

User Guide

Vexira Antivirus for Windows Servers





TABLE OF CONTENTS

VEXIRA ANTIVIRUS FOR WINDOWS SERVERS	4
Minimal System Requirements	4
Installation	5
Normal Installation	5
Installation with Parameters.....	6
If the Installation Has Not Started... ..	7
Removal, Modification, Reparation	7
Starting from the Start Menu	7
System Tray	7
Pop-Up Windows	8
MMC Console Information	10
Starting the Console	10
Options, Setting Parameters	11
ANTIVIRUS SETTINGS	14
Quarantine	15
Quarantine Entries.....	15
Settings Panel	16
Virus Scanner	17
Adding New Task.....	17
Scanner Settings	18
Heuristics	18
Scan Areas	18
Files To Be Scanned	19
Scan Areas	19
Interactivity.....	19
Resident Protection (Server Guard)	20
Settings Panel	20
Virus Scan Areas.....	20
OPERATIONAL SETTINGS	23
General Settings	23
Security Context for Network Connections	23
General Settings.....	23
SMTP Clients.....	24
Tray Icon Settings.....	24
Additional Scan Settings.....	24
Log Settings.....	25
Log	26
Filter.....	27
Central Alert.....	27
Task Manager	30
Tasks and Task Settings	30
Registration	33
Updater	34
Source Settings	34
Tasks	35
ADDITIONAL INFORMATION	37
Virus Scanning Methods	37
Heuristics	37
Actions	37



Vexira Antivirus for Windows Servers

Testing the Virus Scan Engine	38
Windows, Messages	39
Virus Scan Window.....	39
Message Window	40
END USER SOFTWARE LICENSE AGREEMENT	43
CONTACT	45



VEXIRA ANTIVIRUS FOR WINDOWS SERVERS

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

Vexira Antivirus for Windows Servers provides resident protection for data, systems, and, therefore, for the everyday work, optimized to the increased data traffic of servers. The task oriented operation, the flexible settings, the wizard style and advanced user interfaces provide an easy way of use with the highest level of security in the most flexible way.

Main features:

- Effective resident protection for servers against viruses and other harmful codes
- Separate protection areas to handle storage disks or their smaller areas of servers separately
- Manual, automatic, and scheduled virus scans
- Incremental virus database update
- Easy to use, wizard style user interface
- Advanced interface for advanced settings
- Task oriented operation, modular updates
- Intelligent quarantine for infected files
- Supports Windows Security Center

Minimal System Requirements

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

Processor	400 MHz (x86/x64)
Supported operating system - memory	Windows 2000 Server - 256 MB Windows Server 2003/2008 - 512 MB <i>It is recommended to install the latest Service Pack and use at least 1024 MB memory depending on other applications running on the system.</i>
Free hard disk space	200 MB
Browser	Internet Explorer 6
Other	If you need more information, check the readme.txt file – it is in the installation kit.



Installation

Make sure that your computer is virus free before installing the software. The anti-virus software can only operate properly if it was installed on a virus free computer. Perform a virus scan on the computer with the help on Vexira Antivirus Scanner's latest version, which can scan the whole system for viruses in a fast and easy way.

Note!

If an anti-virus software is already installed on the computer, it must be removed before installing Vexira Antivirus. If an older version of Vexira Antivirus is installed on the computer, it must be removed as well.

The product can be installed from a self-extracting archive ([winsrv.exe](#)). After executing the file, the installation package is decompressed and installation is started.

Normal Installation

Follow the installation instructions that guide you through the installation process.

Welcome Panel

You can move forward from the welcome screen by clicking on the **|Next >|** button. The end user license agreement is displayed in the next window. Generally, you can step back with the **|< Back|** button (available on the bottom of every window) and quit the installation process with the **|Cancel|** or **|Exit|** buttons.

Displaying and Accepting the License Agreement

Read the agreement and select the **|Yes|** button, if you accept the term and conditions and would like to continue the installation process. If you do not accept the terms and conditions of the above agreement, choose the **|No|** button to terminate the installation process and exit from the wizard.

Information About the Product

Continue by clicking on the **|Next >|** button and specifying the installation path.

Choosing the Installation Path

By default, the product is installed on the system partition in the `Program files\Vexira Antivirus\` directory, but it can be changed by clicking on the **|Browse...|** button, where you can browse through the drives and directories available on your computer and choose the needed path for installation. After selecting the installation path, you can move forward by clicking on the **|Next >|** button.

Choosing the Installation Mode

The most suitable installation mode in most cases is *Typical*, and if there is no reason to choose one of the other two options, this one must be selected. The *Compact* installation mode only installs basic components. The product is operational, but some of the extra functions may not be accessible if this option is selected. The following panel is: [Specifying registration information](#) window.

The *Custom* installation mode is only advised for experienced users. The user can specify the components to be installed if this option is selected.



After selecting install modes, you can continue the installation by clicking on the **|Next >|** button.

Choosing Components (Customization)

Information is displayed about the selected module on the right side of the window under *Description* by clicking on one of the components.

The *MS Office* and *MS Outlook* protection components can only be selected (installed) if the product to be protected by these components is installed on the computer. After selecting the needed components, you can move forward by clicking on the **|Next >|** button. The display of the following panels depends on the selected components.

Specifying the Update Source (Customization)

Select the suitable update source types for your system and network. You can set additional proxy settings in case selecting the *HTTP* source.

Specifying Registration Information

The software can be registered during the installation process by typing the username and the license key in the appropriate fields. The software can be installed without registration by selecting the *Register later* option and by clicking on the **|Next >|** button.

Security Data

Enter user name and password to specify a Windows account: the updater tasks are run with the permission that belongs to the specified account by default. This setting can be modified later in the *General settings* option.

Additional Data

You can enable/disable displaying the icon of the product on the Desktop or select the language of the program.

Start Copying

Finally, you can check the settings and components to be used during the installation of the product. Copying the files is started by clicking on the **|Next >|** button.

Successful Installation

If the installation was finished without any problems, you can exit the installer after all files are copied by clicking on the **|Finish|** button, the software is installed successfully. You may need to restart your computer after installation. This is indicated by the software at the end of the installation.

Installation with Parameters

By specifying parameters after the installation file, other installation modes can be enabled that are not



Vexira Antivirus for Windows Servers

available during regular installation. You can find information about these parameters and installation modes in the [readme.txt](#) file, which can be found in the *Readme* folder of the installed product.

If the Installation Has Not Started...

Check that your computer fits all minimal system requirements. Check if your system has all the needed system and program components. Without these, installation cannot be performed and an error message informs you about the needed system component that is required in your computer before installing the antivirus software. You can find detailed information about this topic in the [readme.txt](#) file, which can be found in the *Readme* folder of the installed product.

The product can also not be installed if another antivirus product can be found on the computer. In this case, you have to remove the existing av application before installing the Vexira Antivirus.

Removal, Modification, Reparation

If you want to remove Vexira Antivirus from you computer or modify the installed components or reinstall installed components, perform the following:

1. Click on the *Add/remove program* icon on the *Control panel*.
2. Search for the product to be removed from the list and select it.
3. Click on the **Modify/remove** button.

You can select the needed operation in the window that is displayed:

- *Modify*
If you select this option, a component list appears after clicking on the **Next >** button. By selecting or deselecting components in the list, you can add new components or remove installed ones. The needed operations (installation/removal) are performed after clicking on the next button.
- *Repair*
Reinstalls installed components.
- *Remove*
Uninstalls all installed components from the computer.

Starting from the Start Menu

The Vexira Antivirus for Windows Servers product is available under Start / Programs / Vexira Antivirus Server after installation. All the shortcuts related to the product are placed here, the software can be started here and product-related documentation can also be opened from this menu.

System Tray

The Vexira Antivirus product can be accessed from the system tray. A Vexira icon is displayed in the tray after installation, indicating that the Vexira Antivirus product is present in the system.



Vexira Icon on the System Tray



Vexira Antivirus for Windows Servers

The little shield on the icon indicates the status of the *Guard (Resident protection)*, which provides continuous virus protection for the system (if this function is not installed, the shield is not displayed). The color of the shield indicates the status of the resident protection:

- *Green*
Guard is active, the computer is protected against viruses (if the product is registered or is in a trial period).
- *Gray*
Guard is not working, there is no resident virus protection.

The most important functions of the program can be accessed from the system tray easily, the most commonly used components and tasks can be started from here. By right-clicking on the Vexira icon (1), a local menu appears where the needed function can be selected. If a menu has a sub-menu, it is indicated with a little arrow in front of the name of the menu item (2).



Vexira Icon on the System Tray – Local Menu

The following items are always listed in the menu:

- *Registration*
This menu item contains all functions related to purchasing or registering the software. Detailed information about this topic can be found under the [Registration](#) section.
- *Support*
This menu item contains three items, which are the following:
 - Help*
The documentation files of the installed products can be accessed here.
 - Contact us*
With the help of this function, you can send an e-mail to Vexira Antivirus about the product if the *Mailer* component is installed (detailed description under the [SMTP Client](#) subsection).
 - Information*
This menu item opens Vexira's home page.

After registering the software or during the trial period, the most important installed components and the available scanning or update tasks can be accessed from the menu. The Vexira Antivirus Console can be started by double-clicking on the menu.

Pop-Up Windows

Through pop-up windows displayed above the System Tray, users get quick and immediate information about the status of the antivirus system and events occurred during the operation of the software.



Pop-up Window

The title highlighted with bold characters shows the „sender” of the displayed message. The message informs users about the operation or message of this module. In certain cases, there is a button placed between the message lines. By clicking on it, users can navigate to the offered function directly (for example, if the message warns the user about the virus database update, the action can be started immediately by clicking on the **Update** button).

The pop-up window closes after a short period of time, but users can also do it by clicking on the **X** button placed in the top-right corner of the pop-up window.



