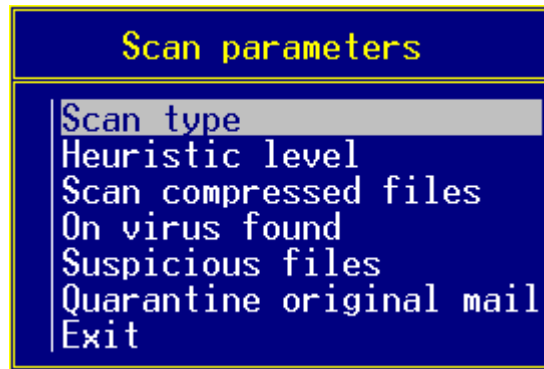
The list is empty by default, use the **Insert** key to add events. If you press the key, you will get a new list including system events. Use the **Enter** key to select one of them then you will get back to the main list extended with the selected event. Repeat this if you want to set several events to be reported. Use the **Delete** key to delete events from the list.

Mail to user

User notification when the selected event(s) occurs. You have to fill the same list as described above.



Scan parameters



Scan settings

Scan type

These values are the same as you can select in the [Scan type](#) options of Internet Agent section.

Heuristic level

These values are the same as you can select in the [Heuristic level](#) options of Internet Agent section.

Scan compressed files

If you select this option, the scanner will scan also the compressed files.

On virus found

Select action for virus incidents. On failed kill attempt, the program changes the file to a text file named: [<filename>.txt](#). You can find more information in this text file about action taken.

Suspicious files

Select action for suspicious files.

Quarantine original mail

If the mail is modified during the scan and you have activated this function, the program will move the original instance of the mail to the quarantine. Set the quarantine folder in the [Quarantine IMAP folder](#) option.

Post Offices

In this menu you can add Post Offices to be protected by Vexira Antivirus for GroupWise. Entering the menu a list window appears including the Post Offices selected by you. This list is empty by default which is announced by a warning message.

To add new Post Offices to the list, use the **Insert** key. After entering a name for the Post Office, you need to specify additional data to complete Post Office definition in the appearing window. You can modify these data at any time you want later selecting the name of the Post Office with the **Enter** key. If you want to delete an existed Post Office from the list, select it and use the **Delete** key.



Post Office settings

Post Office name

ID of Post Office in the antivirus system. You can refer to the specified Post Office by this name.

Host name

Server computer's name or IP address the Post Office is found on.

Port

Enter the port number for the Post Office.

Scan only new mails

If you launch a scan and this option is active, the scanner will only scan the recently received mails.

Scan all users

All users of the current Post Office will be scanned if this function is active.

User exceptions

If *Scan all users* option is active, you can define user(s) who will be skipped from the scanning.

Users to scan

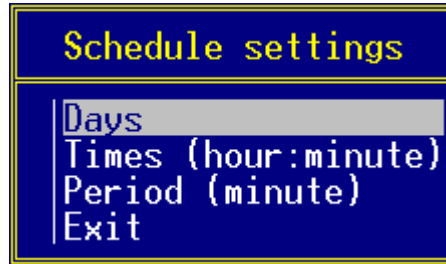
Set users to scan in the current Post Office. There is no reason for setting this option if *Scan all users* option is active.

Quarantine IMAP folder

Set the quarantine folder for storing quarantined objects. Name this folder as `<user>/<folder>` (e.g.: `admin/quar`) which is a common quarantine folder. It is possible to create quarantine folder for each user, use the following form: `%CURRENT_USER%/<folder>`

Scheduler

Schedule the scanning of Post Offices in this menu. Entering the menu, first you have to select a Post Office then specify the schedule settings for the selected one.



Schedule settings

You can define period or exact time to schedule virus scanning. The following settings are available to customize automatic scanning for the selected Post Office:

Days

Define a day or days on which you want to launch virus scan automatically. You can select days from a list the same way as it is described in the [General settings \(PO\)](#) section. If you don't set time or period for the day(s) the scanner will not be run.

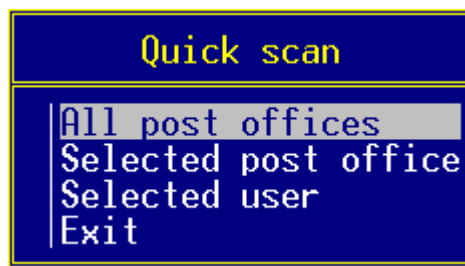
Times (hour:minute)

Set exact time(s) for the selected days (or for every day if the *Days* list is left empty) when you want the virus scan to be launched. A list includes the times, use this list the same way as it is described in the [General settings \(PO\)](#) section. You have to specify the time in the following form: **hh:mm** (hh – hour, mm-minute).

Period (minute)

In this setting you can enter a time period in minute. Always when this period expires, the program will start the virus scan.

Quick scan



Quick scan

All post offices

Scans all the Post Offices protected by the anti-virus system (listed in the *Post Offices* menu). It will only scan the allowed users of Post Offices.

Selected post office

You can select one from the protected Post Offices to scan. It will only scan the allowed users of Post Offices.

Selected user

First you have to select a Post Office then select the user you want to scan.



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, 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



Vexira Antivirus for GroupWise

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.

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



Vexira Antivirus for GroupWise

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
E-mail sales@centralcommand.com
support@centralcommand.com