



Waredot Antivirus

USER GUIDE

CONTENTS

Introduction	3
Waredot Antivirus System Requirements	4
Installation of Waredot Antivirus	5
System Status	10
System Scanning	14
When Waredot Antivirus finds the threats	18
Modules of the antivirus protection	20
Tools	26
Reports	31
Settings of Waredot Antivirus	37
Databases and program modules updates	44
Waredot Antivirus registration	48
About Program	53
Customer Support	54

Introduction

Dear user!

We sincerely thank you for your choice of Waredot Antivirus - reliable complex information security solutions.

Waredot Antivirus includes antivirus functionality (that detects and eliminates viruses, spyware, adware and other malware, worms, Trojans, rootkits and other threats).

Waredot Antivirus – is easy to use product, with modern design and a lot of useful functions, reliable and efficient at the same time.



Waredot Antivirus System Requirements

Minimal system requirements for Waredot Antivirus:

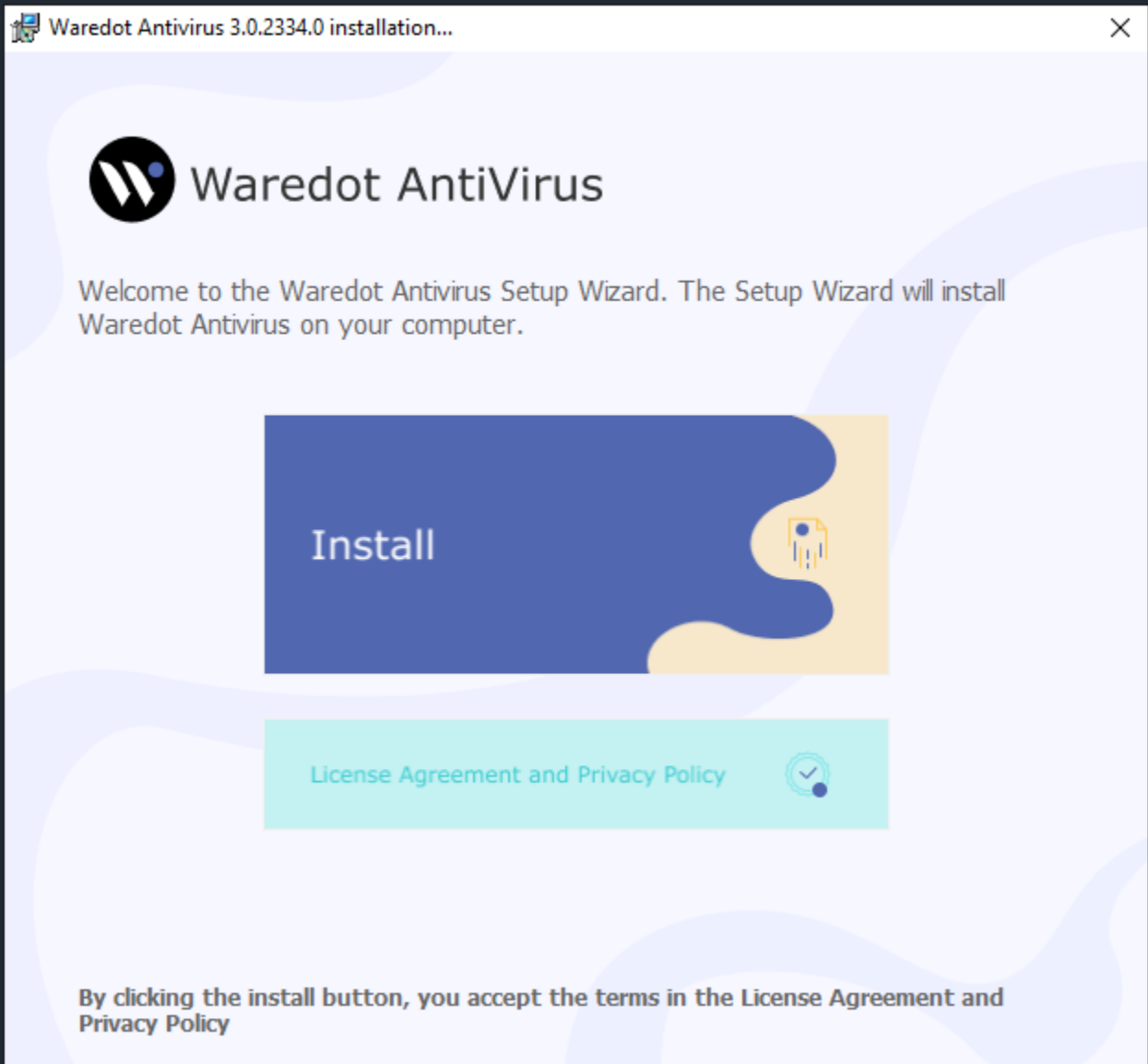
Processor frequency:	1 GHz or higher
RAM:	1 GB or more
Hard disk space:	450 Mb
Operating system:	Windows 7 (x32, x64) (SP1), Windows 8 (x32, x64), Windows 10 (x32, x64)
Screen resolution	1024 x 768 or higher



Installation of Waredot Antivirus

Proper installation of Waredot Antivirus is provided by Waredot Antivirus Installation Wizard. You just need to follow the wizard.

The “Install” button will run immediate installation. By clicking the “Install” button you automatically agree with the License agreement.



Before installing application you can read the License Agreement, click "License" button. After reading the agreement you can return to the installation Wizard by clicking the "Back" button.



ATTENTION

Concurrent usage of Waredot Antivirus with other antivirus software can cause to system errors. We recommend you to delete all other antivirus programs manually before installing of Waredot Antivirus.



There are several reasons that limit the usage of multiple antivirus products on the same computer:

- Antivirus programs request the same system files as you work. Simultaneous requests to system resources can cause conflict or failure of system.
- Some antivirus products offer a scanning service in real time. Such scanning requires system resources. Your computer can start working much slower.

Also, before installing Waredot Antivirus you should remove its previous version.

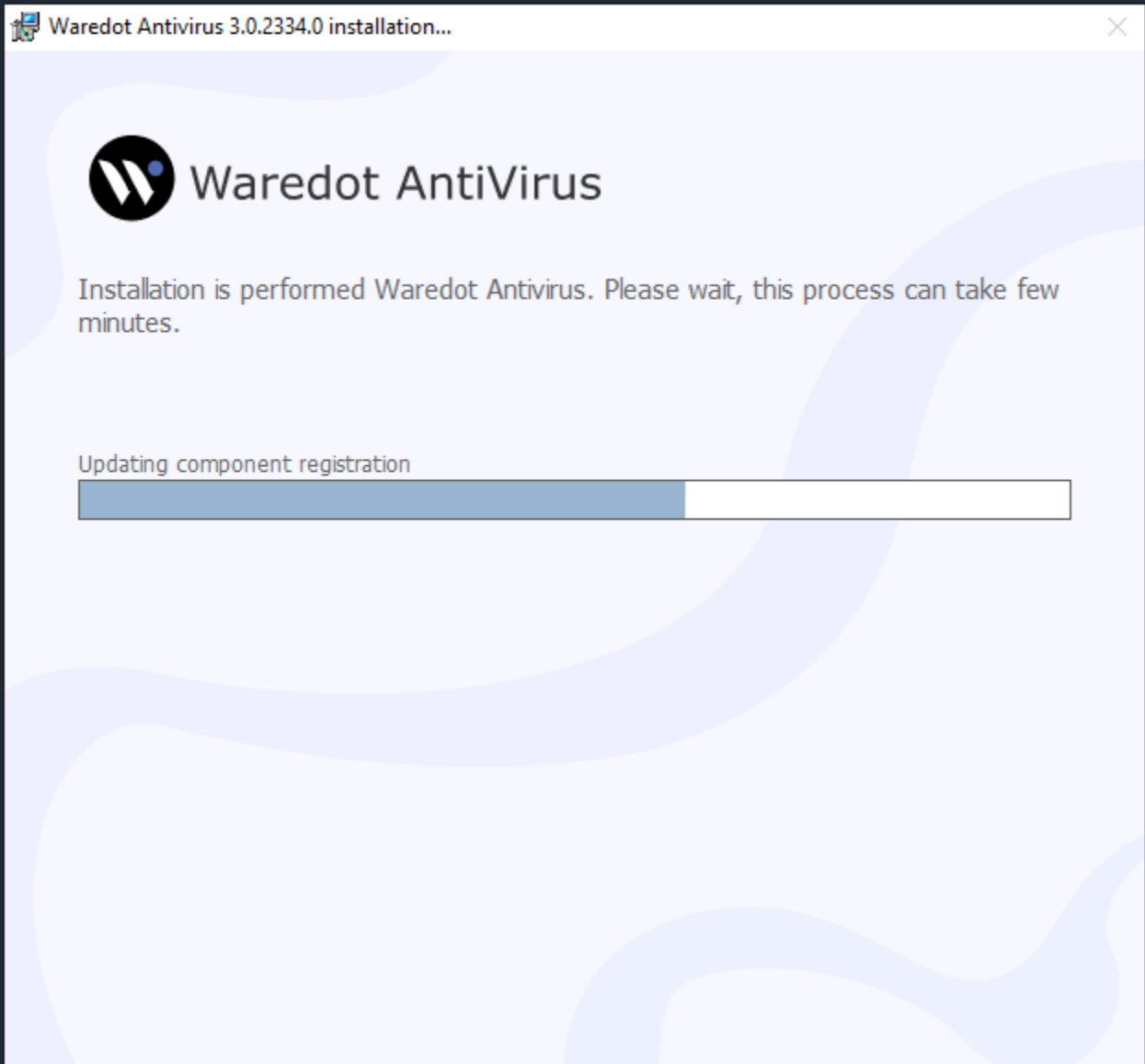
To remove an old version of Waredot Antivirus (antivirus or a previous version) yourself, you should follow these steps:

1. Click **Start**, click **Control Panel** and double-click **Add or Remove Programs**.
2. Select an antivirus program to be deleted in the list of installed programs and click **Remove**.
3. For implementation of changes follow the instructions on screen.

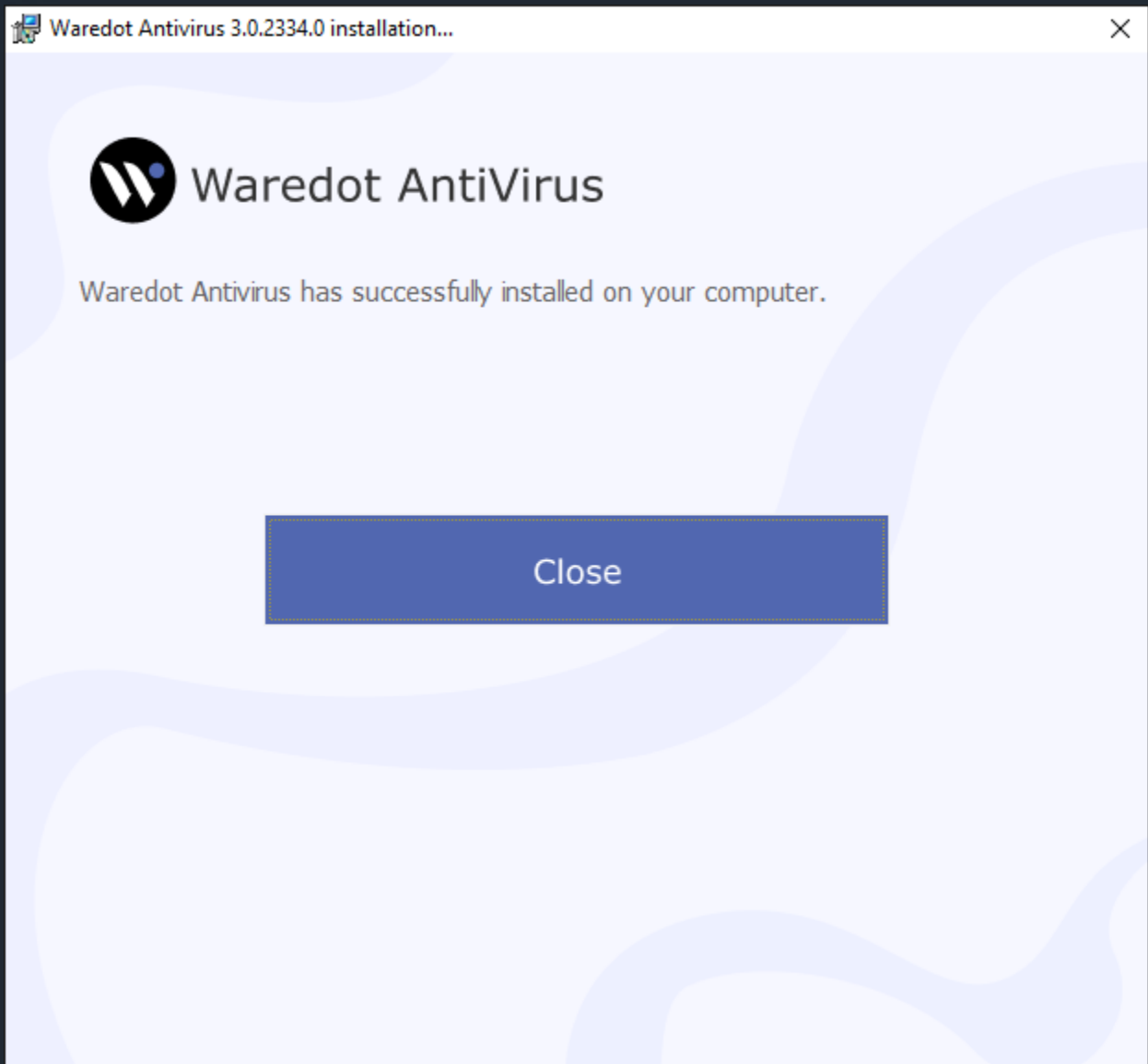
After removal of the previous antivirus program continue to follow the Setup Wizard.



The program is ready to install. You will see installation process after clicking “Install” button.



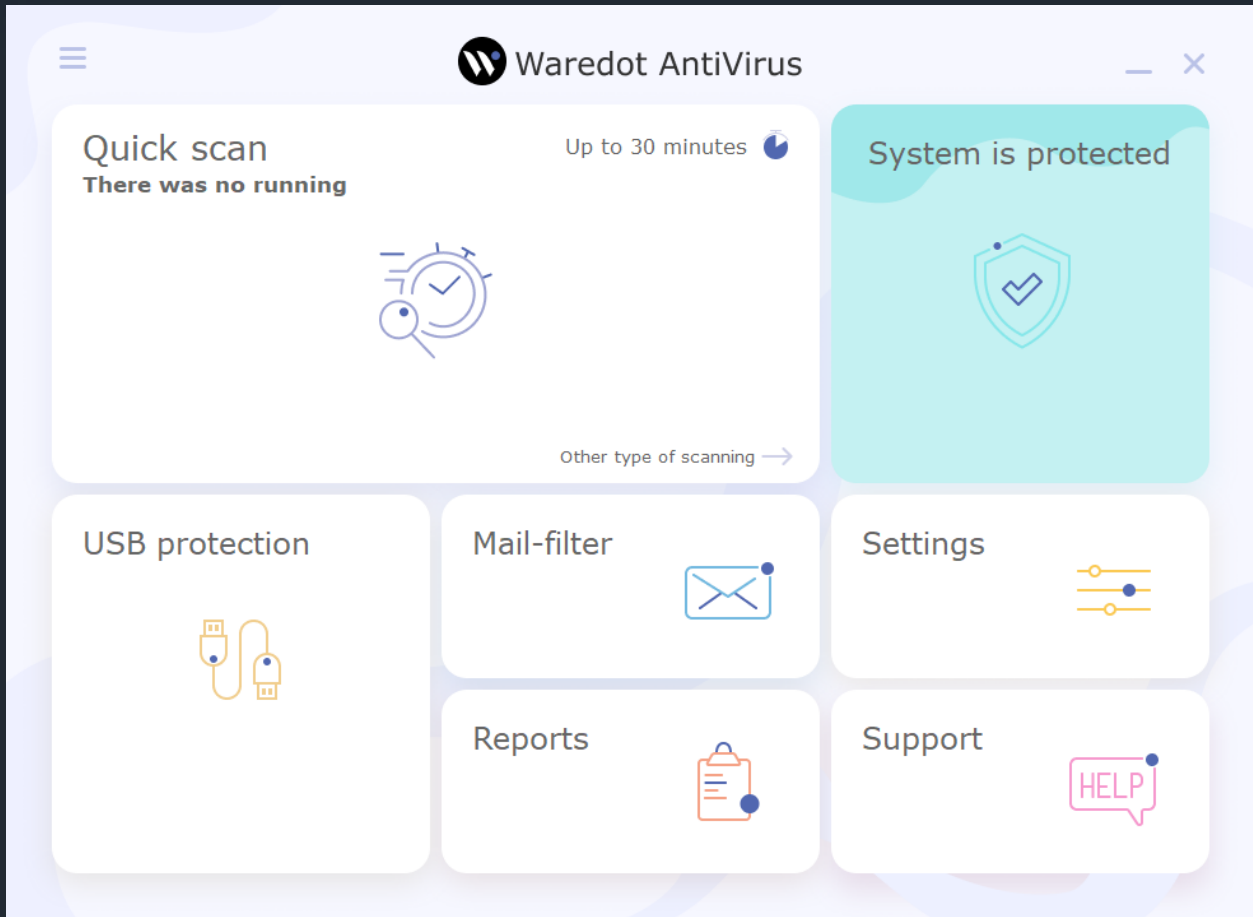
After successful completion of the installation process you will see a window with the next message. Click "Close" button to complete install and run the program.



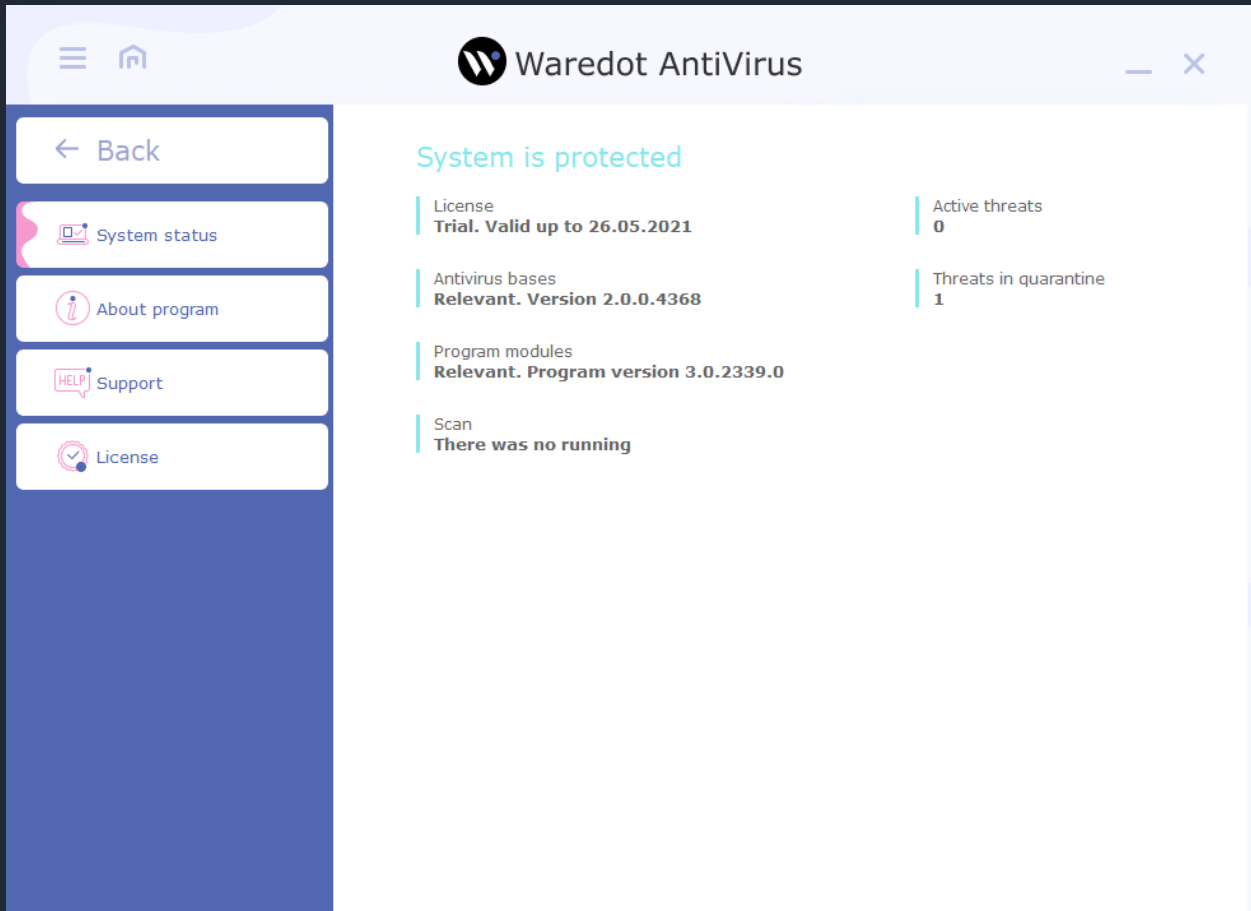
System Status

Waredot Antivirus automatically monitors the system status in terms of security and provides summary information in the System Status in main window of the program.