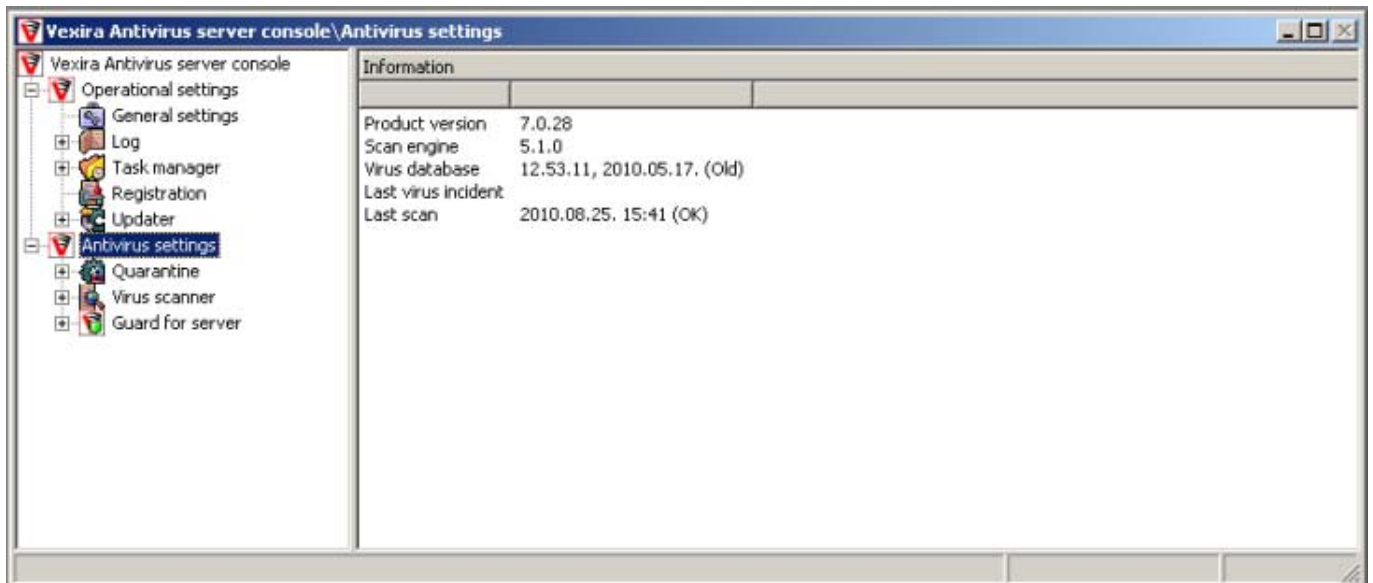
MMC Console Information

The advantage of Microsoft Management Console (MMC) is that experienced users can perform tasks in the hierarchical system in a matter of minutes and modifying settings and configuration is much easier.

Starting the Console

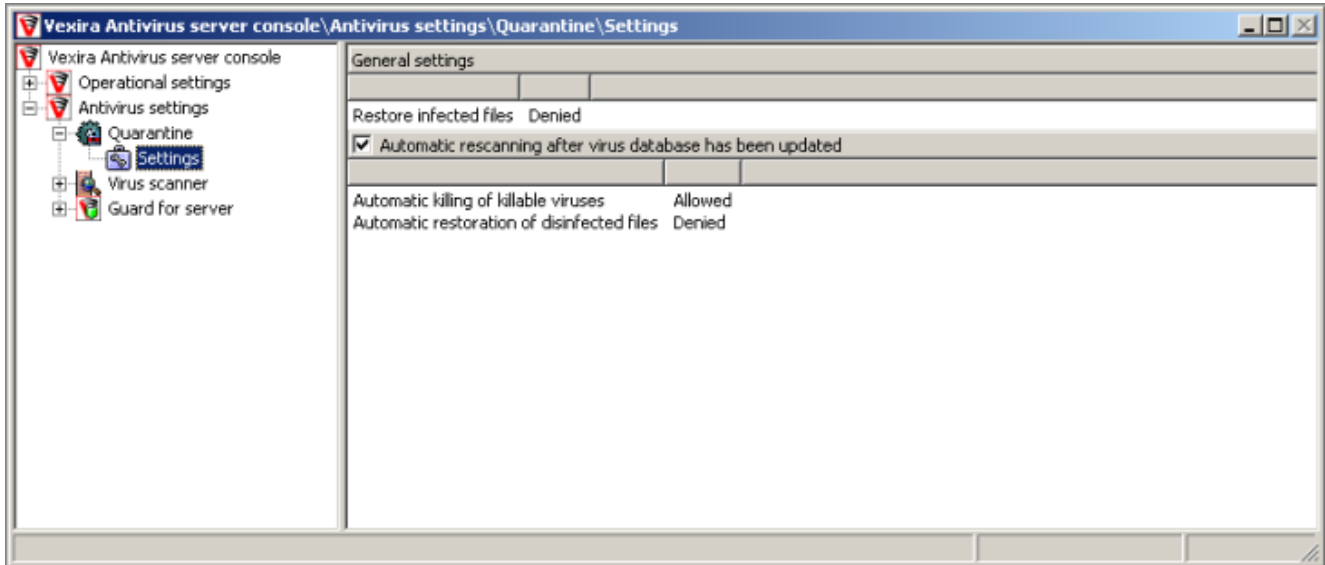
To start the MMC user interface, start the 'Vexira Antivirus Server Console' program from the *Start menu* (Start menu / Programs / Vexira Antivirus Server / Vexira Antivirus MMC Console (Server)), and the MMC console elements are displayed in a parent window (Vexira Antivirus Server Console). This window contains the menu and the toolbar with commands to open or create additional consoles and to save them. When launching the product, the parent window already contains the Vexira Antivirus Server console window where you can access the product settings.

General modules of the product are located in the *Operational settings* node. The modules for the customization of the antivirus protection are available under the *Antivirus settings* node.



An Installed Product and Its Module Versions

To access module settings, click on the plus (+) sign in front of the name of the module, and the settings groups are displayed under the module.



Module Settings

By clicking on the settings groups under the module, the module settings are displayed in the details window. You can modify these by double-clicking on the selected option or by right-clicking on the option and choosing Modify from the local menu. Other functions in the local menu are detailed in the description of each module.

Important!

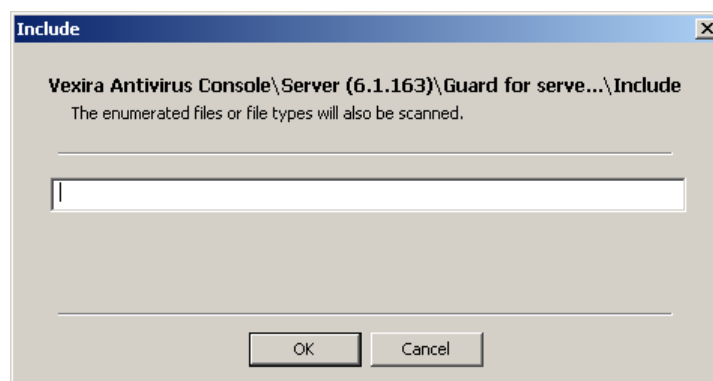
Some of the settings or options above general options can only be accessed in the local menus.

Options, Setting Parameters

You can access the settings of each module by specifying the needed options in the details window. The options can be modified in two ways:

- Double-clicking on the name of the setting
- Right-clicking on the name of the setting and selecting the Modify option

The values of the options can be set in the input dialogs. The simplest setting is when the user must specify the value in an input field.



Simple Input Dialog

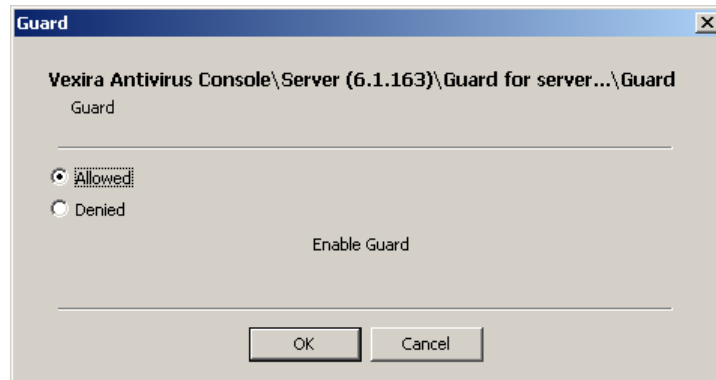
In some cases, the needed value can be specified by clicking on the **Browse ...** button. After having specified or selected the needed value, the window can be closed with the **OK** button and the value of



Vexira Antivirus for Windows Servers

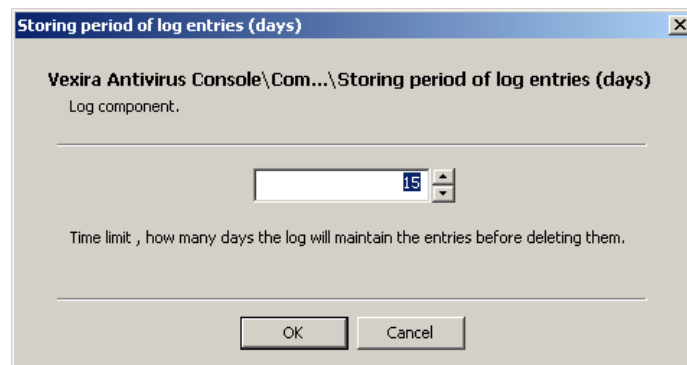
the setting is the parameter specified in the input field. If you do not want to specify a value or you do not want to modify the value, use the **Cancel** button. This applies to all dialog windows.

In some cases, the option can only be enabled or disabled. In this case, the program offers these two options in a dialog window, and you can select the one needed.



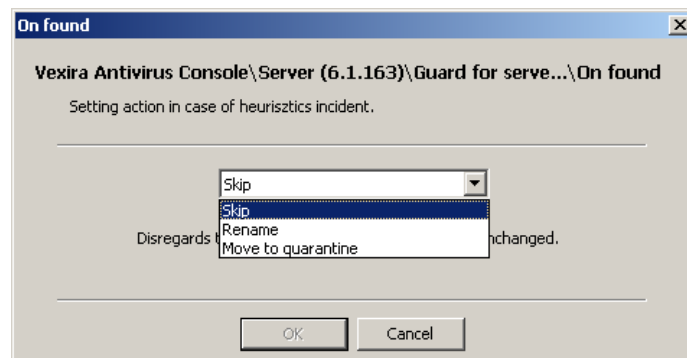
Enable/Disable Option

The values can be set with arrows to increase or decrease the value of the parameter. In this case, you can only specify values between the allowed values. The needed value can be set by typing it as well.