In basic view:



In full view:

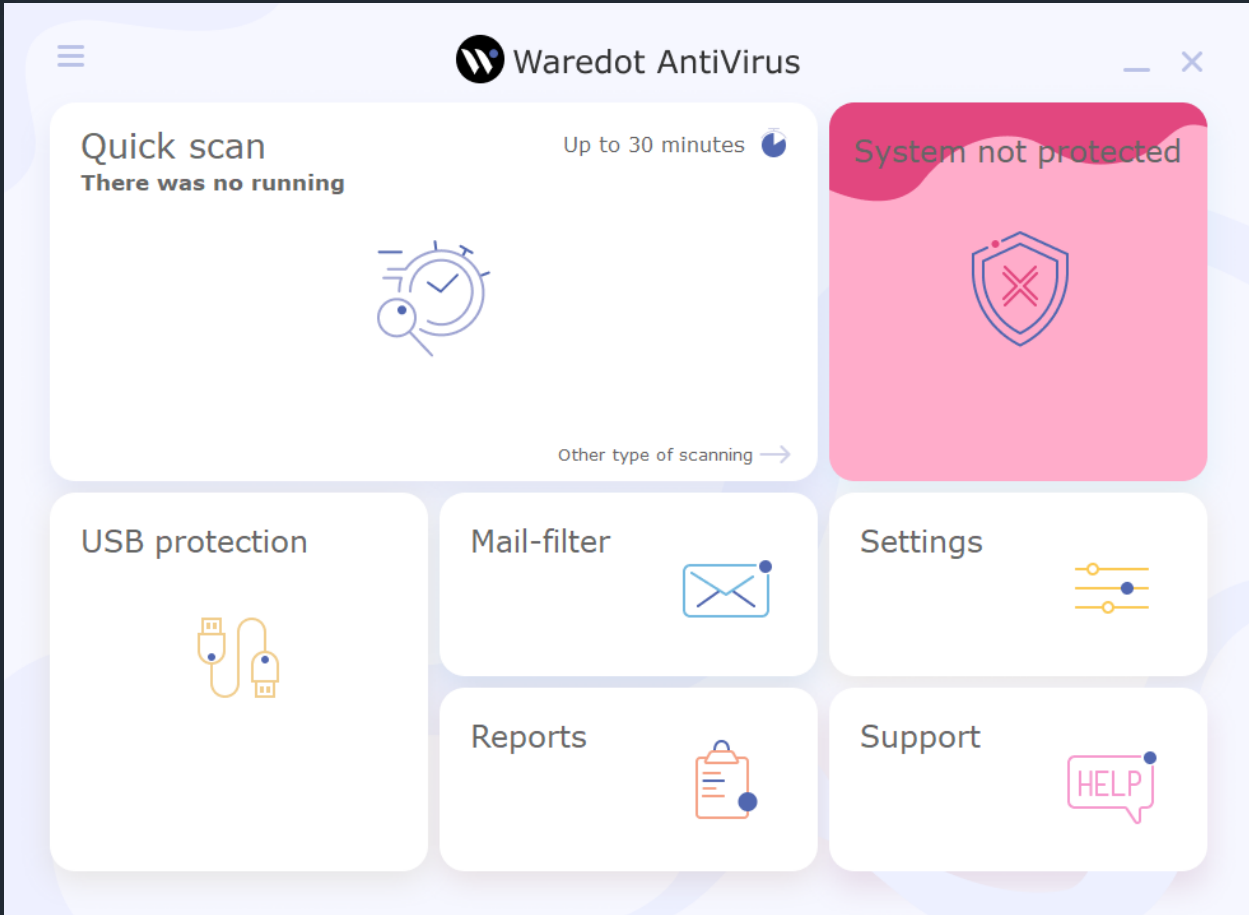


Graphical representation of the system status is presented by Waredot Antivirus in 2 colors.

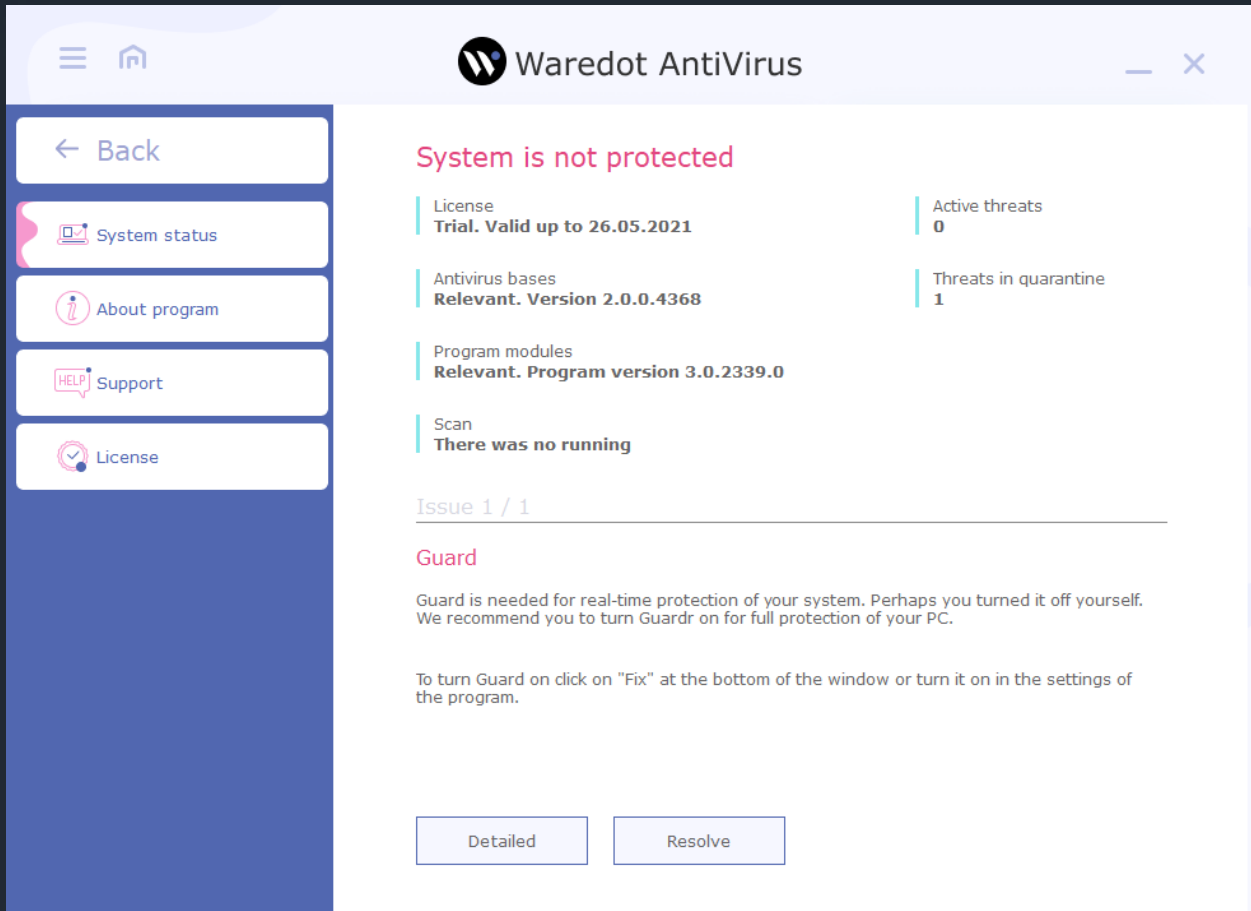
Green color indicates adequate protection for your computer: all systems for protection are on, antivirus databases are up to date and there are no active threats in the system at that time.



Orange color indicates the presence of security vulnerabilities (one or some modules of the product services are turned off, antivirus database are outdated, there are currently active threats etc.) or if antivirus was corrupted and antivirus cannot restored it components for normal antivirus work.



In full view:



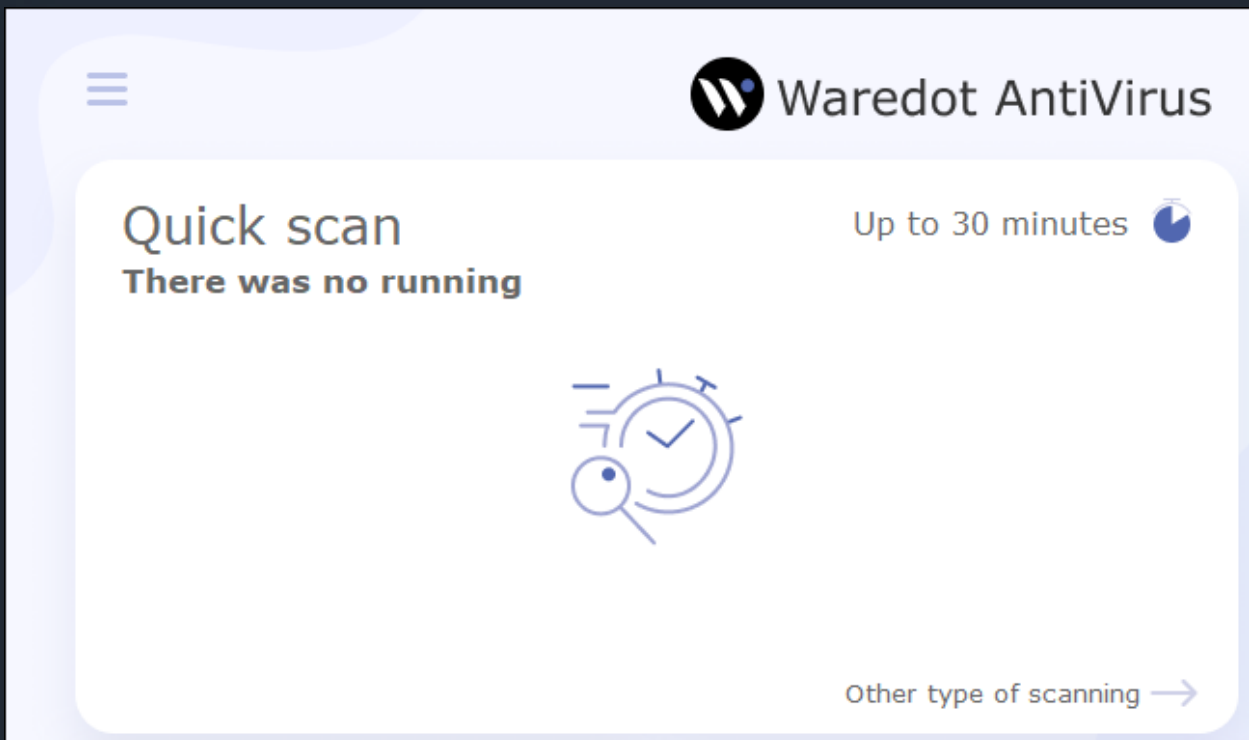
Issue area provides the description on the state of the system and the cause of security vulnerabilities and provides specific actions for their removal. You should follow the advice and guidance offered by program by clicking **Resolve** button.



System Scanning

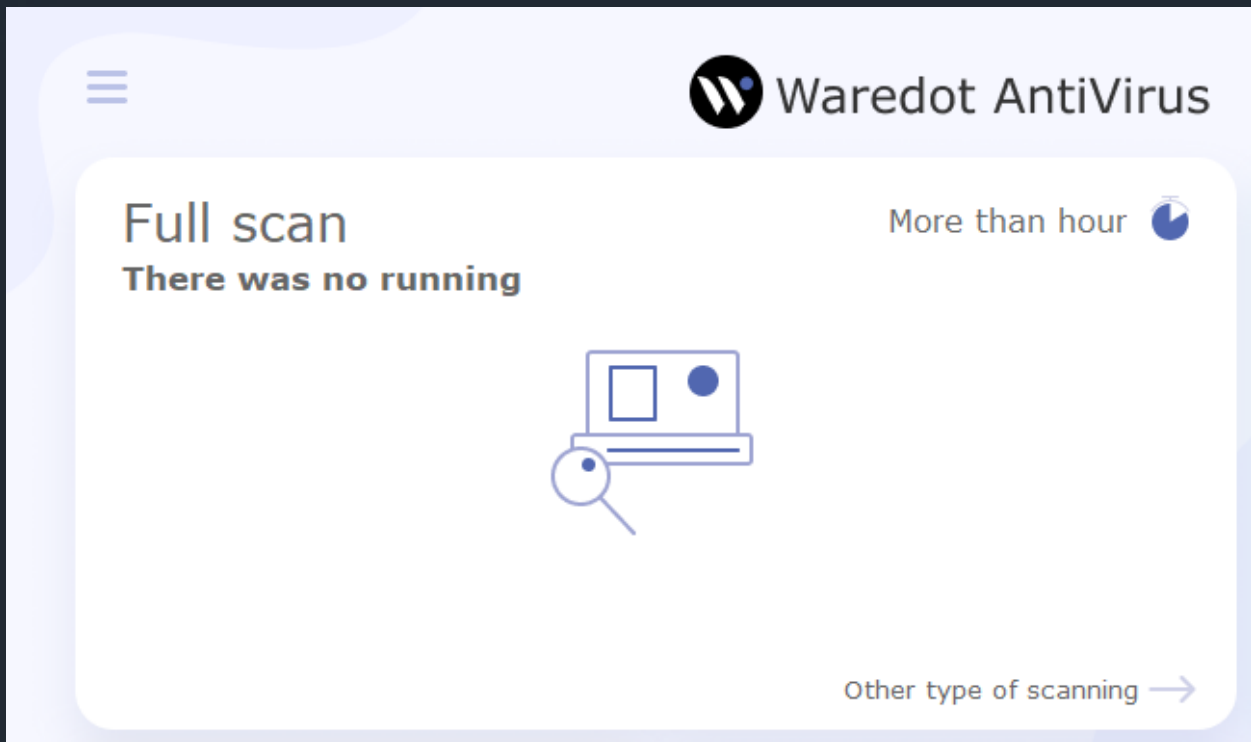
Waredot Antivirus has three scan modes which are available in the main window: **Quick**, **Full** and **Custom Scan**. Each set is provided with certain parameters of the mode. You can choose type of Scan using pointer in the right corner at the bottom of the Scan button.

Quick Scan – express scan of the most vulnerable sectors of system. The following objects are checked: system process, Windows system files, all files in Documents and Settings folder. Quick Scan mode is useful in case of virus suspect after visiting suspicious site or in case when the system works incorrectly.

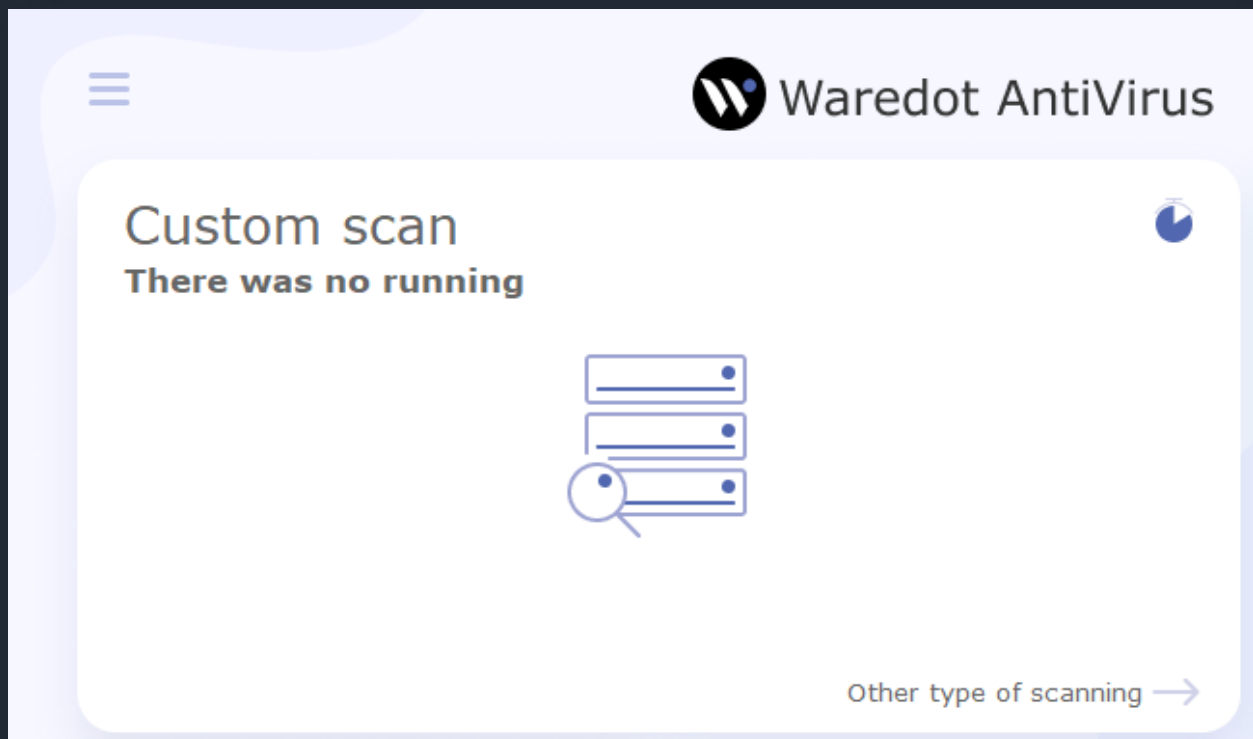


Full Scan – total system check. Thorough scanning of the system. The following items are scanned: system memory, objects that run on startup, backup storage systems, mail bases, hard and removable drives.

We recommend you to make a full system scan at least once a week. You should adjust full scan automatically not to forget about this important operation.



Custom Scan – scanning files according to the user's desire. This type will scan only files, folders and drives which user will choose to check.

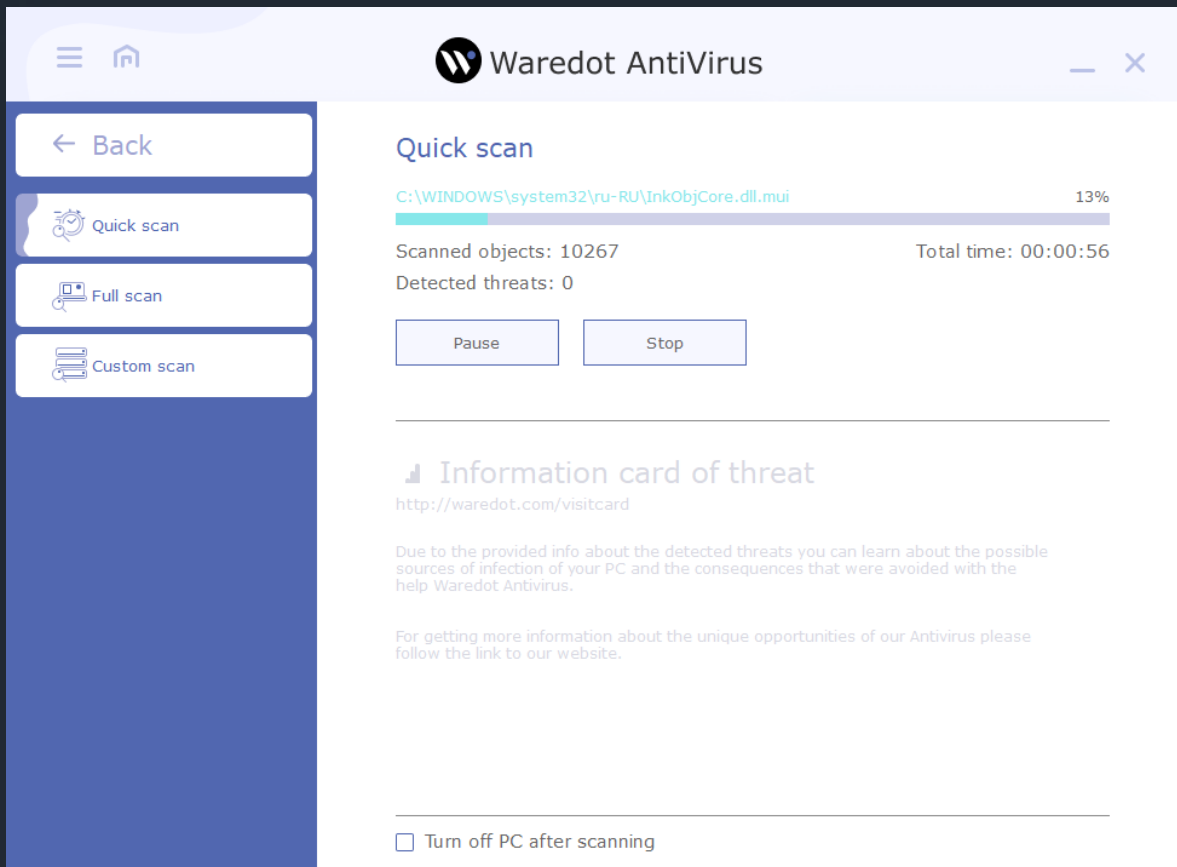


After the scan will be complete you will receive a report with its results: total time of scanning and detailed information about the number of scanned and infected objects.

If the threats will be found there will appear a window with information about their names, level of threat and location. Waredot Antivirus will apply an optimal action to neutralize infected files automatically or offer to user the action for the found threats. The behavior of Waredot Antivirus depends on the settings of antivirus which user can change.



When this process be completed, Waredot Antivirus will show a detailed report on the work done. This report will contain the total time of scanning, number of scanned objects and detected threats, name of infected file and action, applied to it.



There are **three levels** of danger of threats in Waredot Antivirus:

FIRST LEVEL – the files are found using heuristics and these files are potentially malicious files.

SECOND LEVEL – viruses that were found in archives, installation files, disk images, etc. can not cause harm to your PC if you are not running their etc.

THIRD LEVEL – infected files, which were found on the computer. These are the most dangerous files, they can lead to infection of the Operating System and to lowering of its performance. These viruses may be dangerous for users' data too. We recommend users to apply one of the long-term actions for neutralizing of these threats.

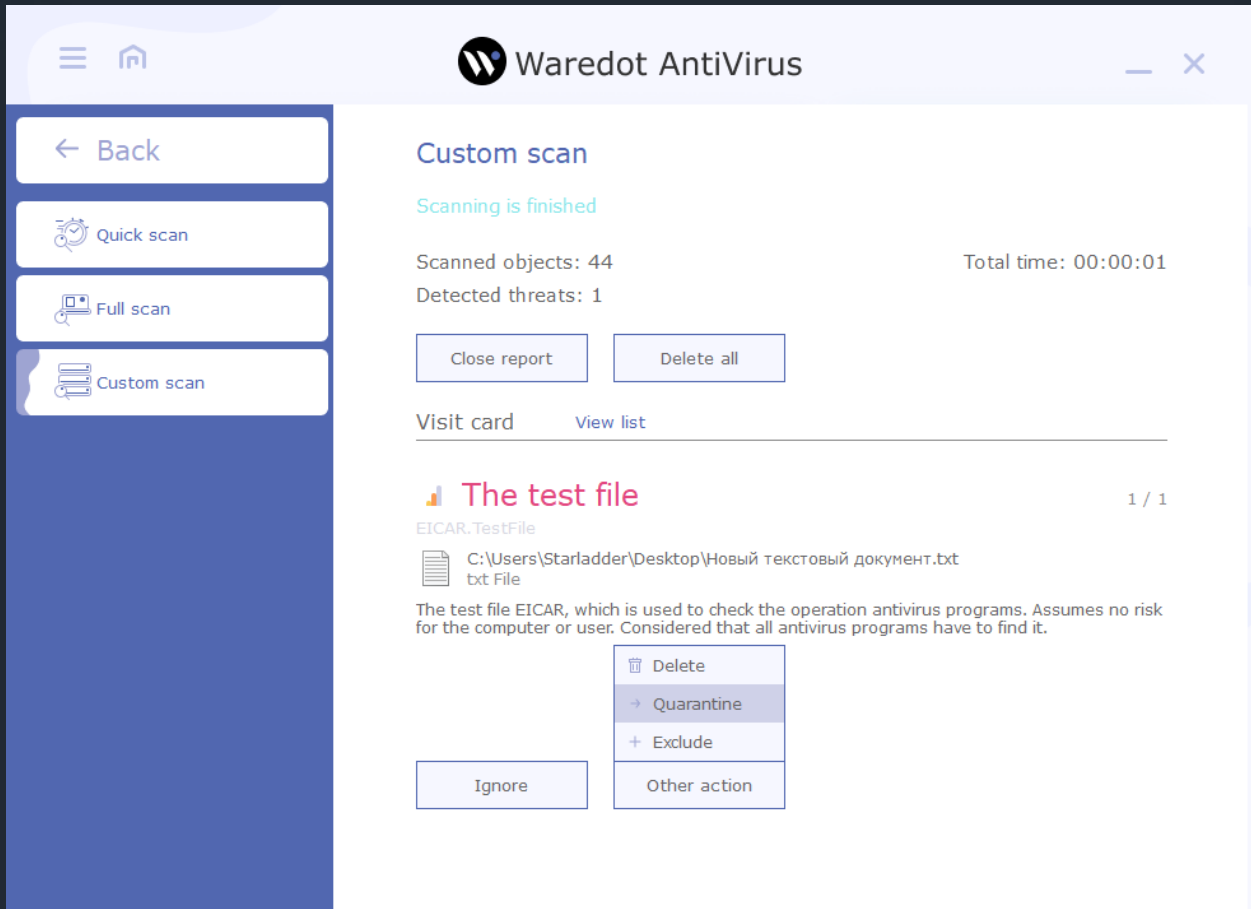
If you do not have time or you do not want to wait for the scan is complete, you can use an option that is placed at the bottom of the window – "Turn off the PC after scanning."



When Waredot Antivirus Detects Threats

Waredot Antivirus has a built-in algorithm of analysis of the detected threat and determination of the optimal action (ignore/cure/quarantine/delete), which needs to be applied. You can view the actions offered by program for certain threats after the scan completed.

In the Report of scan you can view information about active threats (name, short description, security level, location) and make a decision on their future fate.



You can change the reaction of antivirus module for the object, if you are unsure in actions of antivirus.

In some cases, to remove an infected object you have to restart your computer. So do not worry, if not all infected files can be deleted. But in case when even after restart of computer the problem still exists, please seek help from customer service.



Waredot Antivirus can do **following actions on threats**:

Ignore – the action for the ignoring the threat till the next scan.

Quarantine – applying of this action move the threat to the temporary hidden system folders in the root of every local drive. Waredot Antivirus crypts and moves the files to these folders every time when action “Quarantine”. Files in the Quarantine are absolutely safe for the user’s data and software.

Cure – this action run the curing of the infected files and extracting the malicious code from the infected files.

Block – via applying of this action user block the threats. After applying of the action “Block” the file is blocked by Waredot Antivirus and stays in Active threats until user will choose and apply the other action for this threat. If Waredot Antivirus blocks the virus or infected file in this case this virus or infected file is not dangerous for user’s data and PC till Waredot Antivirus is turned on this PC.

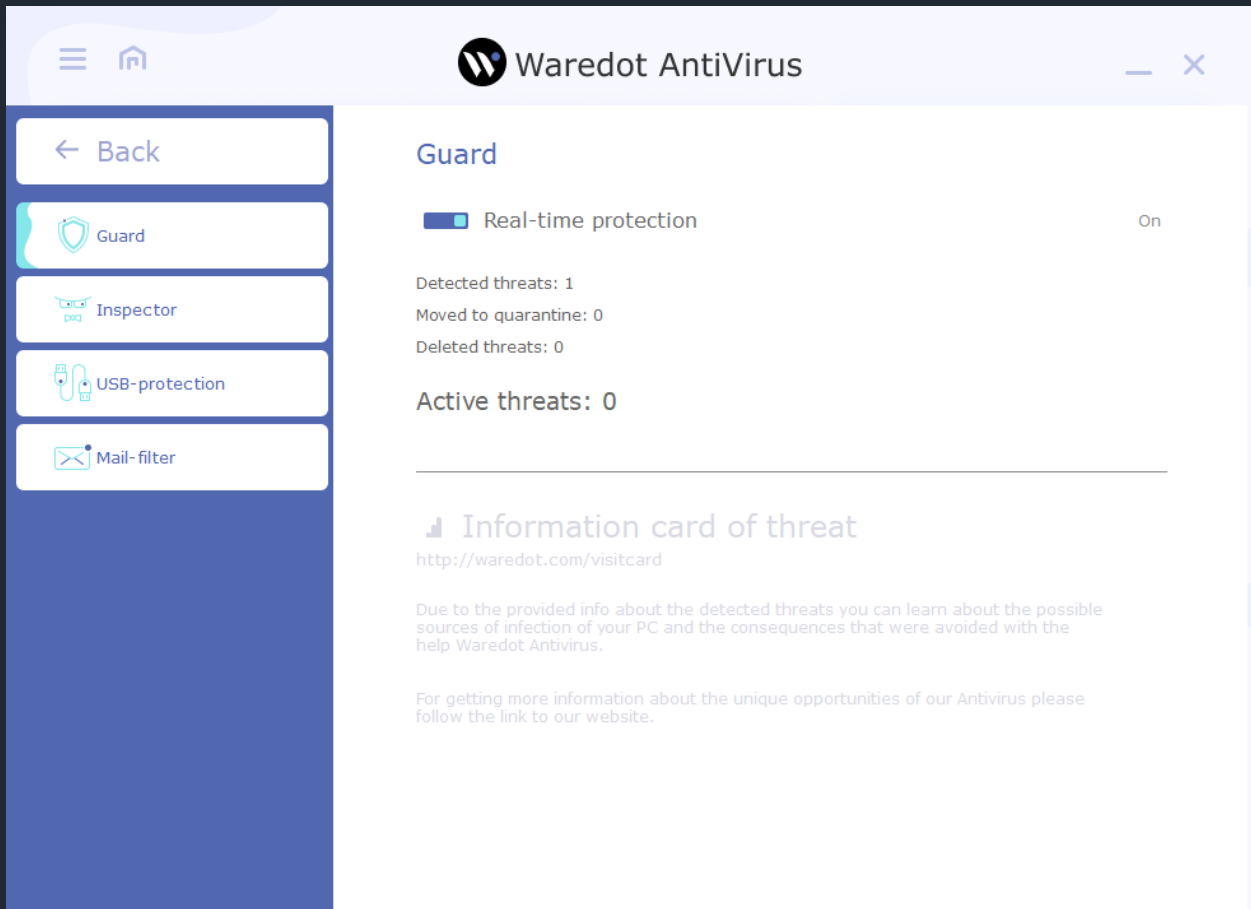
Delete – this action initializes the deleting of the infected file or threat. After deleting user will not be able to restore this file. If user may use this infected file, we recommend to user to apply the action Quarantine to this file and keep these file in Quarantine until it will be needed. Before using this infected file it is needed to add its to Exclusions of Waredot Antivirus.



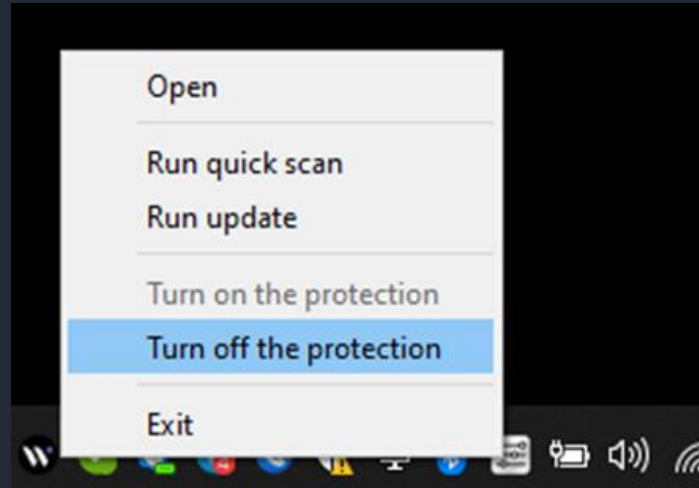
Modules of the Antivirus Protection

Antivirus Protection Includes:

Guard - System File Checker in real time, which is designed to detect viruses and other malicious programs that try to penetrate the PC. Guard detects viruses and other malicious programs "at the moment" effectively blocking them even before the entry into the operating system or files, tracks running processes and thus ensures reliable prevention of infection.



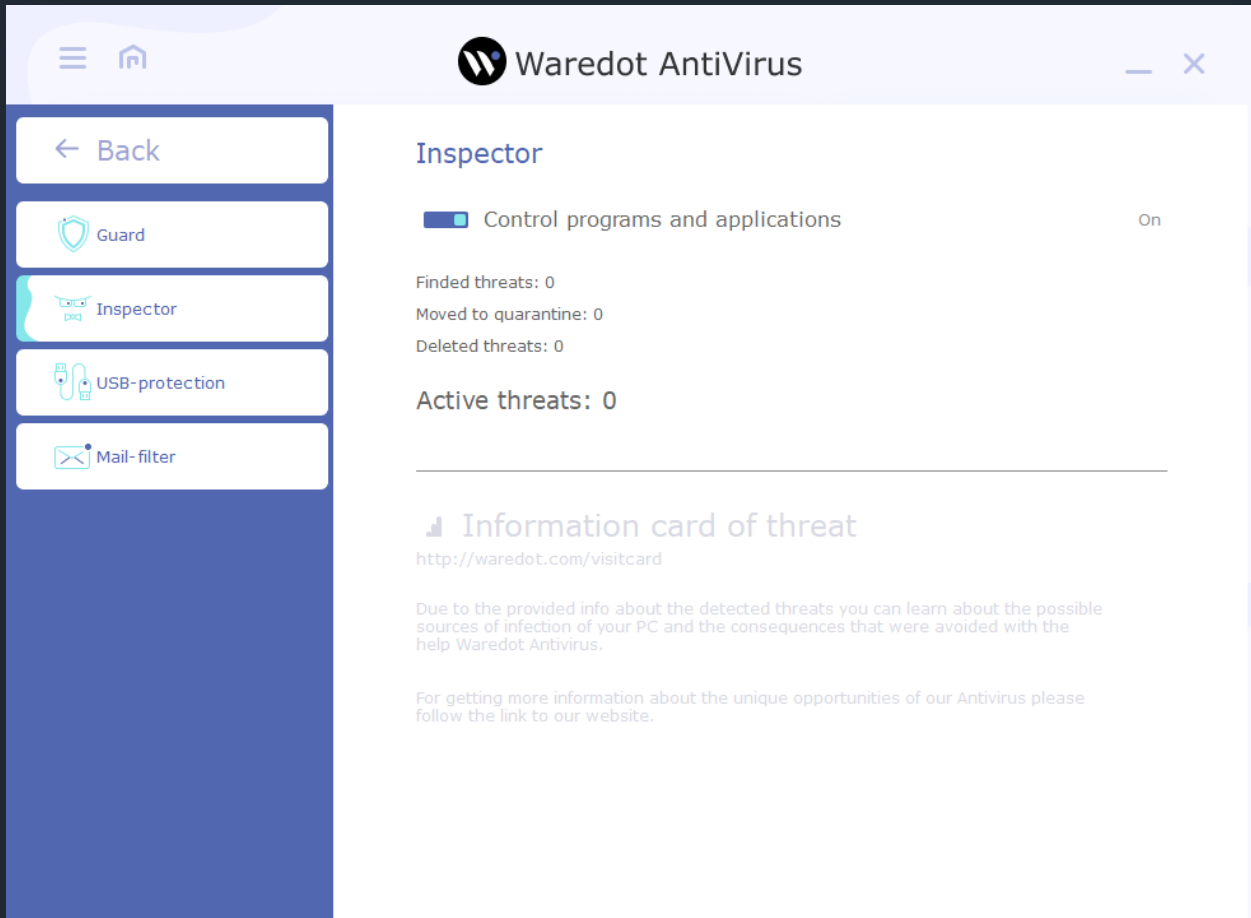
By default, the **Guard** is automatically activated every time you start the program. This is a very important component of protection. We do not recommend you disable this feature. To check whether the Guard is turned on, click the right mouse button on Waredot Antivirus icon in the taskbar notification area or go to the item Turn on the **protection**.



Guard on tab “Settings” – allows you to choose the action which will be applied in the case of detection of threat by Waredot Antivirus.

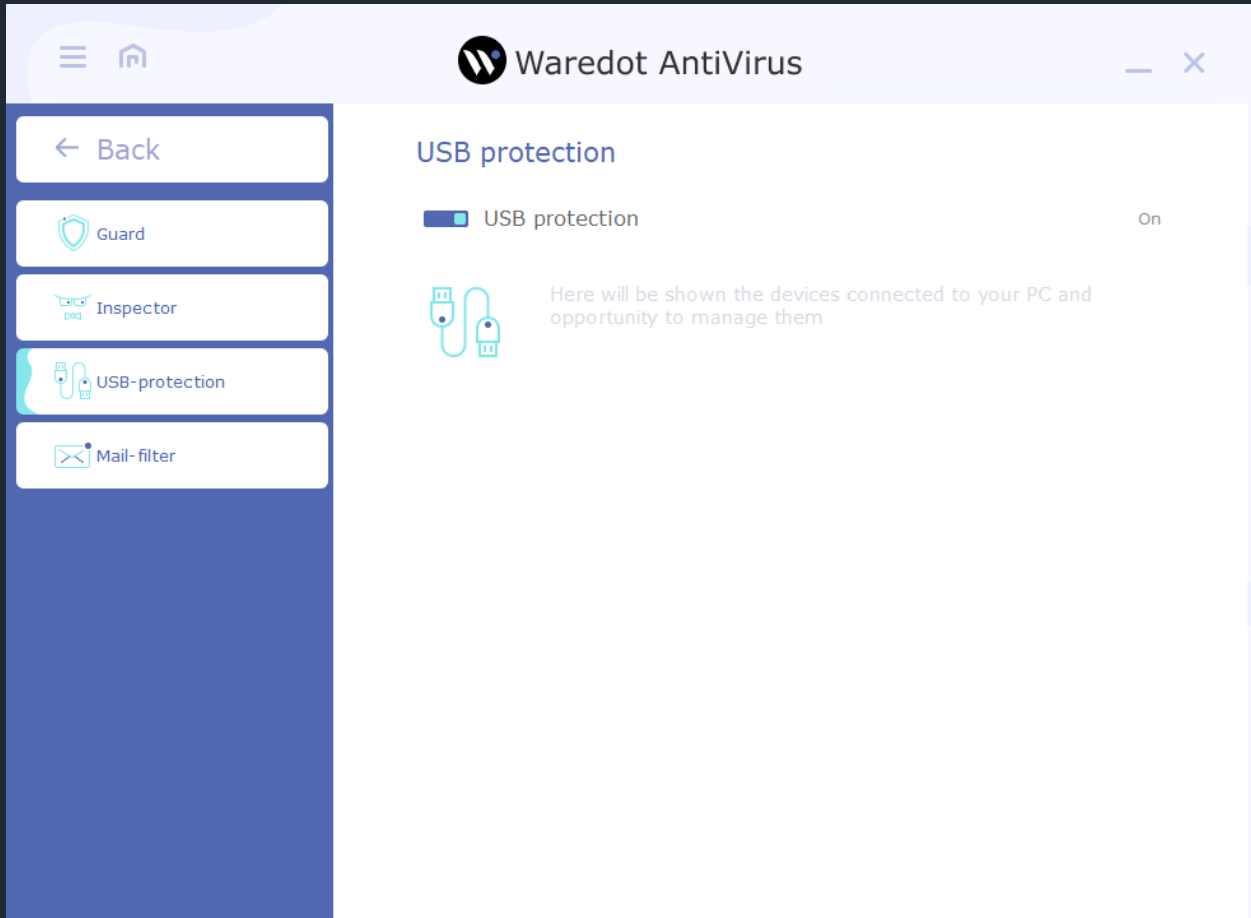
Inspector (Behavioral analyzer, HIPS) - One of the most important modules of all range of antiviruses Waredot is the presence of so-called behavioral analyzer (HIPS).