Parameter Settings Window

In the following window, the value of the settings can only be a pre-defined parameter; in this case, these can be selected from a drop-down list:

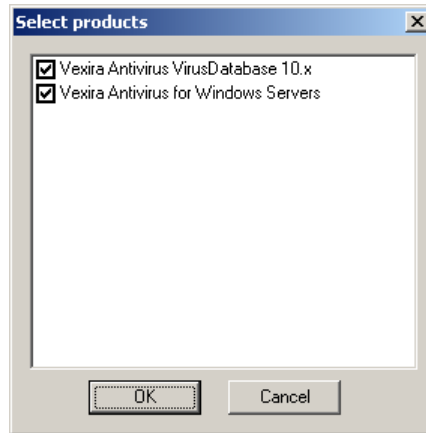


Selecting a Value from a Drop-down List



Vexira Antivirus for Windows Servers

The settings group may only be modified in a comprehensive dialog window (like selecting products for an update task). In this case, the comprehensive window is displayed if any of the options is modified, and you can specify the value of all the settings in the group in this window.



Comprehensive Settings Window



ANTIVIRUS SETTINGS

The modules of the *Antivirus settings* are the following:

- [Quarantine](#)
- [Virus scanner](#)
- [Shield for server](#) (resident protection)

If you click on *Antivirus settings*, information about the product appears in the window on the right side:

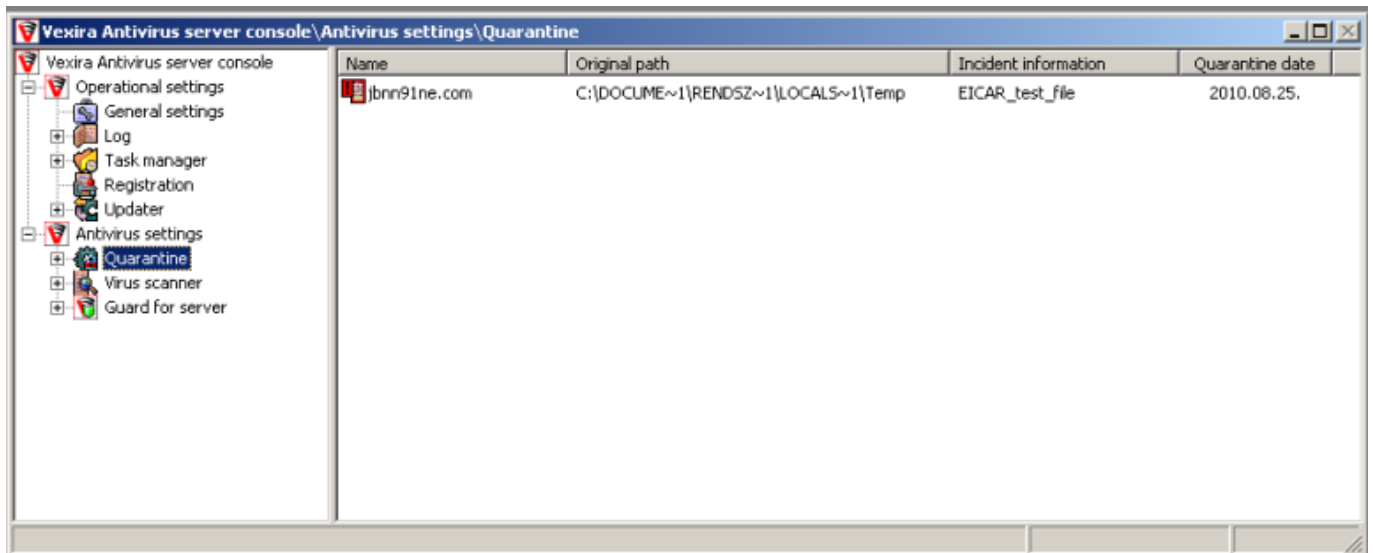
- *Product version*
The version number of the installed product.
- *Scan engine*
The version number of the virus scan engine.
- *Virus database*
It displays the version number of the virus database and shows if it is up-to-date or needs updating (older than two days) in brackets.
- *Last virus incident*
The date of the last malware incident.
- *Last scan*
It displays the date and result (in brackets) of the last scan of the machine.
For the details of the virus scan, right-click on this setting and select the Details option. The log messages of the last scan is displayed.



Quarantine

The task of this component is to store and process non-killable viruses according to the settings.

By clicking on the Quarantine component, the items placed in it are displayed in the right-side details window. By clicking on the plus (+) sign in front of the component, you can display the icon of the panel containing the other settings and options of the Quarantine.



Quarantine

Quarantine Entries

The following information is displayed in the quarantine window:

- *Name*
The original name of the quarantined file
- *Original path*
The file's original path (before it was moved to the quarantine)
- *Incident information*
It displays the detected malware and its path.
- *Quarantine date*

Several actions can be performed on files stored in the quarantine, these are available in the local menu. To access the local menu, right-click on the needed entry.

- *Rescan*
The software scans the selected file(s) again and kills all viruses if possible.
- *Restore*
The program restores the file to its original path and status if the *Restore infected files* function is enabled on the *Settings* panel of the component (only if the file is infected with a virus), the original path exists, and there is no file with the same name on the path. If there is a file with the same name on the original path or the path does not exist, the quarantine restores the file to the temporary folder of the software.
- *Save as...*
It saves the file with the specified name. The program encodes the file, so that the virus is inactive and the file can be sent for virus analysis.



- *Send...*
It sends the selected file(s) to Vexira Antivirus for analysis. Proper SMTP settings are required for sending a file and they can be specified on the [SMTP client](#) setting of the Operational settings/General settings panel. You can modify these data before sending by clicking on the [Mailer settings ...](#) button in the sending window.
- *Delete*
The program deletes the selected file(s) permanently.

Settings Panel

Other settings that affect the operation of the quarantine can be specified in this panel. You can enable the restore function of the quarantine with the help of the *Restore infected files* option. If it is enabled, infected files can be restored from the quarantine.

If the *Automatic rescanning after virus database has been updated* option is enabled, the program rescans all files in the quarantine after a virus database update and kills all viruses in them if possible.

The following options can only be modified if automatic rescanning is enabled:

- *Automatic killing of killable viruses*
If this option is enabled, the program kills all viruses in the quarantined files after a virus database update if possible.
- *Automatic restoration of disinfected files*
If this option is enabled, the program restores all files that were disinfected automatically after a virus database update.

Important!

It is not required to specify a quarantine directory, the program uses the [Quarantine](#) folder of the installation directory automatically.



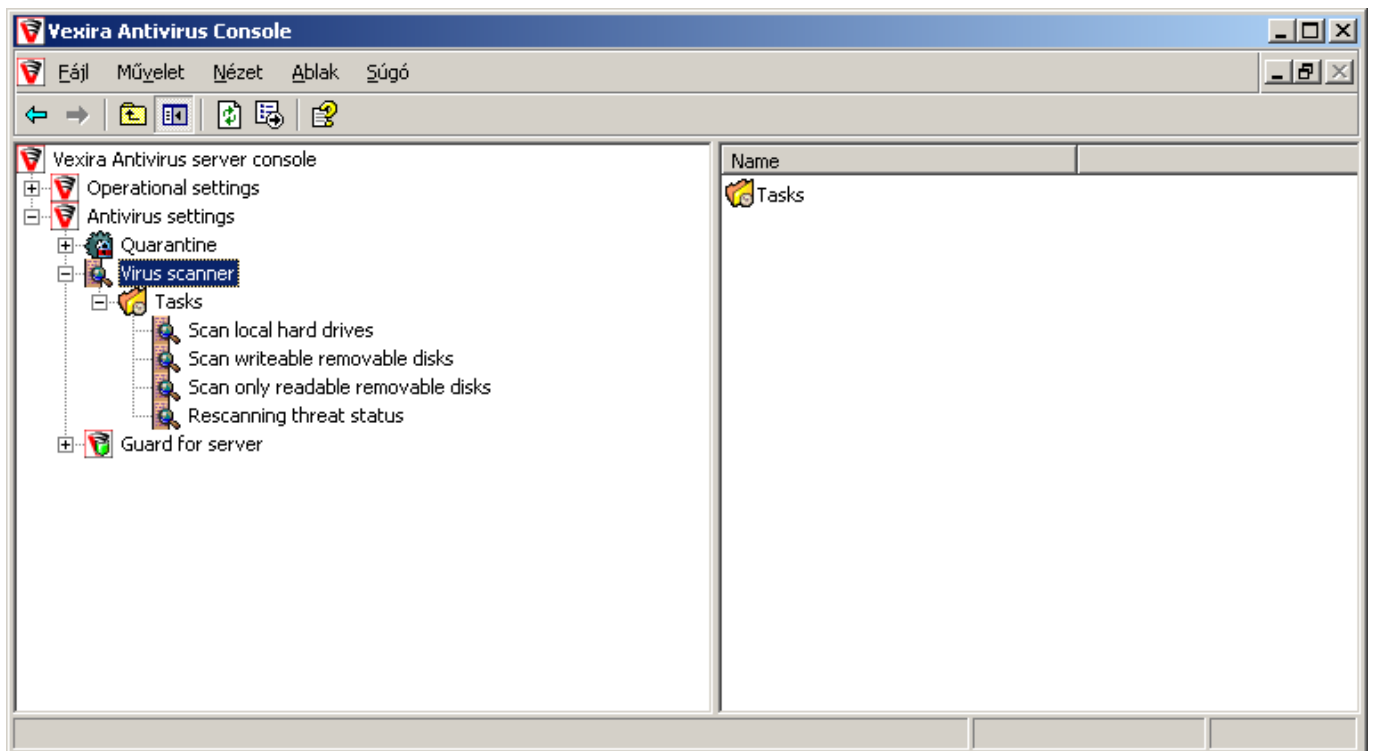
Virus Scanner

Virus scanning tasks can be added and modified, and virus scans can be initiated in this component. Virus scanning is based on tasks: a virus scan can be started with a few clicks or can be scheduled for a specific date or a trigger event with the pre-defined parameters.

You can access the *Tasks* folder in the following two ways:

- After clicking on the Virus scanner component, the *Tasks* folder is displayed in the right-side details window. By double-clicking on it, you can check the existing virus scanning tasks.
- Click on the plus (+) sign in front of the component in the list on the left panel. In this case, the *Tasks* folder is displayed in the left-side tree as well and tasks can be displayed by clicking on it.

The icon in front of the name of the task in the details window indicates the status of the task (started, stopped, or paused).



Virus Scanner

Tasks can be modified, deleted, or scheduled in the local menu that is described in the [Tasks and Task Settings](#) section.

Adding New Task

A new task can be added in the local menu. Right-click on the *Tasks* folder in the left-side list or anywhere in the details window and choose the *Add* option.

When adding a new task, first the name of the task must be specified. After specifying a name, the task is created with default settings. To modify these:

- Select the new name of the task from the left-side task list.



- Double-click on the name of the task in the right side details window.