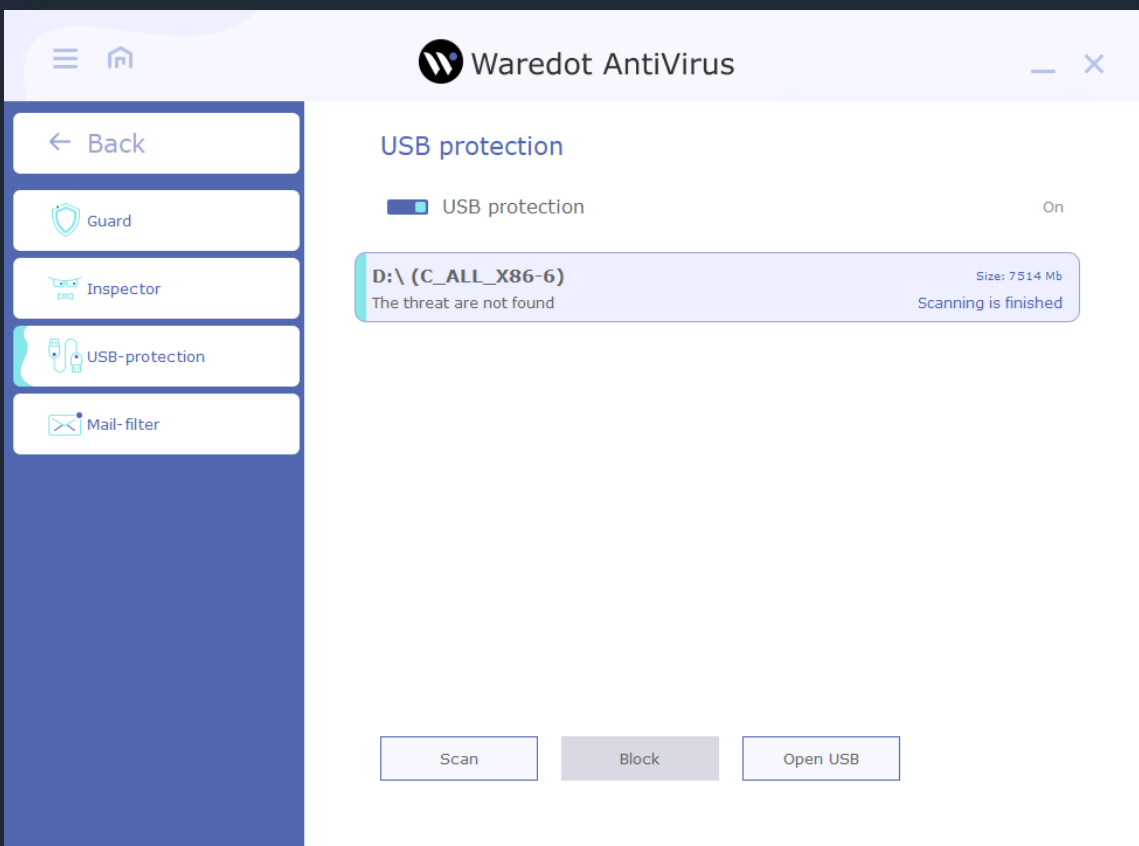
This technology allows to scan and analyze of programs, to determine likelihood of malicious behavior. If HIPS will notice that some program performs actions that could potentially harm PC, it will be blocked even before its launch.



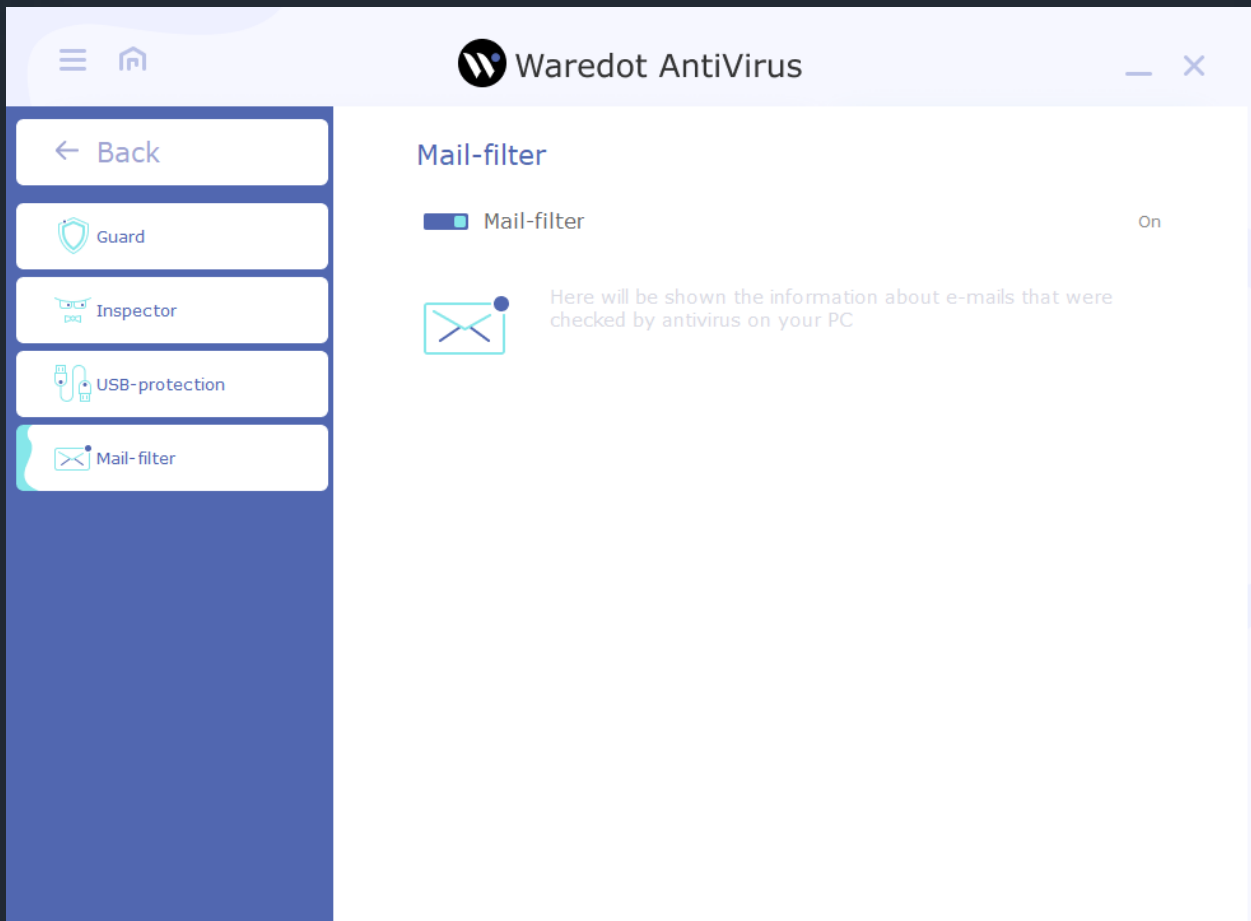
USB – Protection - Security module of USB-drives controls the connection of any drive to the USB-ports. Preliminary analysis with following informing of user reliably protects the computer from automatically downloaded objects on disks. So now Waredot will protect you from the automatic start from the flash drive of a virus or worm, even if it is a completely new, unknown virus.

When a new USB-drive is connected, Waredot detects it, performs a brief analysis and informs the user about the evaluated level of security of the disc. In the case of detection of the viruses or any suspicious objects on the flash drive, antivirus immediately prompts the user to remove them.





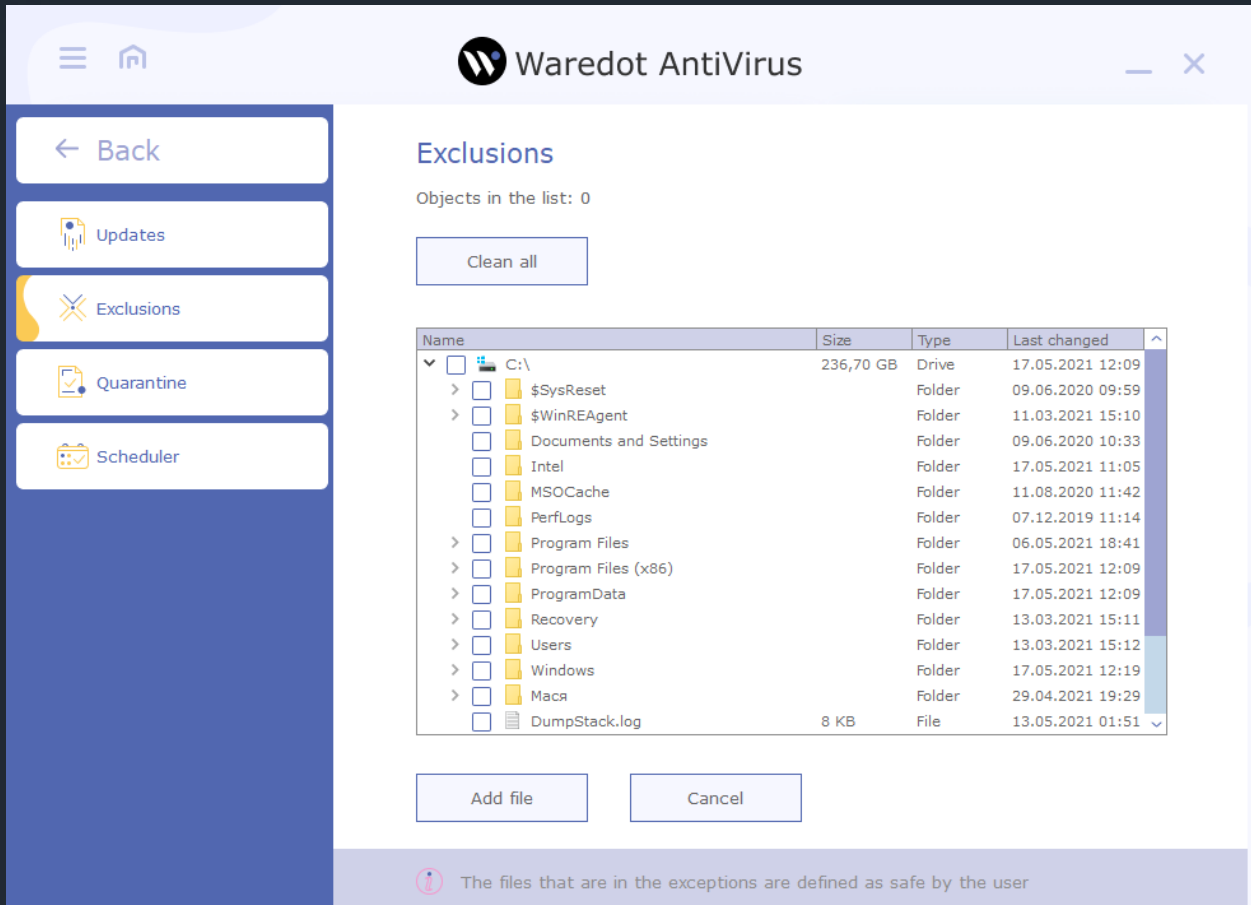
Mail Filter checks all incoming and outgoing email messages for malicious objects, thus avoiding possible infiltration of threats in the system by means of e-mail.



Tools

Exclusions tab contains files which were marked as exclusions by Waredot Antivirus. It means that Waredot Antivirus will skip these files during the scan include the scan with Guard.

You can find the list of Exclusions in the main window of Waredot Antivirus, click the “burger” button in the left upper side of the window and go to “Antivirus protection” section, press the item Exclusions.



Button “Add file” - you can use it for adding files, folders and drives to Exclusions of Waredot Antivirus. For adding the exclusion user need to click the button “Add file” and choose the file, folder or drive. After choosing the item user need to click the button “Add file” again and this item will be shown in the general list of Exclusions.



Please, note: we do not recommend you to add the not trusted files to the Exclusions of Waredot Antivirus because all files in Exclusions are not scanned by Waredot Antivirus till they stay in Exclusions.

Button “Delete” - you can use it for deleting files, folders and drives from the Exclusions of Waredot Antivirus. For deleting the item from the Exclusions we recommend you to choose the object (the file, folder or drive) and click the button “Delete”.

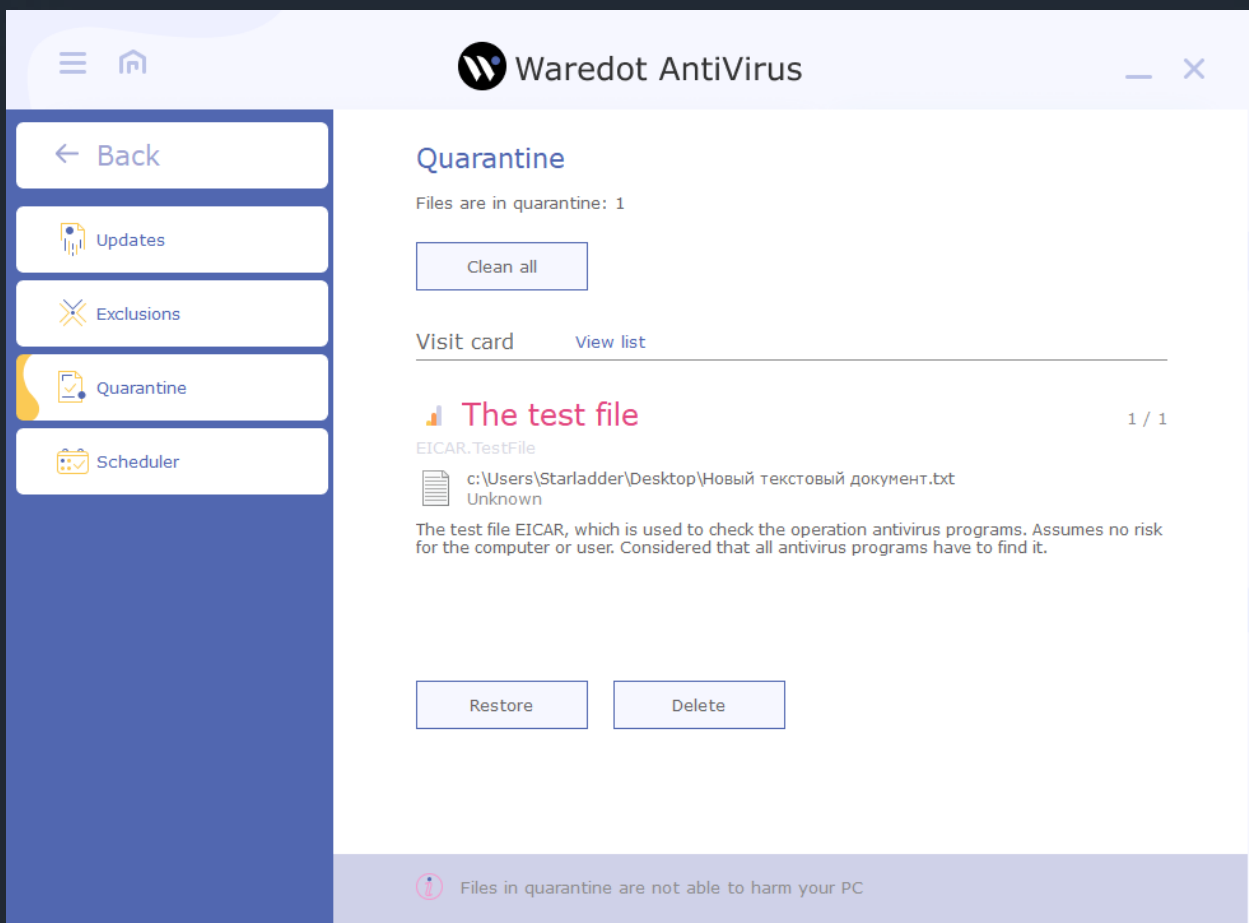
Button “Clean all” – allows user to clear whole list of the Exclusions of Waredot Antivirus with a single click of this button.



Quarantine tab contains the files which were marked by **Waredot Antivirus** as infected and moved by program to Quarantine.

We do not recommend to user to delete the files from the Quarantine. Until the files are in the Quarantine, user may restore them if it be needed in the future. In some cases the value of the file exceeds of the risk of threats for the user. So in this case user may restore the needed file from the Quarantine and it will function as before.

In the Quarantine all files are crypted and they could not be run by the virus or user or three-side software. So the files which are in the Quarantine of **Waredot Antivirus** **do not threaten for the data or software on the user's PC.**



There are two types of presentation the threats in the Quarantine of Waredot Antivirus:

- **Visit Card** – presentation of every threat in the visit card. Visit card contains the name of threat, name of the infected file and full path to the threat and level of its dangerous. Visit card contains the detailed description of the threat. This type of presentation is set as default setting.
- **View List** – presentation of all threats in the list. The list contains the name of the infected file and full path to it, and action which was apply to the threat.

With the buttons “Renew”, “Delete” and “Clean all” user may apply any proper action to the threat in Quarantine of Waredot Antivirus.

Button “Renew” – allows user to renew the threat from the Quarantine tab of Waredot Antivirus.

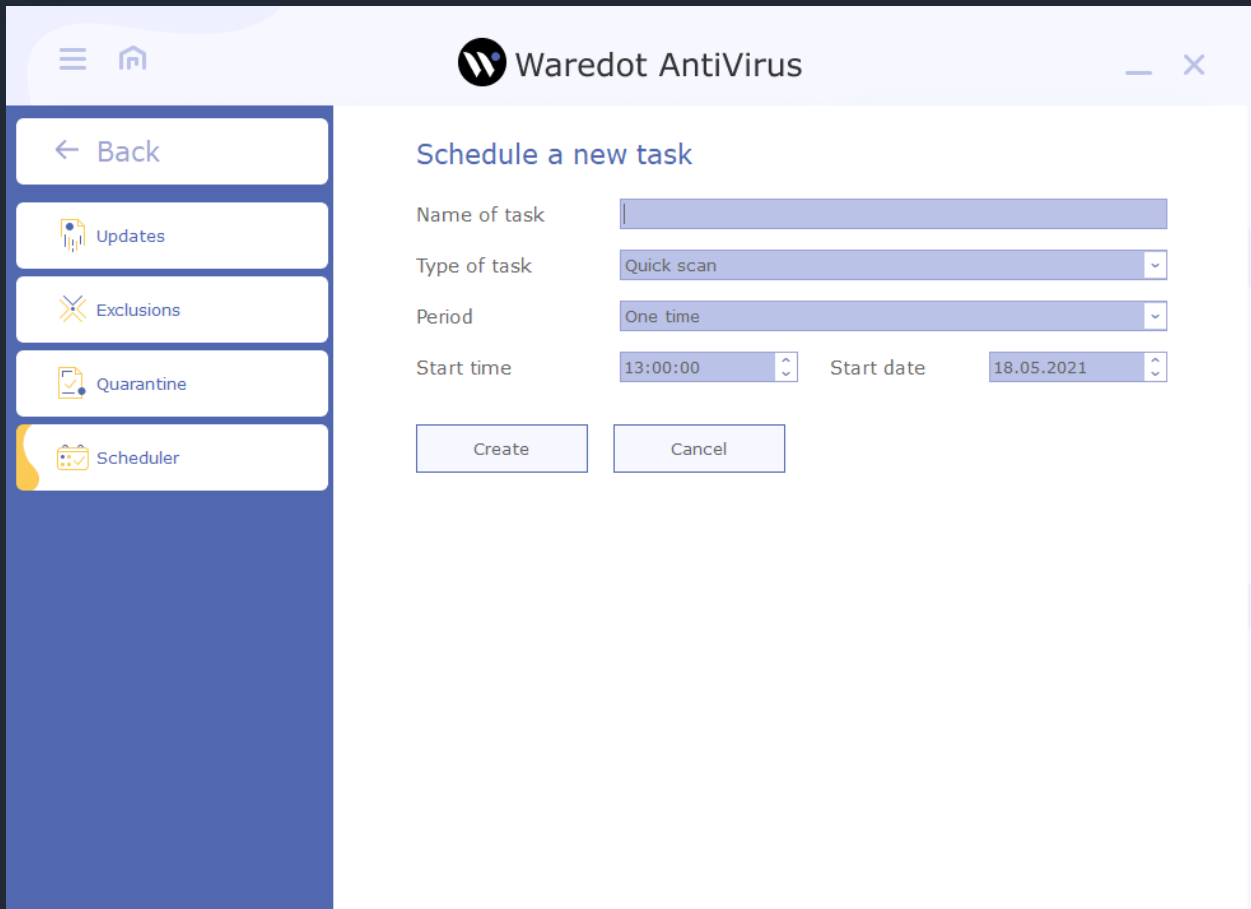
Please, note: after applying the action “Renew” the file will be automatically marked as safe for Waredot Antivirus and it will be added to the Exclusions of Waredot Antivirus. This file will stay in the Exclusions list of Waredot Antivirus till user will not remove this infected file or the file of virus from the Exclusions list manually.