Scanner Settings

The *Scanning method* can be specified on the following levels:

- [Fast/Extensive/Full](#)

You can specify the actions to be performed (automatic mode) or to be suggested (interactive mode) when a virus is found on the Virus found settings panel. The selected primary action can be set in the Virus found option. If this cannot be performed (for example, the virus cannot be killed), the secondary action (set at the *In case of unsuccessful disinfection* option) is performed or suggested. When a virus is found, all actions can be performed on the file except for Kill, so it is not required to set a secondary action if the set value for the primary action is other than Kill. You can set an action for heuristic detections.

The available actions *On virus found* can be one of the following:

- [Kill/Move to Quarantine/Skip/Delete/Rename](#)

Available secondary actions are one of the following:

- [Move to Quarantine/Skip/Delete/Rename](#)

Heuristics

Heuristics *Sensitivity* settings can be one of the following:

- [Off/Medium/High](#)

Available actions in case of heuristics found are one of the following:

- [Move to Quarantine/Skip/Rename](#)

Scan Areas

You can specify the areas to be scanned here. The following areas can be selected (*Enabled*) or deselected (*Disabled*):

- *Memory*
Scans the memory of the computer.
- *Master boot record*
Scans the first boot record of the computer.
- *Boot sector*
Scans the current boot sector.
- *Compressed files*
Scans all files compressed with known compression methods.
- *Folders*
Scans the selected folders.
- *Selected files*
Scans the selected files.



Files To Be Scanned

If the *Scan all files option is enabled*, all file types (all extensions) are scanned. If this option is disabled, you can specify the file types to be scanned. These can be set based on pre-defined groups. If the *Allowed* value is selected, the specified file type is scanned.

- Jet database engine files
- Sheet files
- Document files
- Power Point files
- Program files
- Script files

You can specify file types to be scanned or not individually. To be able to do this, the *Included file types* or the *Excluded file types* option must be selected. In this case, the files to be scanned or not must be specified in the *Include* or *Exclude* fields separated with a semicolon (;) (for example, *.rxx; *.qqq). When specifying file types, joker characters can be used (for example, *.qwe, *.?ab).

Scan Areas

The drives and network shares or their individual directories to be scanned can be set here. Right-click on this option to be able to add, modify, and delete scan areas.

You can enter or browse a new scan area in the browser window. More scan areas can also be added.

When selecting the *Recursive* checkbox, the selected folder with all its subfolders and files are scanned.

If you would like to scan all the available drives on the client, enter the #ALLHARDDRIVES keyword for the path.

Interactivity

If the *Interactive communication* option is enabled, the program prompts the user for further instructions in case of every incident and offers the set actions as default. If the option is disabled, the set actions are performed automatically on the infected file.

If the *Status window* option is enabled, you can monitor the scanning process in the [virus scanning process status window](#).

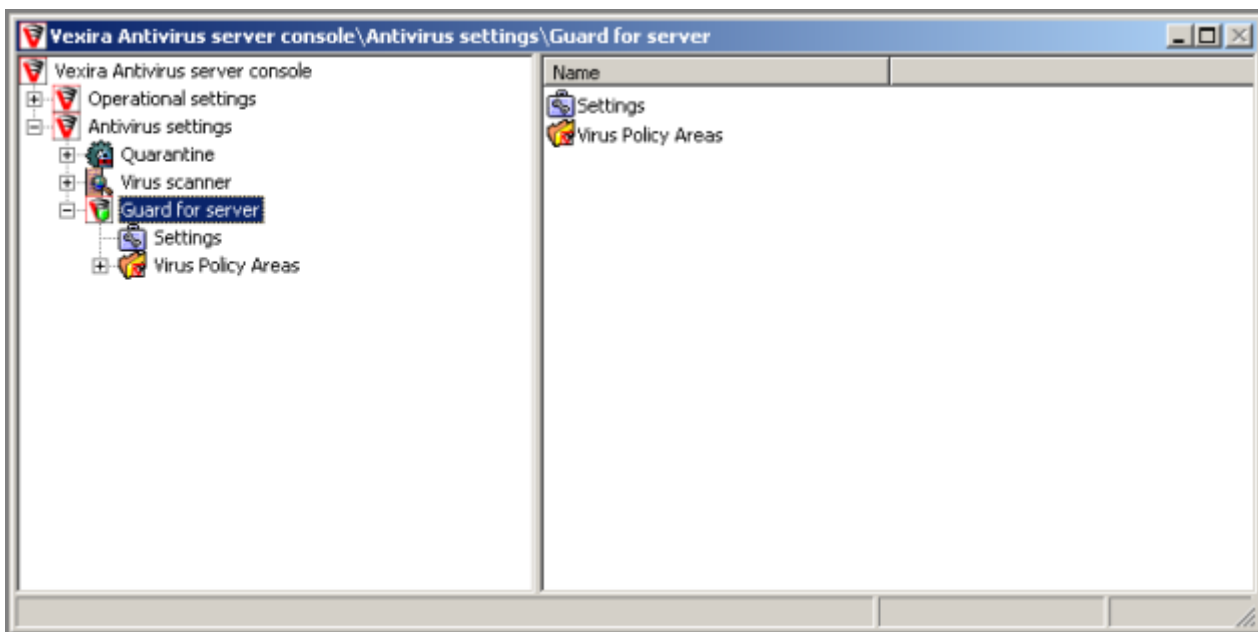


Resident Protection (Server Guard)

This component provides resident protection against viruses. Its main task is to search for viruses and disinfect them by working in the background. The resident protection scans files when they are accessed (for example, reading and writing).

If the resident protection is enabled, the attached removable devices (such as USB stick) can also be scanned quickly. When you are plugging a new device, a pop-up window will be displayed above the tray on which you can click to start scanning. If you don't click it, the window will disappear automatically after a while.

After clicking on the Server Guard component the icon of the *Settings* panel and the *Scan areas* folder are displayed in the right side details window. If you double-click on these, you can view their contents. You can display these two options by clicking on the plus (+) sign in front of the component in the left side list. In this case, the panel's icon and the folder are displayed in the tree.



Server Guard

Settings Panel

The Server Guard can be switched on or off in the *Resident protection* option (*Enabled/Disabled*).

You are notified about virus incidents if the *Display warning* option is enabled. If it is disabled, the program performs the set actions, but the user is not informed about the incident; it is only stored in the log.

Note!

Messages created by the network only appear if Windows Messenger Service is active.

Virus Scan Areas

One of the important functions of the server resident protection that separate virus policy areas (VPAs) can be created with different virus scanning settings. For example, two different directories on the



computer can be protected with different settings against viruses. For this, two different virus scan areas must be added with the needed individual settings.

The protection areas can be found in the *Virus policy areas* folder in the following two ways:

- Click on the folder, so that existing protection areas are displayed in the details window on the right.
- Click on the plus (+) sign in front of the folder, the same list appears in left side tree structure.

By default, only the *Default VPA* scan area is added to the system and it cannot be removed, but its settings can be modified.

To view the settings of a scan area, click on its name in the left side tree structure once, or in the details windows twice. The settings of the scan area are displayed in the right side details window.

New scan areas can be added by using the local menu. Right-click on one of the following:

- The *Virus policy areas* folder on the left side
- Any of the set protection settings
- Anywhere in details window

Select *New*.

When adding a new scan area, specify its name first. The required area is created with default settings.

To modify the settings of a scan area, select the name of the area in the left side list or double-click on the name in the right side details window.

To delete a scan area, click on its name and select *Delete* from the local menu.

Virus Scan Areas Settings

General Settings

You can enable or disable the selected protection area in the *Resident protection* option. If it is disabled, the virus protection options are not used and the path specified in the *VPA path* field are not protected.

You can specify the path or drive to be protected in the *VPA path* field. The protection is recursive, so the selected directory and all of its sub-directories and all files in them are protected according to the settings.

File Access Settings

You can specify whether the following files can be accessed in the system or not:

- *Access to infected files*
Disabled: Local or remote users cannot access files marked as infected by the system.
- *Access to suspicious files*
Disabled: Files found suspicious during the heuristic analysis cannot be accessed.
- *Access in case of scanning error*
Disabled: If there is an error during scanning (it cannot be determined whether the file is clean or not), the resident protection denies access to the file.



Scan Settings

Scan settings are the same as the ones described in the [Scan settings](#) section.

Heuristics

The heuristics levels and the performed actions are the same as detailed in the [Heuristics](#) section of the Virus scanner component.

Protection of File Groups

Files or groups of files can be specified inside a VPA path (in case of non-server protection: globally), so that they have special limitations or exceptions. When specifying file groups, joker characters can be used ('*', '?'), so that file groups can be added flexibly. To form file groups, file masks to be included or excluded must be typed in the field separated by a semicolon (;).

The following are types of protection that can be activated by selecting:

- *Delete protection of file group*
You can specify files or file groups in the *Include* option that cannot be deleted, because the resident protection prevents it.
- *Write protection of file group*
You can specify files or file groups in the *Include* option that cannot be written, because the resident protection prevents it.
- *Rename protection of file groups*
You can specify files or file groups in the *Include* option that cannot be renamed, because the resident protection prevents it.

Should you wish to specify more than one entry for any of the above options, separate them with semicolons (;).

Files or file types specified in the *Exclude* option are not excluded from the file group protection.

For example: if you want to prevent writing of **.exe** files beginning with **va** and **ve** characters, but you do not want to protect **.exe** files beginning with the **val** characters, set the following values in the *Write protection of file group* option:

- Include: **va*.exe; ve*.exe**
- Exclude: **val*.exe**

Important!

Remember that if an application tries to delete, write, or rename the protected file, it may cause several log records showing the actions. It occurs, because different file managers perform the requested action on the file repeatedly trying to delete, write, or rename it. Each attempt is registered in the log.

Scanning of File Types

The settings of file types which are selected for scanning are the same as described in the [Files To Be Scanned](#) section of the Virus scanner component.



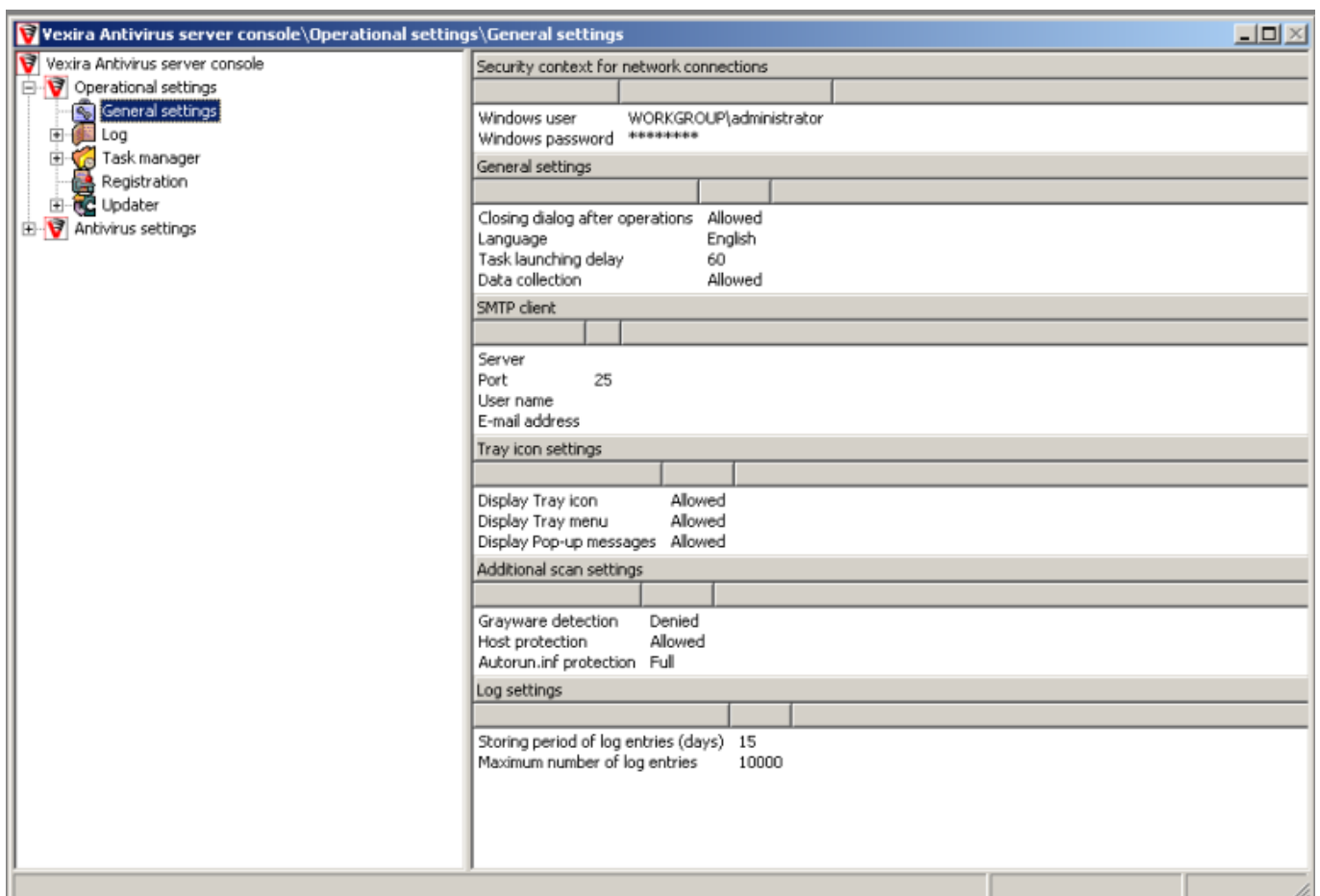
OPERATIONAL SETTINGS

The modules which are grouped under the *Operational settings* node provide general functions for the current product.

General Settings

Security Context for Network Connections

Enter the username and password to specify a Windows account: the updater tasks are run with the permission that belongs to the specified account by default. The account must be specified in the following format: NETWORK\User (for example, WORKGROUP\Admin).



General Settings

General Settings

If the *Close dialog after operations* option is enabled, the dialog window (if there is one) is closed automatically after an operation. If it is disabled, the program waits for the user to close the window.

You can change the language of the product by selecting a new language from the available values of the *Language* setting. After selecting a new language, restart the product to apply the new setting to it. For changing the language in the tray menu as well, restart the computer.



Task launching delay: If starting a task is triggered by an event, it may be needed to delay task launching, so that the task can be performed. A task can be scheduled to start at system startup, for example. In this case, it may be needed to delay it for some time after the login process, so that initialization processes can be performed and applications can be loaded. The delay can be set in seconds.

Data collection: With the help of this option, the software can send reports about virus incidents to Central Command to further improve antivirus protection. Information only about the installed product and the detected malware incidents, but no personal data are sent.

SMTP Clients

It is possible to send a direct message to Vexira Antivirus from the program if you have a question or a problem. Proper SMTP settings must be specified for this with the following values set:

- *SMTP server*
Name of the server delivering the e-mails, usually this name is given by the Internet Service Provider (ISP) or it is the name of the Exchange server (this information can be found in the mailer client settings /Outlook, Thunderbird, and so on/ or you can ask your system administrator or ISP).
- *Port number*
The port number of the mail server (25 by default).
- *Username*
This name is displayed in the mail you sent us as 'sender'. Tokens can also be used in this field:
%m% - computer name
%u% - username
- *E-mail address*
This is your e-mail address, to which the response is sent.

Tray Icon Settings

These options allow you to customize the operation of the System Tray menu and the Pop-up windows.

- *Display Tray icon*
Denied: The System Tray icon is not shown on the Tray.
- *Display Tray menu*
Denied: The local menu of the System Tray icon is not displayed even if right-clicking on the icon.
- *Display Pop-up messages*
Denied: The application does not warn the user with the help of pop-up windows (displayed right above the System Tray) about problems and events occurring during operation. This setting has no effect on displaying other information windows (virus alerts, warnings) of the product.

Additional Scan Settings

- *Grayware detection*
If this switch is enabled, the program can detect products in the grayware category and perform the action specified for the applications detected.
Grayware is software which may fall into different categories, depending on its use. Normally, if the user approved the installation and use of these applications, they cannot be considered malware. However, they may also be installed without the user's consent, and their functionalities may be abused for malicious activities. Such software may include ftp server programs and remote access applications. So the presence of such a program in itself is not necessarily



harmful. Whether it is harmful or not on a given machine is determined by the circumstances of its installation.

- *Hosts protection*

With the help of this option, the protection of the hosts file of a machine (that is in the System32\drivers\etc folder inside the Windows system folder) can be specified. It is enabled by default and works in case active resident protection.

- *Autorun.inf protection*

With the help of this option, you can set that the autorun.inf files (running software automatically) in CD/DVD and plug-in drives cannot be accessed in order to be protected.

In this option, you can select the protection level of the autorun.inf file from a dropdown menu. The following protection levels are:

- *Disabled*

The autorun.inf file is available with no restrictions, it is not protected.

- *Normal*

The autorun.inf file is only readable, but cannot be modified.

- *Full*

The autorun.inf file is read- and write-protected. This is the default value.

Autorun.inf protection is enabled in case of active resident protection.

Log Settings

You can modify the settings of storing log messages here. If you double-click, a pop-up window appears where you can choose the value from a drop-down list. The two elements of this setting are:

- *Storing period of log entries*

You can specify the number of days the system stores log messages here.

Default value: 30 days

- *Maximum number of log entries*

You can specify the maximum number of log messages to be stored by the system.

Default value: 100000



Log

Its main task is to store the messages generated by the various parts (modules) of the software and to forward these to the user if needed.

Physically, the log file is located in the *Bin* folder of the installation path. It is an SQLITE type database file called *local.db*.

The log entries are displayed in the right side details window by clicking on the component. By clicking on the plus (+) sign in front of the component, you can display the icon of the panel containing the other settings of the Log component.

Date	Message	User	Module
2010.08.26. 12:16:37	The "Rescanning threat status" task has finished.	SYSTEM	Task manager
2010.08.26. 12:16:37	Virus scan finished	SYSTEM	Virus scanner
2010.08.26. 12:16:37	Scan started - The virus database is old!	SYSTEM	Virus scanner
2010.08.26. 12:16:36	The "VDB Update" task has finished.	SYSTEM	Task manager
2010.08.26. 12:16:36	Failed to launch updater application for "Updater task: VDB Update".	SYSTEM	Updater
2010.08.26. 12:16:33	The virus database is old!	SYSTEM	Virus database
2010.08.26. 12:16:31	The virus database is old!	SYSTEM	Virus database
2010.08.26. 12:16:30	Quarantine rescan finished.	SYSTEM	Quarantine
2010.08.26. 12:16:27	The "VDB Update" task has started.	SYSTEM	Task manager
2010.08.26. 12:16:24	The "Rescanning threat status" task has started.	SYSTEM	Task manager
2010.08.26. 12:16:24	The virus database is old!	SYSTEM	Virus database
2010.08.25. 16:57:27	Virus scan finished	SYSTEM	Virus scanner
2010.08.25. 16:57:20	Scan problem - File not found	SYSTEM	Virus scanner
2010.08.25. 16:56:58	Scan started - The virus database is old!	SYSTEM	Virus scanner
2010.08.25. 16:55:05	The "Program Update" task has finished.	SYSTEM	Task manager
2010.08.25. 16:55:05	Failed to launch updater application for "Updater task: Program Update".	SYSTEM	Updater
2010.08.25. 16:55:04	The "Program Update" task has started.	SYSTEM	Task manager
2010.08.25. 16:55:02	The "VDB Update" task has finished.	SYSTEM	Task manager

Log

Default structure of the messages:

- **Date**
The date when the message was created.
- **Message**
The content of the message.
- **User**
The name of the user who started the application generating the message.
- **Module**
The name of the module creating the message.

The first icon indicates the message's type and the second, paper clip indicates if the message has a detailed description.

The program refreshes the list automatically if the new message is created or deleted. The refresh cannot modify the selected item provided it is not the one which has just been deleted.

A local menu appears by right-clicking on the items, in which the separate fields of the messages can be switched on or off and the following actions can be performed:

- Save as...



Saves the content of the message to the specified file.

- *Send...*
Sends the message and the log file to the support division of Central Command, Inc. You can finish sending the message in the *Mailer component* window.
- *Refresh*
Refreshes the list.
- *Delete*
Deletes ALL messages from the list.

If you double-click on a message, the details of the message are displayed and you can view its detailed description.

Filter

The filtering function is available in the Log elements of the product.

The filtering function can be selected by right-clicking on a given element. The *Filter settings* pop-up window appears with the options that you can filter:

- You can select the categories and the event types (for more information, refer to the [Central Alert](#) section).
- You can filter message content by entering text in the empty field beside the element to be filtered.
- From a drop-down list, you can select the modules to be filtered.
- And you can also select the period to be filtered by specifying the start and end date of the logs.