Button “Delete” – user can use it for deleting the files from the Quarantine of Waredot Antivirus. For deleting the item from the Quarantine we recommend you to select the file and click the button “Delete”. After deleting the file it could not be restored.

Button “Clean all” – allows user to clear whole list of the Quarantine of Waredot Antivirus with a single click of this button.



Scheduler allows you to configure when and how often run any type of scan. In the "task name" indicates the name for the planned tasks. Task Type allows user to select a type of scan should be run: "Quick Scan", "Full Scan" or "Custom Scan". With the "Custom Scan", select the scan that file \ directory \ drive. "Period" - indicates how often the task should run the "one-off", "hourly", "daily", "weekly" and "monthly". "Time" indicates 24-hour format the time to start the task. "Start Date" - the date for the scan.



The screenshot displays the Waredot AntiVirus application window. The title bar reads "Waredot AntiVirus". On the left is a navigation sidebar with a "Back" button and menu items for "Updates", "Exclusions", "Quarantine", and "Scheduler". The main content area is titled "Schedule a new task" and contains the following fields:

- Name of task:
- Type of task:
- Period:
- Start time:
- Start date:

At the bottom of the form are two buttons: "Create" and "Cancel".

Reports

Last events - all events that have been made by Antivirus displayed on this tab. Information displayed in list format.

Waredot AntiVirus

Log of past events

- USB scanning** 12:20 17.05.2021
Threats are not detected **Finished**
- EICAR.TestFile** 12:16 17.05.2021
C:\Users\Starladder\Desk...ый текстовый документ.txt **Ignored**
- Waredot Antivirus has b... successfully installed** 12:09 17.05.2021
Congratulations!

EICAR.TestFile Ignored

Threat name	EICAR.TestFile
Threat level	
Date of detection	12:16 17.05.2021
Path	C:\Users\Starladder\Desk...ый текстовый документ.txt



Scan - on this tab displays the information about scanning, when the scan was started, how long lasted the scanning, how many files were scanned, how many files have been verified as threats, how many threats was added to the quarantine, cured or removed. Information is displayed in list format.

The screenshot shows the Waredot AntiVirus application interface. On the left is a navigation sidebar with options: Back, Last events, Scan (highlighted), Threats, USB-protection, Mail-filter, and Updates. The main area is titled 'Log of past events of scanning' and displays a summary card for a 'USB scanning' event that occurred at 12:20 on 17.05.2021 and is 'Finished'. Below this, a detailed table provides the following data:

USB scanning		Finished
Time of start	12:20	17.05.2021
Took time	00:00:18	
Checked objects	1732	
Detected threats	0	
Cured threats	0	
Deleted threats	0	
Threats added to quarantine	0	

Threats - this tab displays the information about what threats were detected, date of detection, path to the threat, names of this threats and level of dangerous. Information is displayed in list format.

The screenshot shows the Waredot AntiVirus application window. The title bar reads "Waredot AntiVirus". On the left is a sidebar with a "Back" button and several menu items: "Last events", "Scan", "Threats" (which is highlighted), "USB-protection", "Mail-filter", and "Updates". The main content area is titled "Log of past events with threats". It displays a single event for "EICAR.TestFile" detected at "12:16 17.05.2021" at the path "C:\Users\Starladder\Desktop\...ый текстовый документ.txt" with a status of "Ignored". Below this, a detailed view of the threat is shown in a box, listing: Threat name (EICAR.TestFile), Threat level (Ignored), Date of detection (12:16 17.05.2021), and Path (C:\Users\Starladder\Desktop\...ый текстовый документ.txt).

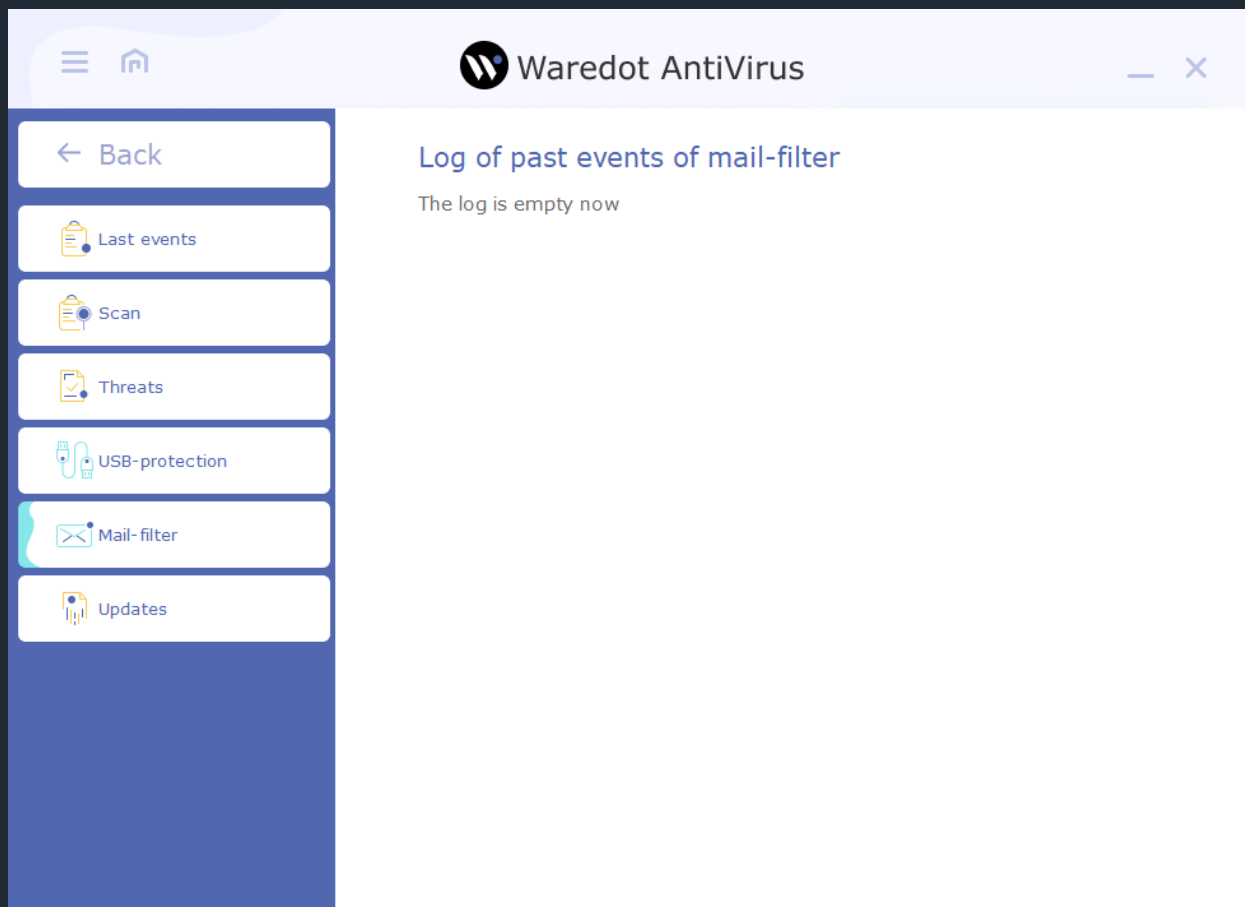


USB-protection - this tab displays the information about scanning USB pen drives, when the scan was started, how long lasted the scanning, how many files were scanned, how many files have been verified as threats, how many threats was added to the quarantine, cured or removed. Information is displayed in list format.

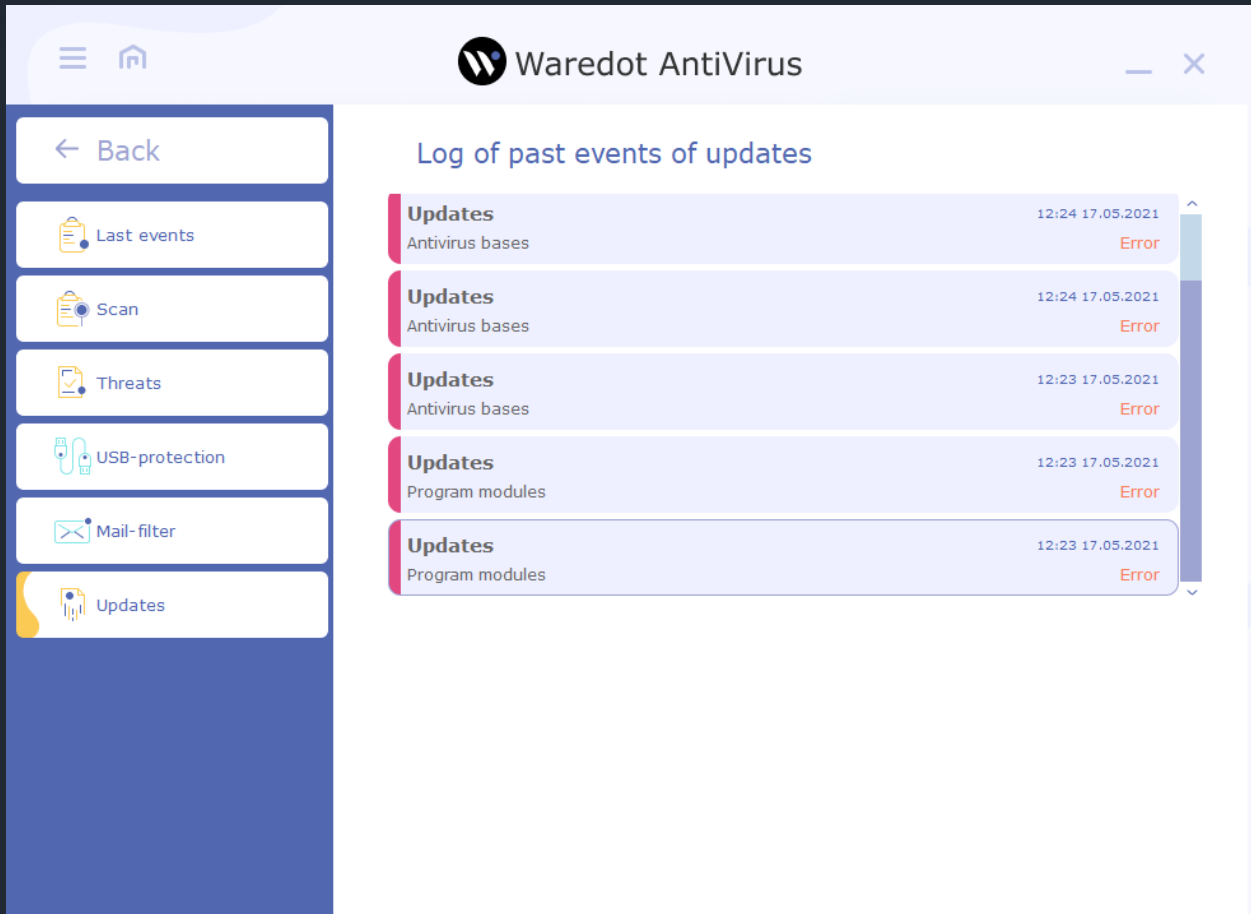
The screenshot shows the Waredot AntiVirus interface. On the left is a navigation sidebar with options: Back, Last events, Scan, Threats, USB-protection (highlighted), Mail-filter, and Updates. The main area is titled 'Log of past events of USB-protection' and shows a summary card for a 'USB scanning' event that occurred at 12:20 on 17.05.2021, with the status 'Finished' and the message 'Threats are not detected'. Below this is a detailed table for the same event.

USB scanning		Finished
Time of start	12:20	17.05.2021
Took time	00:00:18	
Checked objects	1732	
Detected threats	0	
Cured threats	0	
Deleted threats	0	
Threats added to quarantine	0	

Mail-filter - this tab displays the information about the letters in which attachments were detected threats. Antivirus scans only letters in the mail clients (like The Bat, Outlook Express, Mozilla Thunderbird, etc.) rather than in a web browser. Information is displayed in list format.



Update - this tab displays the information (last date and version) about updates of antivirus program modules and AV Bases. Information is displayed in list format.

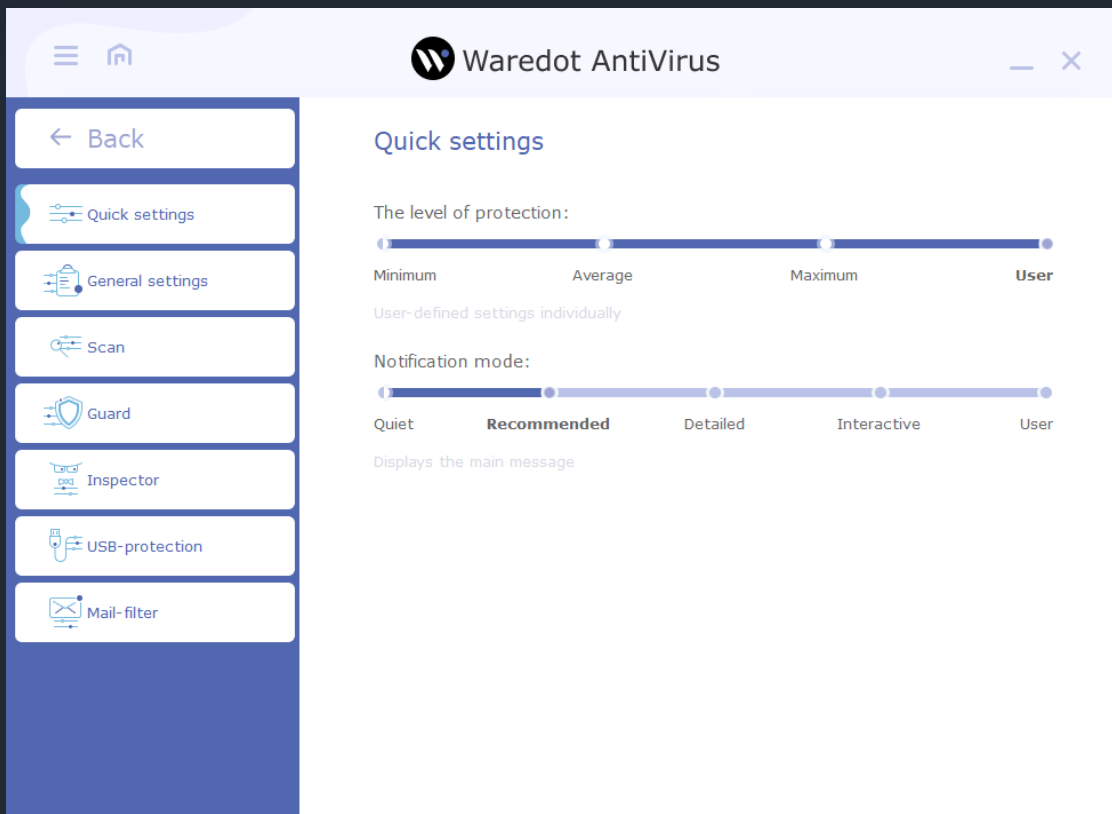


Settings of Waredot Antivirus

User can set up Waredot Antivirus in two mode: Quick settings and Advanced settings.

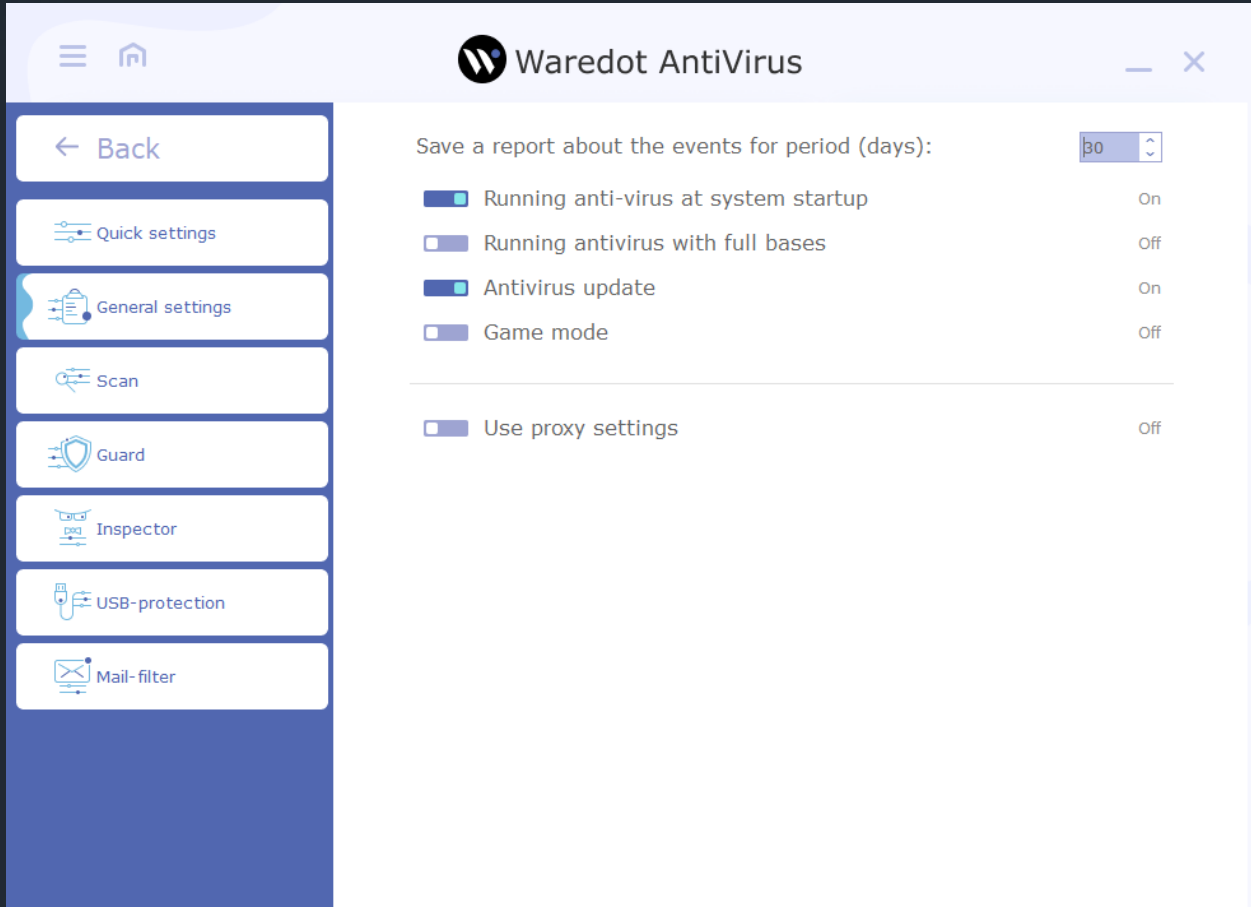
In the **Quick settings mode** are available such settings:

1. Settings of The level of protection:
 - Minimum – provides a minimum essential levels protection;
 - Average – provides an optimal protection;
 - Maximum – provides a highest possible level of protection;
 - User – provides a level of protection according to the settings which were set by user.
2. Settings of **Notification mode**:
 - Quite – messages are not displayed;
 - Recommended – show the main messages;
 - Detailed – show all messages;
 - Interactive – all messages are displayed in the dialogue with the user;
 - User – displays only messages which were turned on by users.



Advanced settings include General settings and settings for every Protection module.

General settings – allow you to set up such thing as: the starting order of antivirus; showing splash; downloading antivirus with full database; game mode; proxy server settings etc.