Depending on which element you are at in the GUI when opening the *Filter settings* window, some options may not be defined, so that you cannot select them.

Minimum one category and event type must be selected in order to start filtering.

When filtering for message content, however, you do *not* need to enter the search text between asterisks (*).

If you specify a period for filtering, the start date must be earlier than the end date, otherwise filtering cannot be used.

Central Alert

The task of the component is to send a warning after a new log entry belonging to the category and message type specified appears. This component creates and sends the warnings by using the log messages stored by the *Event log* component. The *Central alert* component requires correct e-mail settings to be able to operate.

Central Alert operation is based on rules (that is, notification settings can be specified in (several) rules). In order to manage rules, select the *Central alert* component in the left-hand tree, then use the local menu (by right-clicking) in the right-hand window. The options are *Add rule*, *Modify rule*, and *Clone rule* (cloning means to create a new rule from an existing one with identical settings).



When adding a new notification rule or modifying an existing one, the following settings of the Central alert appear in a pop-up window:

1. General settings window:

When creating a notification rule, the following must be specified:

- *Rule name*
A unique name to identify the rule.
- *Send detailed message*
You can choose if the system sends a detailed message or not.
- *Type of notification*
E-mail – the notification is sent to a specified e-mail address (Check the mail settings.)
Event logs – the notification is put into the Event logs.
Central database
- *E-mail address* (appears only when e-mail was selected)
The e-mail address Central Alert sends the messages to.

2. Filters settings window:

You can select the events which *Central Alert* sends a message about.
You can choose the event categories and types of the possible filtering settings.
The event categories and types are described below.

3. Flood settings window:

You can enable or disable the given rule. The other options are only available when it is set as enabled.
You can specify the period of frequency when to send the notification or the number of messages to be reached when sending the notification.
And you can also set that the system sends the central alert notification automatically when CMS is started.

There is a default rule in the *Central Alert* component that cannot be deleted, only modified.

The event categories are the following:

- *Malware incidents*
It contains messages about malware incidents on a client (every malware detected, suspicious files).
- *Quarantine events*
It contains messages about the quarantine in a client (for example, restoring, rechecking, saving the quarantine, and so on).
- *Management events*
It contains messages about installation on a CMS (for example, remote installation, allocating licenses, messages about the install copier, and so on).
- *Operational events*
It contains messages created during the operation of the antivirus software (for example, enabling/disabling modules, modifying settings, changing the status of the antivirus protection, and so on).
- *Scan events*
It contains messages about virus scanning (for example, corrupt file, starting/stopping scanning, attachment type not supported, and so on).
- *Update events*
It contains messages about antivirus software updates (for example, outdated virus database,



Vexira Antivirus for Windows Servers

update does not start/started/stopped, update with errors, and so on).

- *All events*
It contains all the messages created on the CMS or clients, which enables an easy understanding and tracking of processes (for example, processes running on one client machine).

The event types can be one of the following:

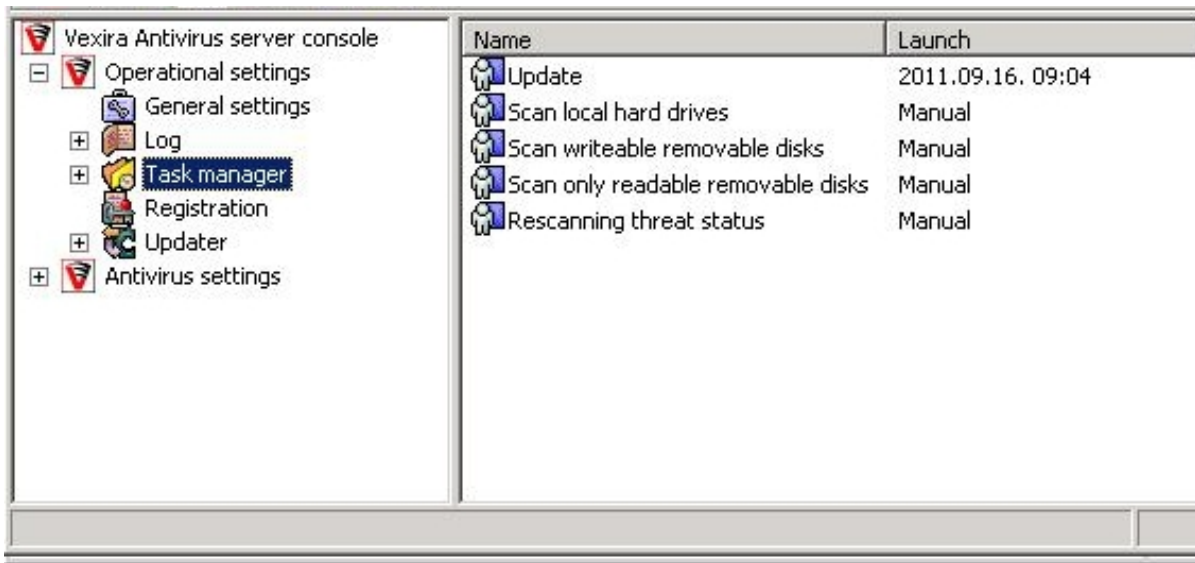
- *Critical*
An event that requires immediate interference (for example, virus database error, scan engine problem, malware detection, and so on)
- *Error*
An event that requires interference (for example, problems with update and installation, lack of license key, and so on)
- *Warning*
An event with lower importance that may cause problems (for example, disabling resident protection, suspicious file detected, file access denied, and so on)
- *Information*
Event not causing any problem (for example, tasks/installation executed successfully)



Task Manager

This component collects all the tasks of the system modules. All tasks added in the program can be managed in this component.

By clicking on the component, all existing (added and default) tasks are displayed in the right side details window. By clicking on the plus (+) sign in front of the component, these tasks are displayed and their types are indicated with the icons in front of them. The icon in front of the name of the task in the details window indicates its status (started, stopped, or paused).



Task Manager

Tasks and Task Settings

You can display the task settings by clicking on it once in the left side list or by double-clicking on it in the details window. The detailed explanation of the settings is available in the section describing the related component.

The following information is displayed next to the name of the task in the details window:

- **Launch**
The method of starting the task. You can read detailed information about this topic in the [Scheduling](#) section.
- **Last launch**
The date when the task was started for the last time.
- **Duration**
The duration of the operation of the task during the last launch.

Functions in the Local Menu

By right-clicking on the task either in the tasks list or in the details window, the local menu appears containing the following functions:

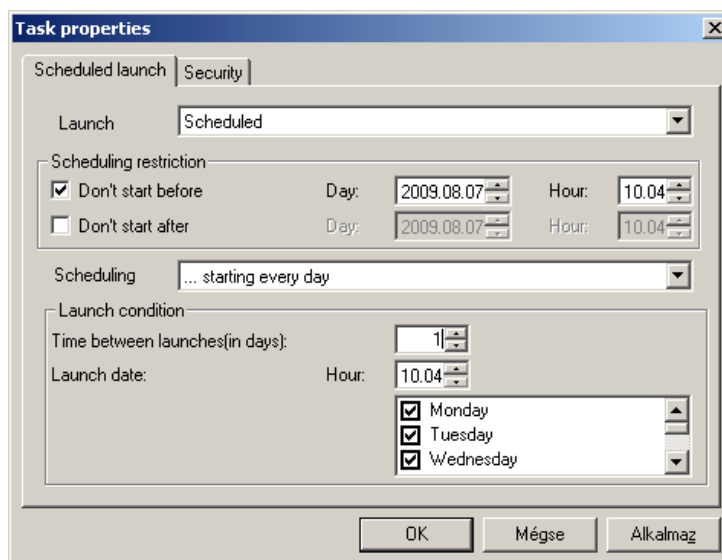
- **Start/Pause/Resume/Stop**
You can start a selected task, pause it, resume a paused task, or stop a running task.



- *Disable/Enable*
It is possible to disable a task. In this case, it cannot be started manually or scheduled until it is enabled again.
- *Manual operation*
It can be used if the task is not started by the user. If you choose this option, the task is set to manual and the user must start it manually. All the specified scheduling parameters are invalid. You can read about scheduling in the [Scheduling](#) section.
- *Modify*
You can modify the selected task settings here. If you select this option, the task settings are displayed in the details window. Default tasks cannot be modified.
- *Delete*
It deletes the selected task from the system.
- *Schedule*
Scheduling of the selected task

Scheduling

You can schedule the task in the local menu. The settings can be specified in a dialog window.



Scheduling

You can select several scheduling options like frequency or a specified date or event. Depending on the task type (update or virus scanning task), the following options can be selected:

- Manual: the task can be started by the user.
- Started in case of a network connection (only in case of virus scanning tasks).
- Scheduled: the start time can be specified in this case.
- Started in case of user login (only in case of virus scanning tasks)
- Started in case of user login and network connection

The *Schedule* type can be selected from a drop-down list:

- Once
- Minutes
- Hours
- Days



Vexira Antivirus for Windows Servers

- Weeks
- Months
- Years

You can set the intervals after which the task must be started on the specified days using the *Time between launches*, *Day and Hour* (hour.minute) settings. For example, if the scan must be started every third week, the *Schedule type* is weekly, the *Time between launches* option is three.

You can assign a user profile to individual schedule settings in the *Security* panel and the task is performed with the specified user's security settings and only if that user is logged in.

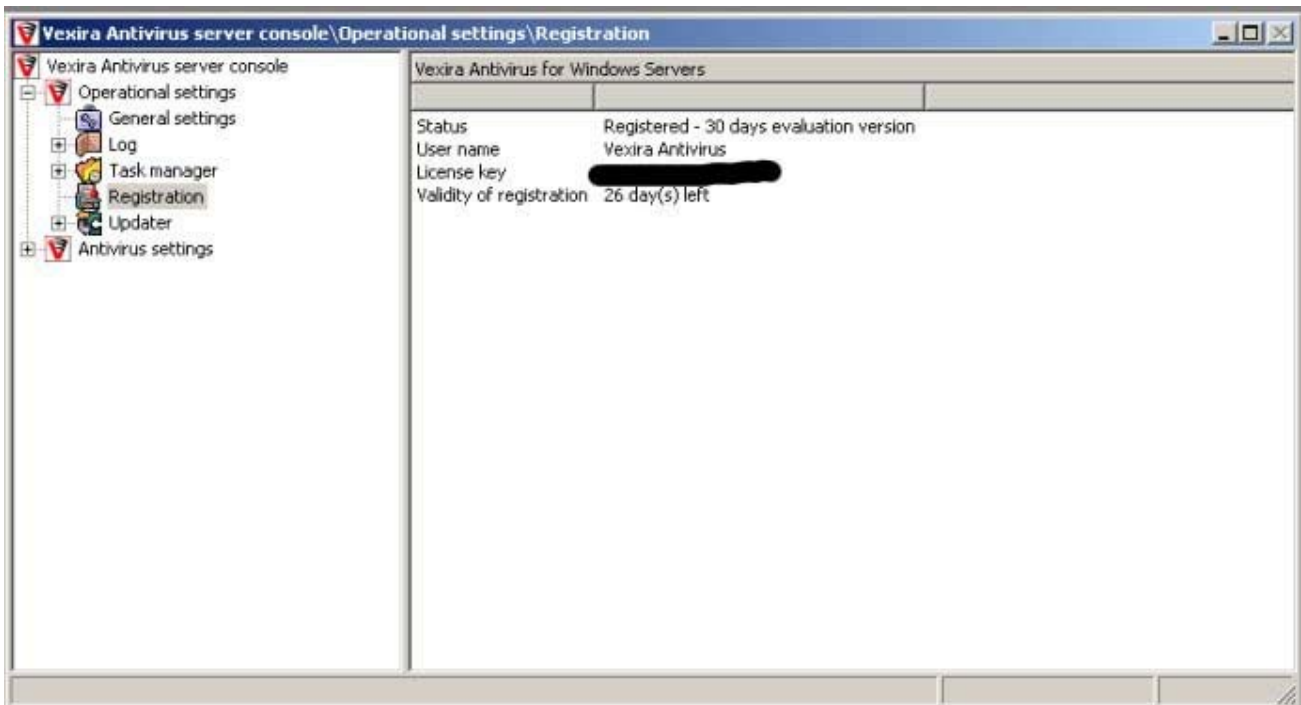
- *Anyone*
The tasks are started in case of any user.
- *Default*
The security context of the user defined in the Operational settings/General settings panel is used.
- *Custom*
You can specify a custom user.



Registration

The task of this component is to check and store the registration data specified by the user. The registration data includes a username and a license key.

After clicking on the Registration component, the installed Vexira Antivirus products and their registration data are displayed. To modify these, right-click on the registration data of the needed product and select Registration from the local menu.



Registration

Select the needed product in the registration window – this is only needed if several Vexira Antivirus products are installed – and specify the registration data in the appropriate fields and click on the **OK** button. In case of a successful registration, the following items are displayed under the name of the product:

- *Status*: Registered
- *User name*: the specified name
- *License key*: the specified registration code
- *Validity of registration*: the date of expiry, the product is registered until this date.



Updater

Updating the software and the virus database is vital for maintaining the protection effective. The software update is based on tasks: the update can be started with a few clicks or can be scheduled for a date or an event and it is performed with the pre-defined settings.

The date of the last update of the product can be checked on the user interface. If there is a virus database installed on the machine, the last update of the virus database is displayed; if there is no virus database on the machine, the last update of the product is displayed here.

The product uses an incremental virus database update mechanism to keep the virus database up-to-date. The advantage of this method is that the program does not 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 additional virus database packages can be released several times a day to improve security. Users can obtain protection against new malware without spending a long time and generating considerable network load for the update. The protection is available almost immediately after the signatures of the newly discovered viruses were processed in our virus lab.

By clicking on the Update component, the *Last started update task* and the *Last performed update* information is displayed, which are the following:

- *Task name*
- *Task started*
The date when the task was started
- *Task source*
The update source assigned to the task
- *Tasks result/updated product*
The result of the task/The name of the updated product

The difference between the two groups is that the last started task may not have been successful, but the last performed update was a successful update process.

By clicking on the plus (+) sign in front of the component, the icon of the Source panel and the Tasks folder are displayed, with the help of which the module settings can be modified.

Source Settings

By selecting the Source panel, the available update sources are displayed in the details window. The sources can be activated by selecting the checkbox next to them. If a source is selected, it is possible to perform an update from it, and it can be selected when adding or modifying a task.

The possible update sources and their settings are the following:

- HTTP
Update through the HTTP protocol. Specify the name, of the HTTP server, the used port (default is 80) and path where the descriptor file can be found. The default setting is:
www.upd.vexira.com:80/pub12
If the connection needs a proxy server to access the update source, you can specify additional settings:
 - Proxy
 - *None* – There is no need for a proxy to access the network.
 - *Specified in Explorer* – The application obtains predefined proxy settings from Windows Internet Explorer.



- *Customized proxy* – If this option is selected, you can manually set proxy settings.
 - Proxy server/port – Address and port settings required to access the proxy server.
 - Proxy user/password – Username and password if the proxy server needs authentication.
- FTP
 - Update through the FTP protocol.
 - The following must be specified:
 - The name of the FTP server
 - The port used by the server (default is 21) and the path
 - The path where the descriptor file can be found
 - The username and password
 - If you use the 'Anonymous' username, type your own e-mail address in the password field. The default setting is: [anonymous@ftp.upd.vexira.com:21/pub12](mailto:anonymous@ftp.upd.vexira.com)
- NetWare path
 - The update can be performed from a Novell NetWare server if the needed path is typed in the field in the UNC format (`\\servername\sharename`).
- Path
 - The update can be performed from a local or a network drive. The path can be specified by clicking on the `|...|` button.
- CD drive
 - If the update is performed from a CD, select the letter of the drive from the drop-down list.

Important!

The update can only be performed from a local or a network path if the user is logged in to the domain.

The update can only be performed from a Novell NetWare network path if the user is logged in to the server.

Tasks

After clicking on the Tasks group, all the existing – default and added – tasks are displayed in the details window. The icon in front of the task name indicates its status (started, stopped, or paused).

The product contains a task called *Update* by default which checks the update source in every hour for new product version or virus database and if it is available, the update process will be started.

Tasks can be modified, deleted, or scheduled from the local menu described in the [Tasks and Task Settings](#) section. The method of adding a new task is detailed in the [Adding New Task](#) section.

Update Task Settings

You can select the update source in the *Type* option, where the program checks if there is a new version available. Only active sources that are set in the [Source](#) panel can be selected.

You can select the products to be updated in the *Products to be updated* option.

If the *Dialog window* option is enabled, you can check the update process step-by-step and the program prompts you at every step if the *Interactivity* option is enabled.

If the update source can be accessed through the network, you can specify the information needed for the network connection in the *Network connection parameters* option. If the *Continuous network connection* option is selected, the task does not try to create a connection and it generates an error if the connection is not available. If the *Dial-up connection* option is selected, the task tries to establish a connection and terminates it after it is performed if the task created the connection. In this case, you can specify a password for the connection.



Vexira Antivirus for Windows Servers

The *Restart computer* option controls the system restart. If you deny it, the computer is never restarted after an update process is finished.

! Important!

Do not disable computer restart unless you have a relevant reason to do it, because there may be changes performed during the update process that need computer restart to be activated. If it is disabled, the resident protection of the computer may not be activated and your computer is not protected.



ADDITIONAL INFORMATION

Virus Scanning Methods

The virus scanning engine can scan for and detect viruses according to the set methods/levels. You can choose the needed scanning method in the components of the software. The following levels are available:

- *Quick*
Scans only the parts of a file that are most likely to contain a virus and does not detect viruses that can only be detected by using a large amount of system resources (for example, Excel FORMULA viruses).
- *Extensive*
Optimized scanning method that detects all viruses registered in the virus database and scans those parts of the file that are most likely to contain a virus.
- *Full*
Detects all viruses registered in the virus database and scans the whole file, even the parts where viruses are not likely to be found.

Heuristics

During a heuristic analysis, the software tries to detect codes and programs that have virus-like characteristics but are not registered in the virus database. If such a *suspicious* file is found, the user is notified. The following levels of heuristic analysis are available:

- *Disabled*
There is 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.

Actions

In case of a virus infection, several actions can be performed on the infected file. The following actions are available:

- *Kill*
Removes the virus from the infected file, the file becomes disinfected and is restored to its original status.
- *Move to quarantine*
It moves the file to the quarantine directory. Viruses moved to the quarantine are not functional, they are not dangerous for the system.
- *Skip*
No action is performed on the infected file.
- *Delete*
It deletes the infected file permanently.
- *Rename*
It changes the first letter of the name of the extension to v in the infected file.



The following actions can be performed on e-mail attachments:

- *Delete attachment*
It deletes the infected attachment from the e-mail:
- *Rename attachment*
It renames the first letter of the name of the extension to w in the infected attachment.

Testing the Virus Scan Engine

In order to see what happens when our virus scanning engine finds an infected file, you can use the European Institute of Computer Antivirus Research (EICAR) Standard Antivirus Test file, which naturally is not a virus, but is detected by our engine as if it were. To create a file that contains the EICAR sequence, type the following string and save it in a file with the **.COM** extension (like **EICAR.COM**):

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

To check the operation of the virus scanning engine, perform a virus scan on the created file or execute the file if the resident protection (Guard) is active. If the engine is operating correctly, the result of the scan or the execution is a warning window.

Note
If executed, this small COM file displays the "EICAR-STANDARD-ANTIVIRUS-TEST-FILE" message and it exits.

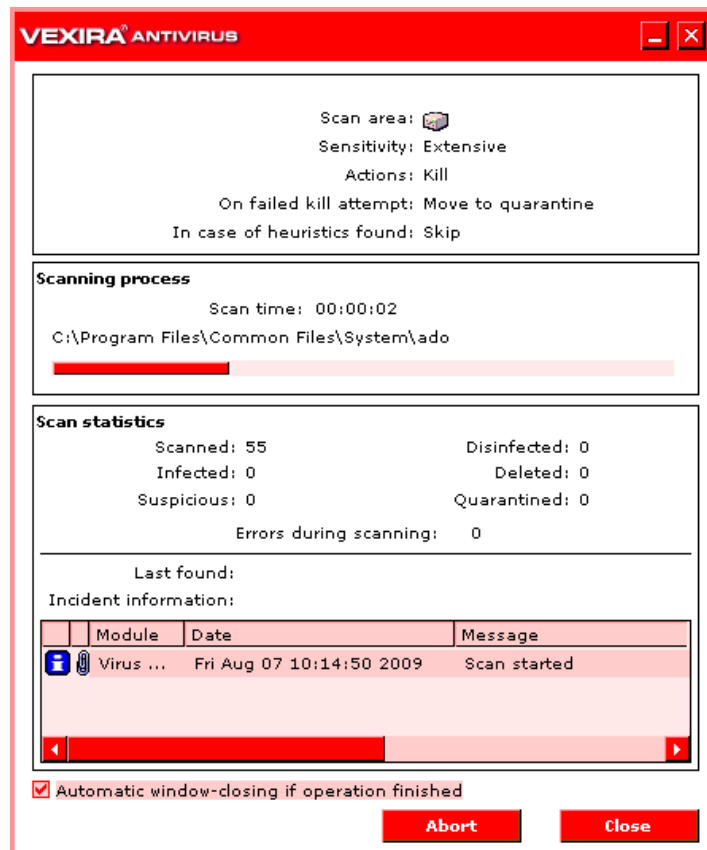


Windows, Messages

Vexira Antivirus displays its messages and information in message windows on the screen to inform the user about viruses or events occurring in the system.