Scan - allows you to set up the settings for all types of scan such as:

Archive Files – scan all types of archive files like .iso, .rar, .zip, .msi etc.

Heuristic Analyzer - analyzes the software code for its match against viruses.

Boot sectors – scan the boot sectors on every drive.

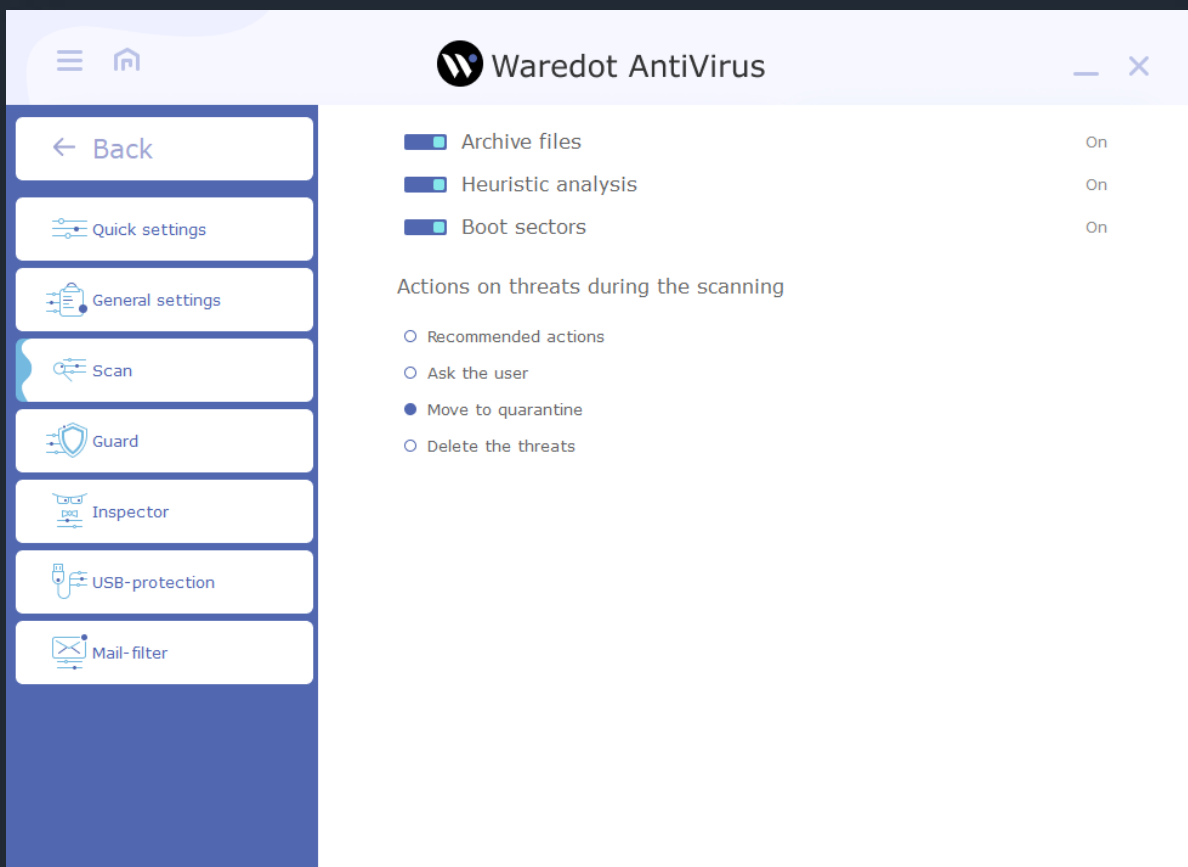
Actions on threats during the scanning:

Recommended Actions – apply the action which are optimal according to our base of actions for threats;

Ask the User – ask the user about the needed action for every detected threat;

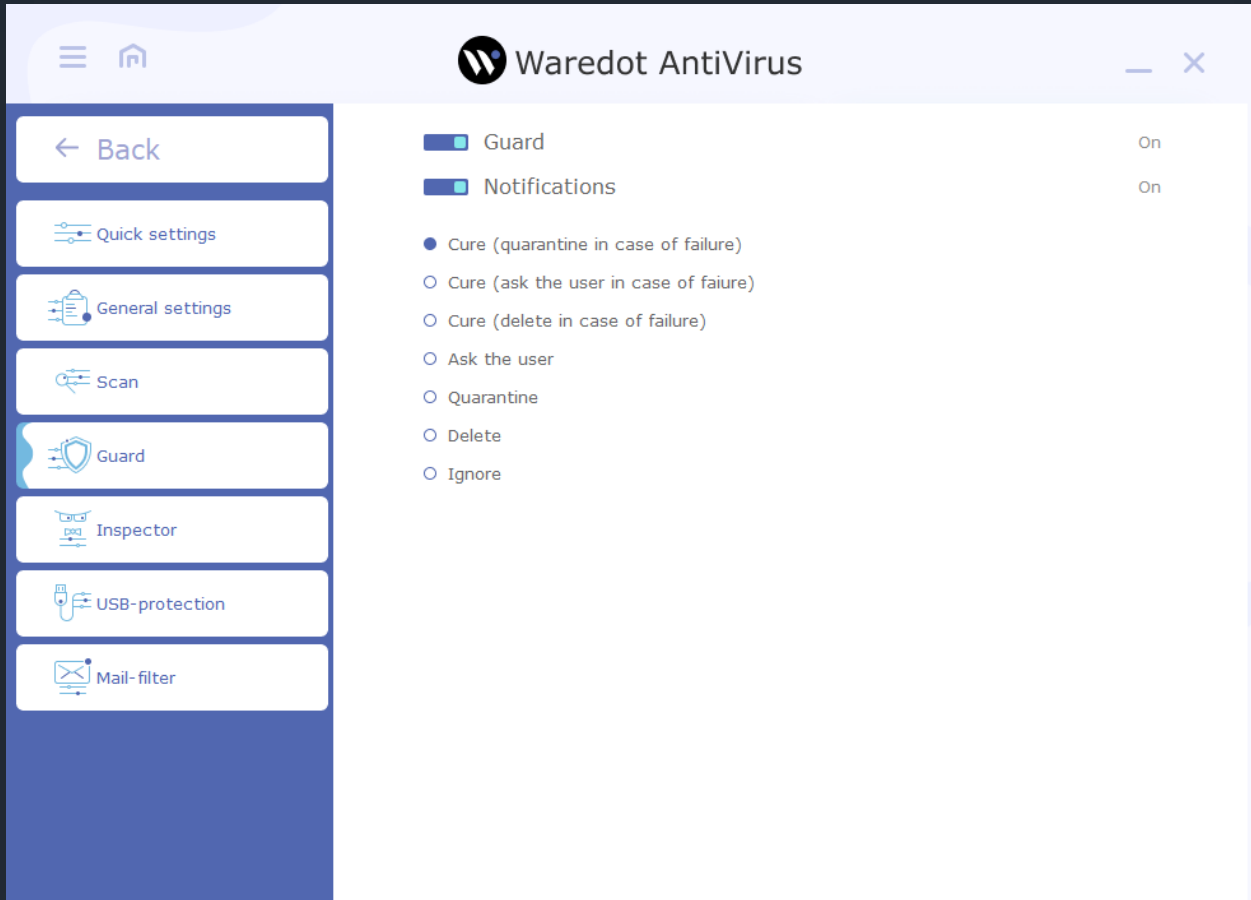
Move to Quarantine – move all detected threats to quarantine of Waredot Antivirus;

Delete the Threats – delete all detected threats from the PC.



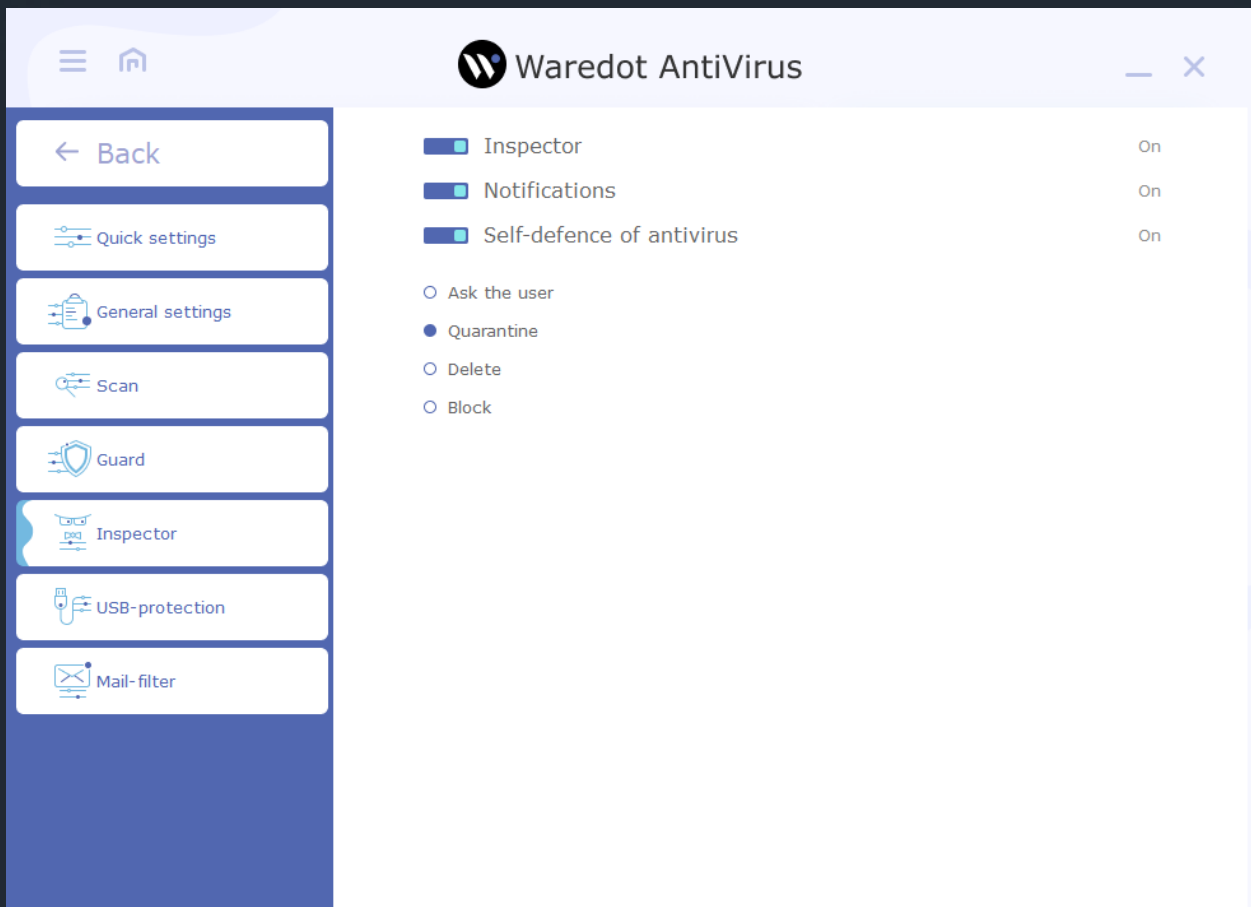
Guard (File Monitor) - continuously monitors the system for threats.

In the Settings on Guard tab user can turn on or turn off the scanning of the files and processes in the real time; turn on and turn off the notifications of it; set and change the default action for the detected threats.



Inspector security (Behavioral analyzer) - monitors the programs installed on your computer to identify malicious activity.

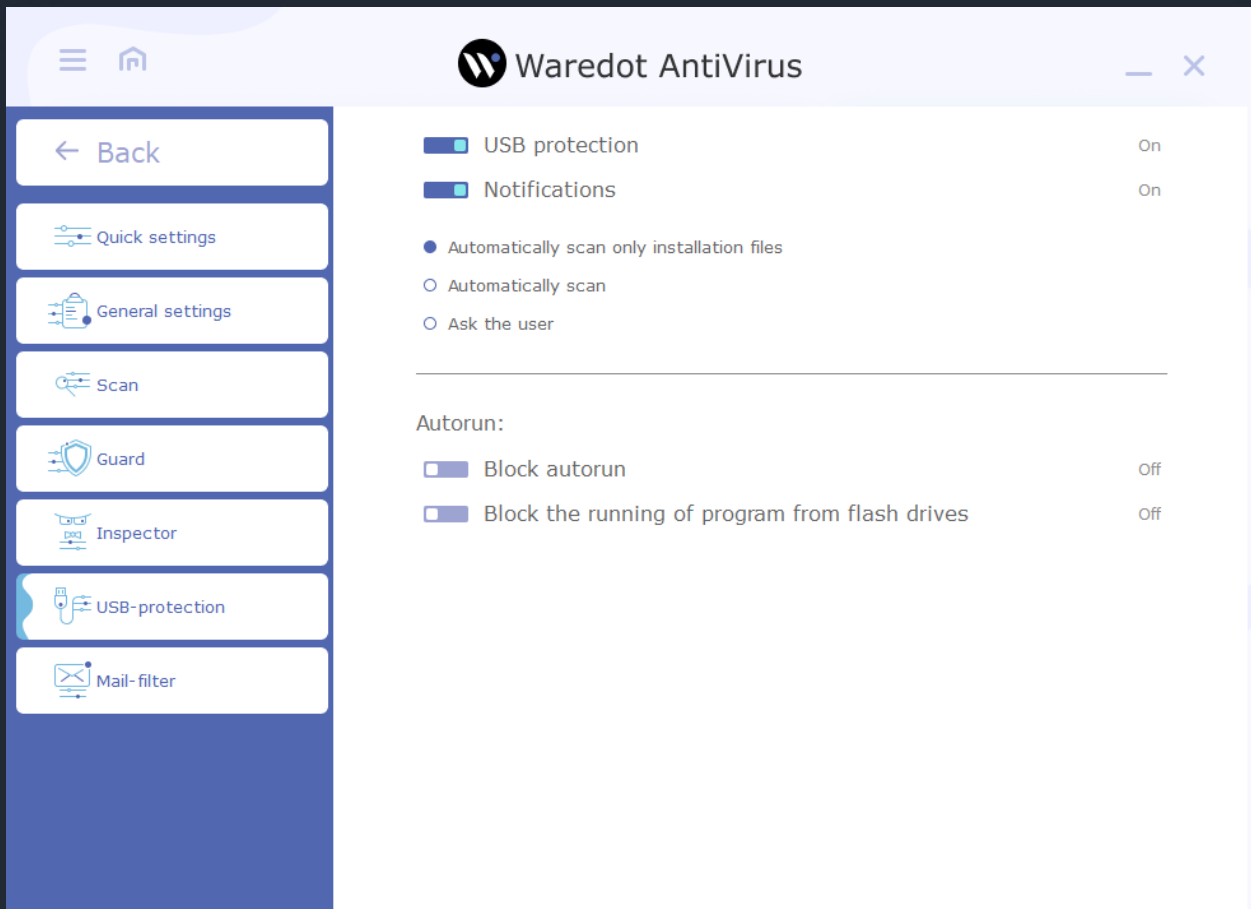
In the Settings on Inspector tab user can turn on or turn off the monitoring of the behavior of the files and programs in the real time; turn on and turn off the notifications of it; turn off and turn on Antivirus self-defense; set and change the default action for the detected threats.



USB – protection - makes penetration of virus threats via removable drives impossible.

In the Settings on USB – protection tab user can turn on or turn off the scanning of the USB pen drives after connecting them to the PC; turn on and turn off the notice of this module and set the default settings for the USB pen drives which were connected to the PC.

In this tab users may set the actions for the files and program which have the parameter “Autorun” and start automatically after connecting the USB pen drives to the PC.

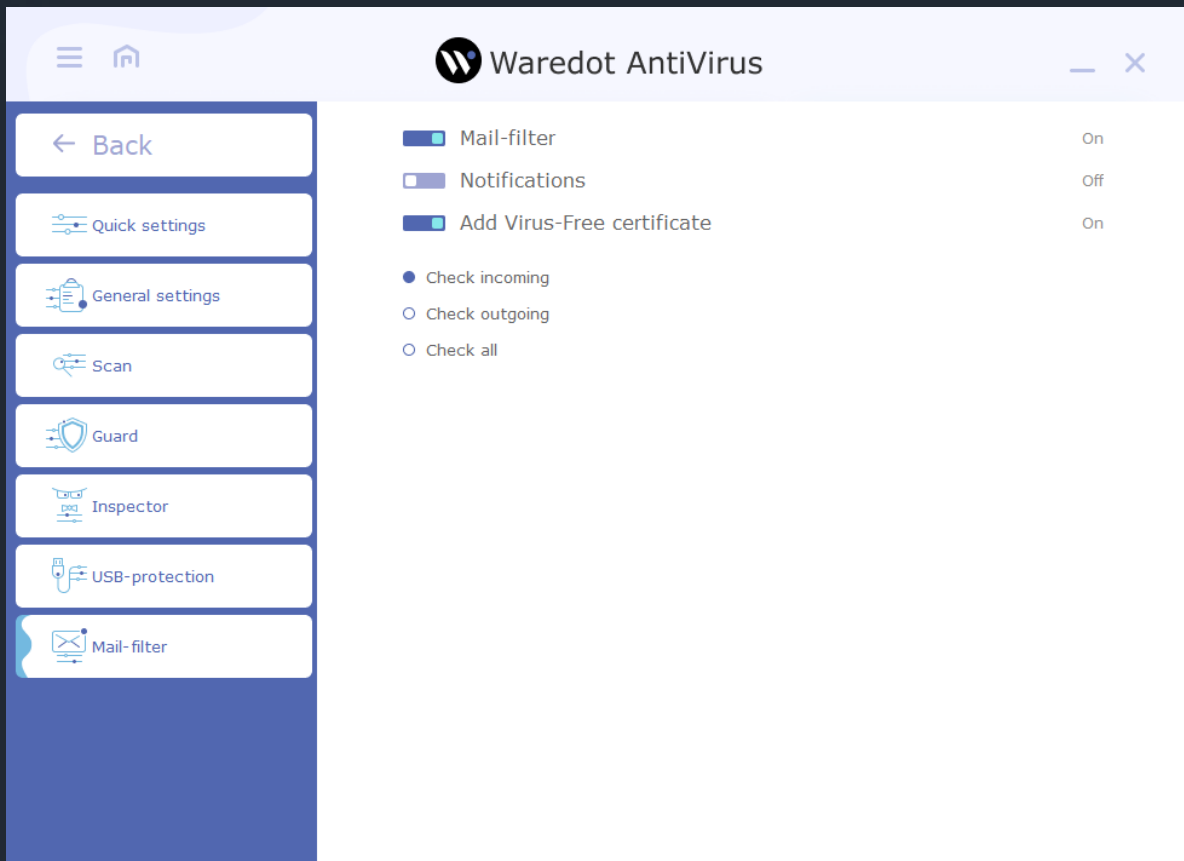


Mail – Filter - scans email for threats.

In the Settings on Mail – filter tab user can turn on or turn off the scanning of the emails for the threats and malware in the real time; turn on and turn off the notice of this module and addition the Virus-Free certificate for the emails which were checked by the Waredot Antivirus.