Virus Scan Window

When a virus scan is started, the scanning process and its parameters are displayed in a window to inform you about the status of the scan.



Virus Scan Window

In the upper part of the window, the main settings of the scanning process and the method of scanning and disinfection are displayed. The *Scanning process* section contains the name of the file currently scanned, its path, the elapsed time, and a status indicator bar. The *Scan statistics* section contains the number of scanned files, the number of infected files, the number of disinfected files, and the number of suspicious files. The *Last found virus* – where the last found infected file and its path are displayed – and the *Virus name* fields inform you about the last found virus. The log entries generated during the scanning process are displayed in a window at the bottom of the panel. You can access detailed information about each entry by double-clicking on an item.

Virus scans can be started in many ways, so the displayed scan windows basically contain the same information, but there are some differences between different types of scans. The above mentioned general information types are always displayed in the window, other displayed settings and buttons depend on the starting method of the virus scanning process.



Virus Scan Window During a Scanning Task and During a Manual Scan

In case of these scanning methods, the virus scan window is not displayed as a separate window, but on the console interface. Above basic information, several buttons are available to control the scanning process:

You can terminate scanning by clicking on the **|Cancel|** button to return to the scanning [Tasks](#).

During scanning:

- **|Stop|**
You can stop scanning any time during the process. After stopping the process, the buttons displayed when scanning is finished become available.
- **|Pause|**
If scanning is paused, the process is stopped temporarily, not permanently. You can continue scanning by clicking on the **|Continue|** button.

After scanning:

- **|Rescan|**
It restarts the scanning task.
- **|Save as ...|**
It saves the log entries of the virus scan to a log file.
- **|Add|** (Only in case of *Manual scanning!*)
The scan with the adjusted settings can be saved as a scanning task that can be started later by clicking on a button. Set [Scheduling](#) and [Task's name](#) to be able to create the new task.

Virus Scan Window During a Quick Scan

In case of a quick scan, a window appears which informs the user about the status of the scan. By enabling the *Automatically close the window after the operation* option at the bottom of the panel, the scan window is automatically closed after scanning is finished. This can also be performed by clicking on the **|Close|** button. The scanning process can be terminated by clicking on the **|Abort|** button.

Message Window

The program uses a message window to display information about virus incidents, the effects of operations started by the users, or other functionality problems occurring in the system.

Recognizing a Virus Infection

During a virus scan, if a file is infected, the program displays a message window.

Infection types:

- *Infected - killable*
The virus scanning engine found an infected file that can be disinfected.
- *Infected – non-killable*
The virus scanning engine found a virus in the file, but has no information in its database about the method of disinfection.
- *Suspicious*
The virus scanning engine found a virus-suspicious file. This means that the file contains code or a code segment indicating the presence of a virus. You can read detailed information about this



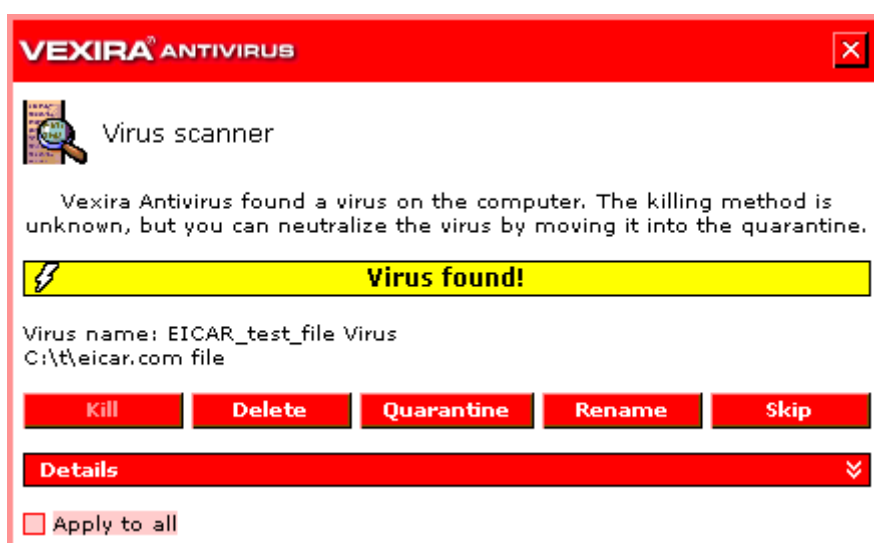
Vexira Antivirus for Windows Servers

topic in the [Heuristics](#) section.

The virus found window can be displayed during the operation of the following modules (if the module is available for the product):

- Scanning task during a quick scan
- If the Guard is active (not interactive)
- MS Office protection (only in case of using Vexira Antivirus Professional)
- MS Outlook protection only in case of using Vexira Antivirus Professional)
- Rescanning of quarantined files

Individual *Virus found settings* can be assigned to all of these modules and the method of disinfection can be set for the found viruses for each module separately.



Virus Found Window

At the top of the window, the icon and the name of the module that sent the message are displayed. This informs you which module found the virus. The red bar in the middle informs you about the type of the infection and you also receive information about the method of disinfection and possible further activities. Below the red bar, the name of the infected file and its path are displayed and next to it – if this information is available, the name of the detected virus can be found.

At the bottom of the interactive panel, there are buttons with the help of which you can specify actions.

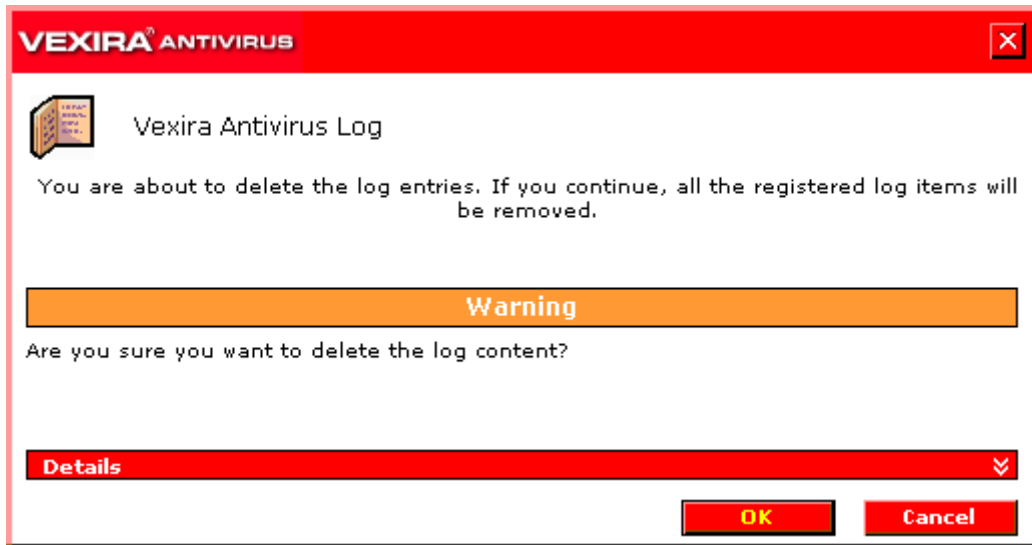
The program can only send a warning message about incidents reported by the *Guard* module, infections are handled as set in the *Virus found settings* section of the module.

By clicking on the **[X]** button in the top right corner of the window, the *Skip* action is performed on the current incident.

By enabling the *Apply to all* option, the system does not notify you about found viruses of this type, and the set actions are performed on the same type of virus incidents occurring.

Warning

These messages provide information about changes and effects or results of an operation initiated by the user.



Warning Message

This window is similar to the virus found window. At the top of the window, the icon and the name of the module that sent the message are displayed. The orange bar contains the message itself and you can read a detailed description in the details window, which can be viewed by clicking on the arrow on the right side of the *Details* bar.

You can confirm the message by clicking on the **[OK]** button, and the operation is continued. If there is a **[Cancel]** button on the panel, you can delete the execution of the started task.



END USER SOFTWARE LICENSE 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, 44258, or fax at +1 330-266-7661. 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 Antivirus for Windows 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.*

DATA COLLECTION AND PROCESSION: *The Software contains technology and functions which will collect computer files and samples of potentially previously unknown, new or known computer malware, spyware, viruses or other similar potentially harmful computer code, instructions or commands and transmit them to Central Command, Inc. together with information about the computer Operating System, hardware, the computer location such as computer name, domain name, IP address and other software programs which are installed or in operation. As part of this data and information collection and transmission configuration data of the Operating System, the Software and other software programs installed or in operation may be sent. This is only a representative list of a limited set of data and information that could be collected by the technology and functions. It is possible that the transmitted data and information may contain additional data and information not published in this list and may include personal information that could identify you, your computer or other personal information that may be valuable to you. Central Command, Inc. will make an effort to limit the collection of personal data and information however it is possible that the forwarded data and information will contain personally identifiable information and data. Central Command, Inc. will use the data and information obtained only to improve the services and the Software and to react and respond to new malware, spyware and viruses. Central Command, Inc. will also sanitize and repurpose only generic data and information to use within its website and other marketing materials. Central Command, Inc. will handle all data and information as confidential and erase, delete and destroy the data and information as soon as it is no longer necessary to retain. Central Command, Inc. may share and redirect all collected data and information with its affiliated companies, business partners and software development contractors. By accepting this Agreement you full understand and accept that you specifically authorize the collection and use of all data and information that is transmitted and forwarded to Central Command, Inc. and grant Central Command, Inc., its affiliated companies, business partners and software development contractors the consent necessary pursuant to local and international laws and regulations to process, store, retain and repurpose the obtained and collected data and information as it deems appropriate within its website and other marketing materials.*

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.*



Vexira Antivirus for Windows Servers

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 trade names 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
support@centralcommand.com