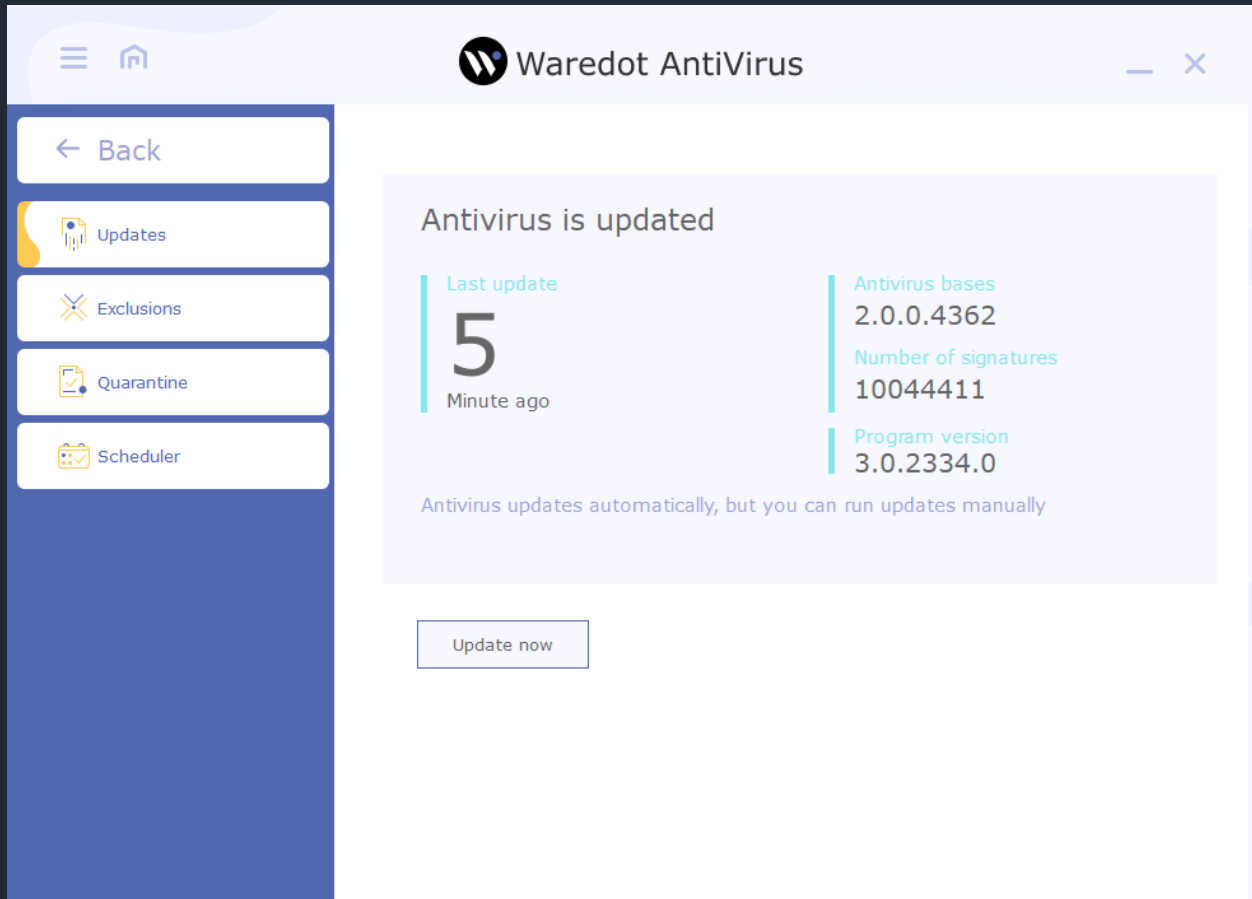
In this tab users may set the actions for the Mail – filter:

- **Check Incoming** – set the scanning of the emails which user receive to his / her email client from the other users only.
- **Check Outgoing** - set the scanning of the emails which user send from his / her email client to the other users only.
- **Check all** - set the scanning of all emails which user receive and send via his / her email client for the other users.



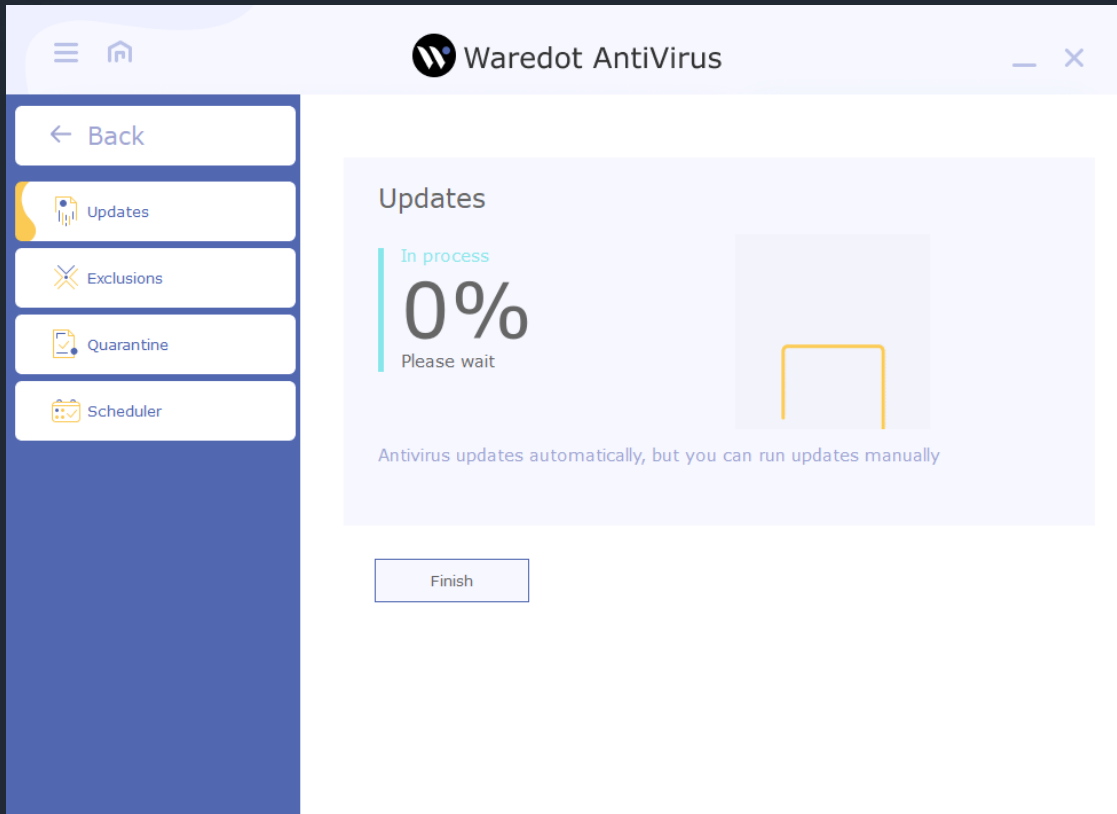
Databases and Program Modules Updates

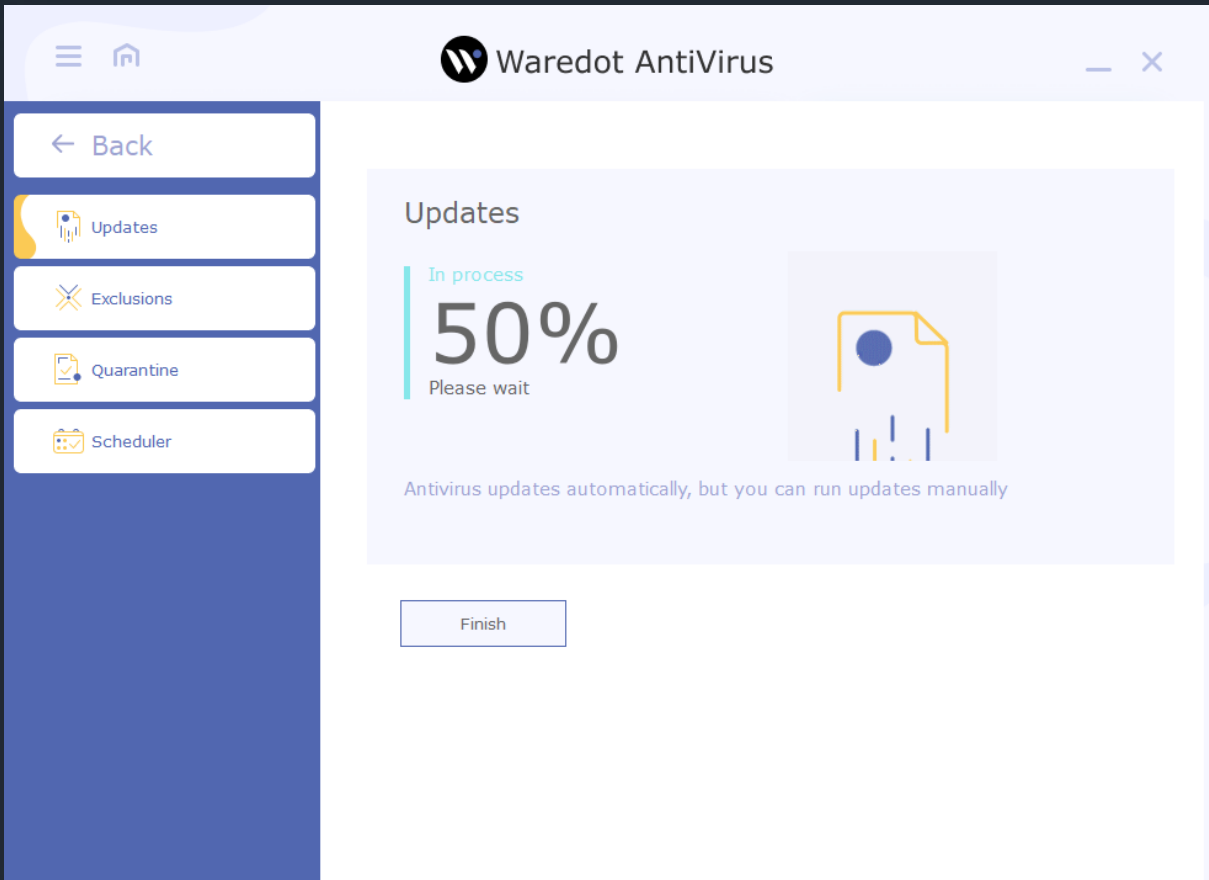
The effectiveness of antivirus product depends on how regularly virus databases are updated. Regular automatic update of databases is critically needed to keep the optimal level of protection of your computer.

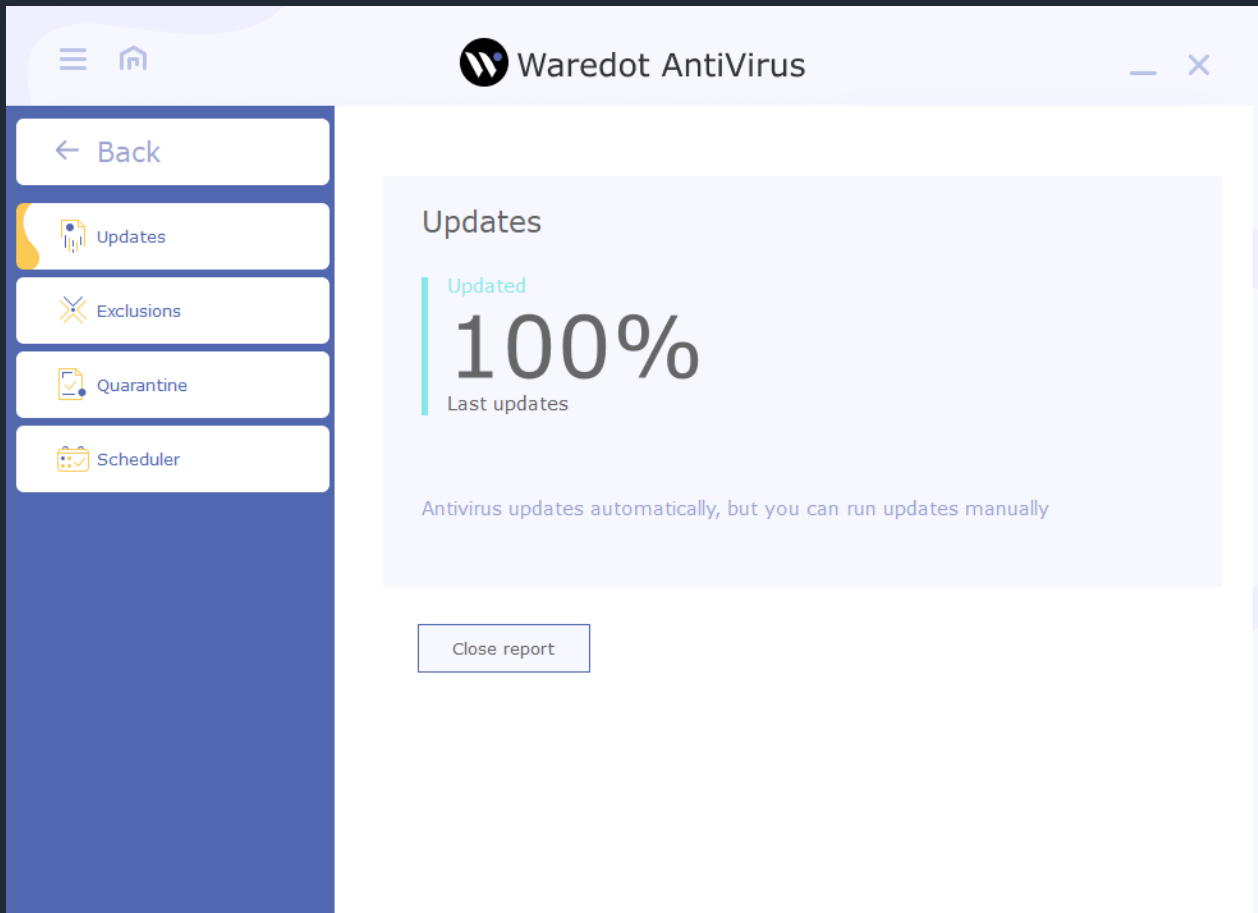


Updating takes place in two stages:

- Updating of virus databases (0 - 50%)
- Updating of program modules (51% - 100%)







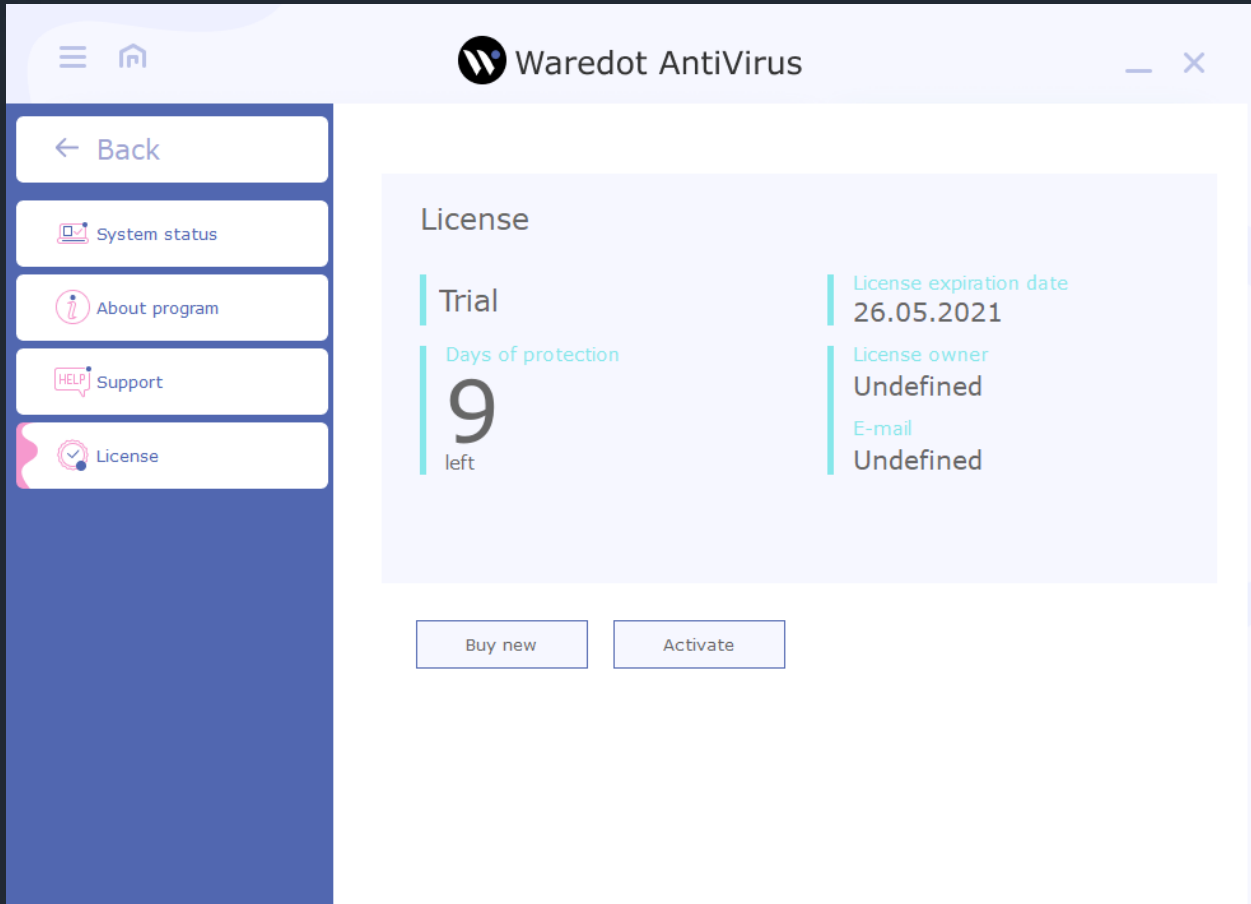
Specialists of our Antivirus Laboratory promptly react to new threats, update the antivirus bases and bases of malware. Typically, virus updates are issued 1-2 times a day. In case of epidemics our Antivirus Laboratory prepares updates in accelerated mode to protect users.

For users who do not have regular access to the Internet, it is possible to use off-line updates of antivirus.

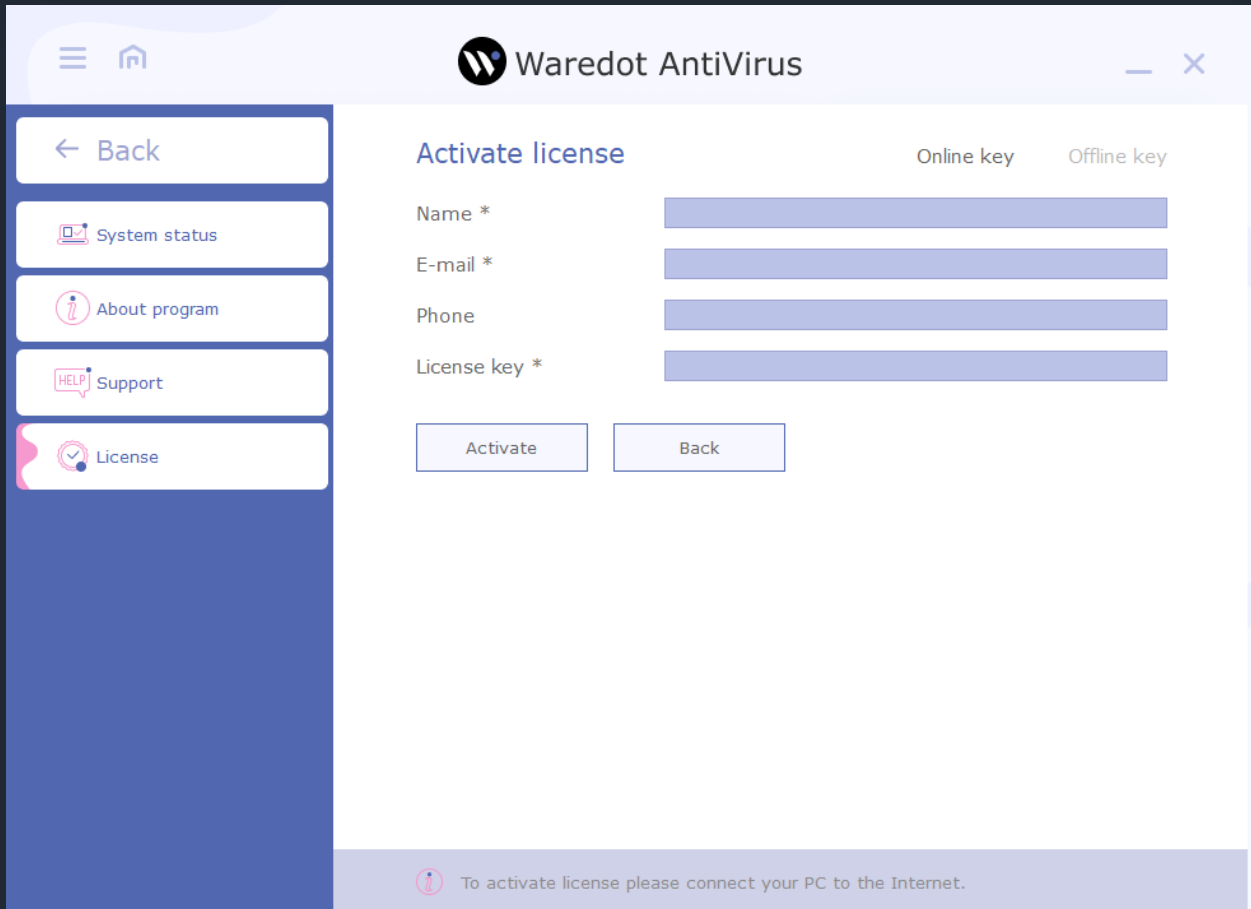


Waredot Antivirus Registration

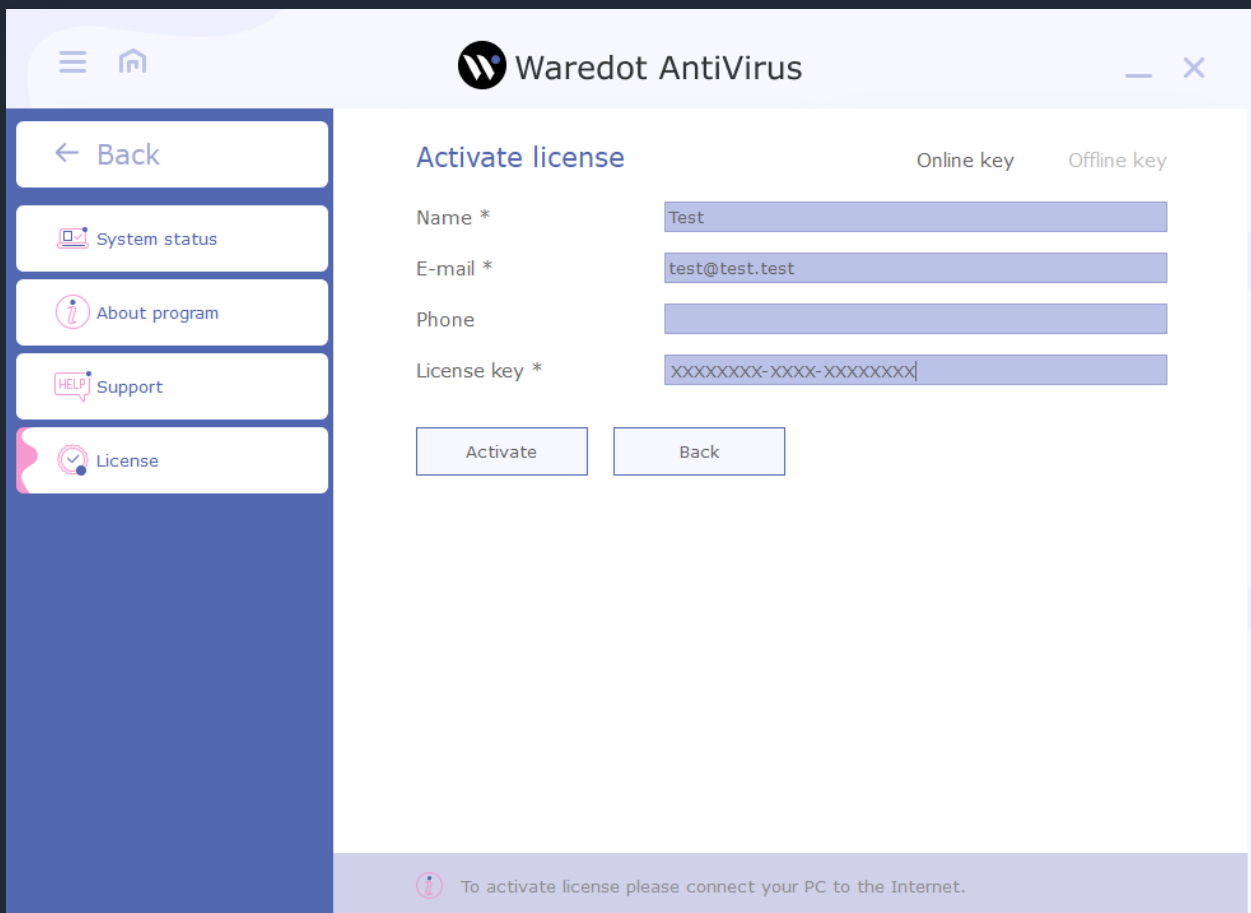
This is how unregistered program window looks like:



To register the program, open the main window of Waredot Antivirus, go to the tab “License” and click “Activate” button or “Buy new” if you need to buy the new License:



Enter your data and License key and click "Activate" button:



Waredot AntiVirus

← Back

System status

About program

Support

License

Activate license

Online key Offline key

Name * Test

E-mail * test@test.test

Phone

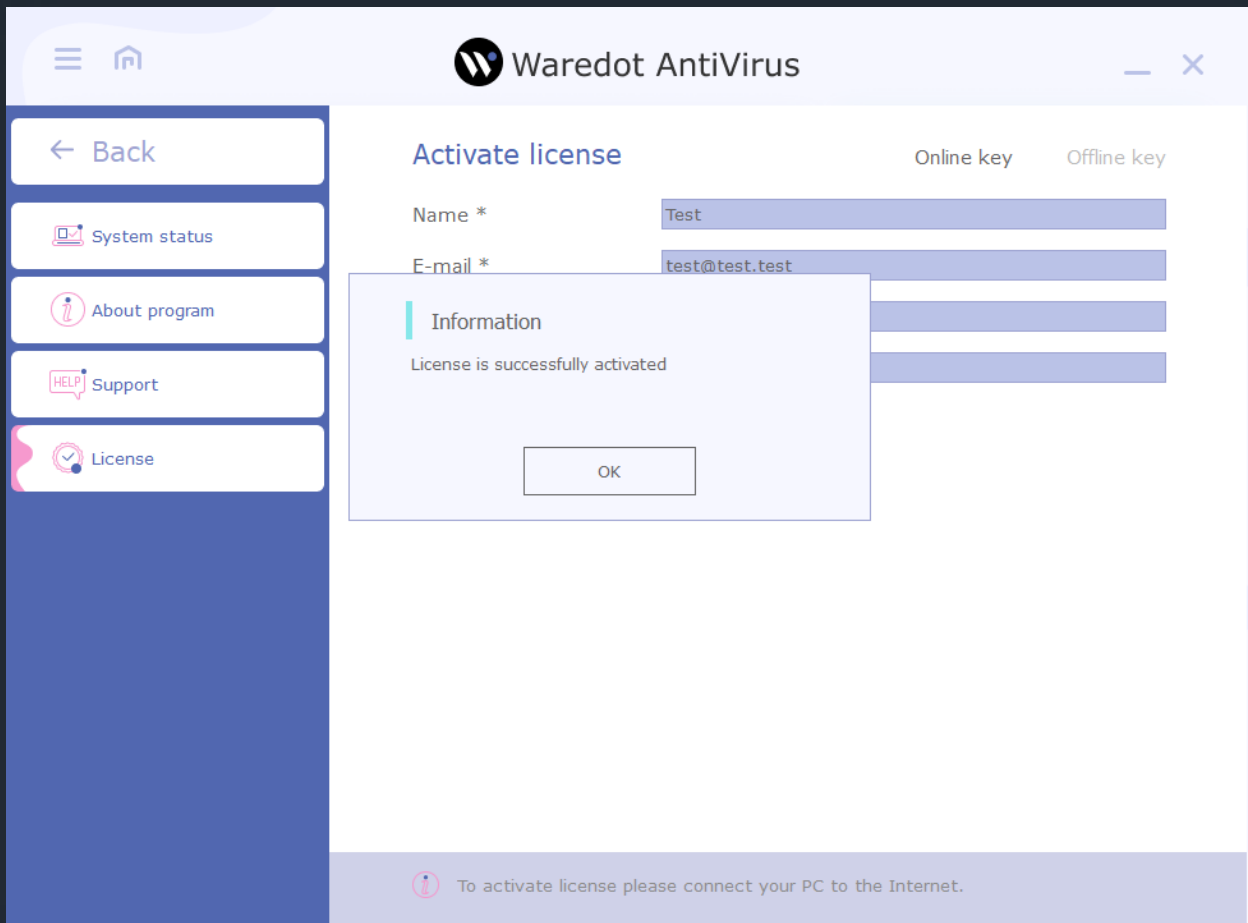
License key * XXXXXXXX-XXXX-XXXXXXXX

Activate Back

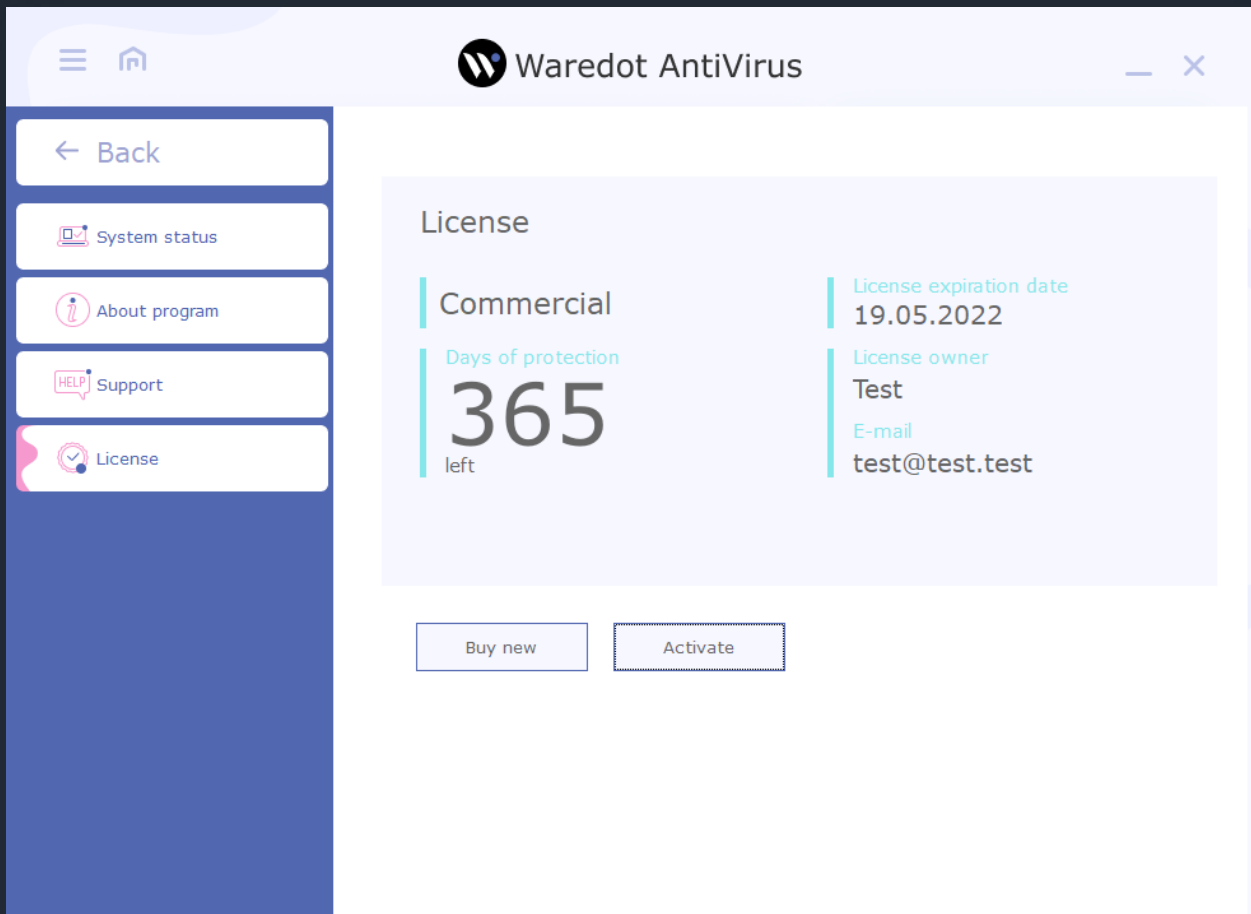
To activate license please connect your PC to the Internet.



Waredot Antivirus will inform you about the result of activation of your License:



This is how the window of successful registered program looks like:

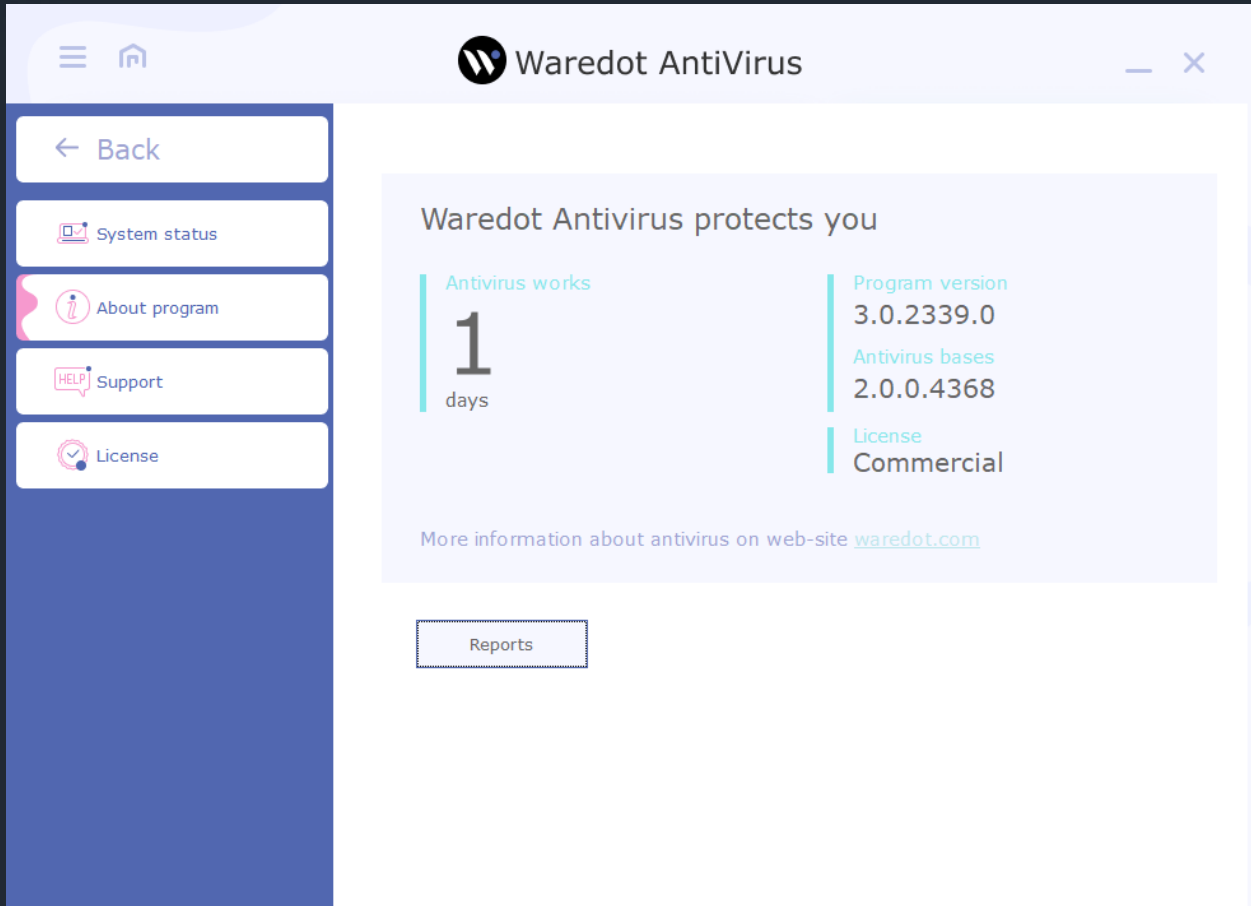


It is also possible to activate Waredot Antivirus on the PC without internet access. To do this, you need to select the "offline key" right at the top of antivirus windows. The activation process is identical to the online activation. The only difference will be the key length - 96 symbols.



About Program

On this tab you can see basic information about the program. Here is information about duration of the protection of this PC with Waredot Antivirus, the version of its software modules and antivirus bases, and also specified license type (commercial or trial).



From the License tab user can go to Reports of Waredot Antivirus by clicking the button Reports.

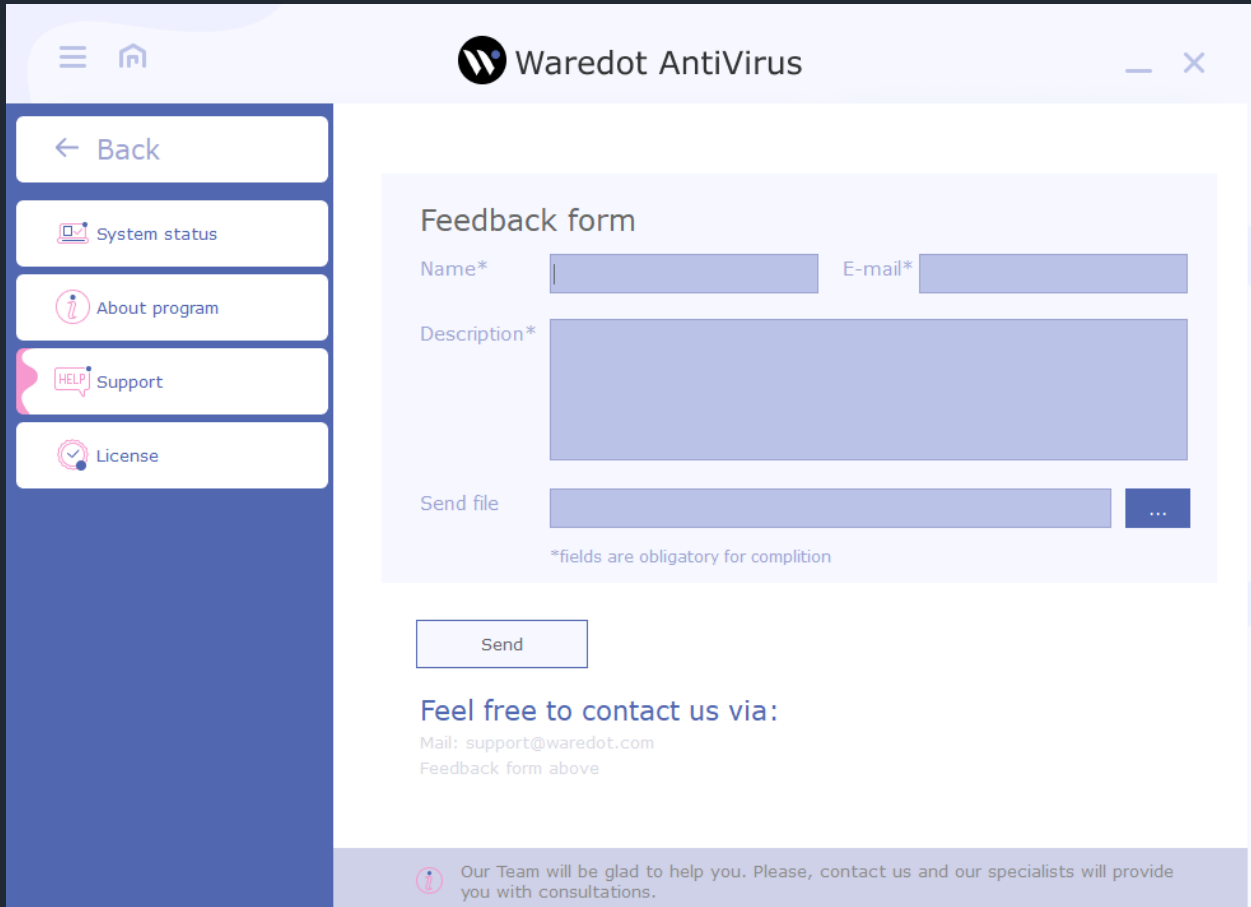


Customer Support

If you have any questions about Waredot Antivirus you can contact our Customer support service.

You can use the following methods:

- E-mail – support@waredot.com
- Fill in the request form to customer service.



The screenshot shows the Waredot AntiVirus application window. The title bar reads "Waredot AntiVirus". On the left is a navigation sidebar with buttons for "Back", "System status", "About program", "Support" (highlighted), and "License". The main content area displays a "Feedback form" with the following fields: "Name*" (text input), "E-mail*" (text input), "Description*" (text area), and "Send file" (file input with a dropdown menu). A note below the form states "*fields are obligatory for completion". A "Send" button is located below the form. Below the button, it says "Feel free to contact us via:" followed by "Mail: support@waredot.com" and "Feedback form above". At the bottom, a footer message reads: "Our Team will be glad to help you. Please, contact us and our specialists will provide you with consultations."

