



Waredot Ultimate

USER GUIDE

CONTENTS

Introduction	3
Waredot Ultimate System Requirements	4
Installation of Waredot Ultimate	5
System Status	10
System Scanning	14
When Waredot Ultimate finds the threats	18
Modules of the antivirus protection	20
Modules of the Network protection	28
Tools	39
Reports	55
Settings of Waredot Ultimate	61
Databases and program modules updates	71
Waredot Ultimate registration	74
Customer support	80

Introduction

Dear user!

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

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

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



Waredot Ultimate System Requirements

Minimal system requirements for Waredot Ultimate:

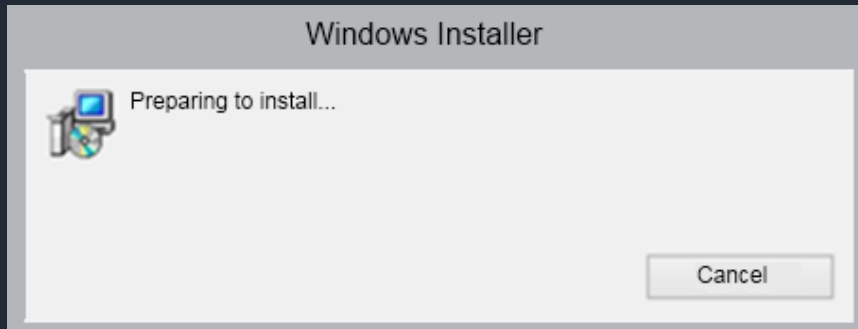
Processor frequency:	1 GHz or higher
RAM:	1 GB or more
Hard disk space:	450 Mb
Operating system:	Windows 7 (x32, x64) (SP1), Windows 8 (x32, x64), Windows 10 (x32, x64)
Screen resolution	1024 x 768 or higher



Installation of Waredot Ultimate

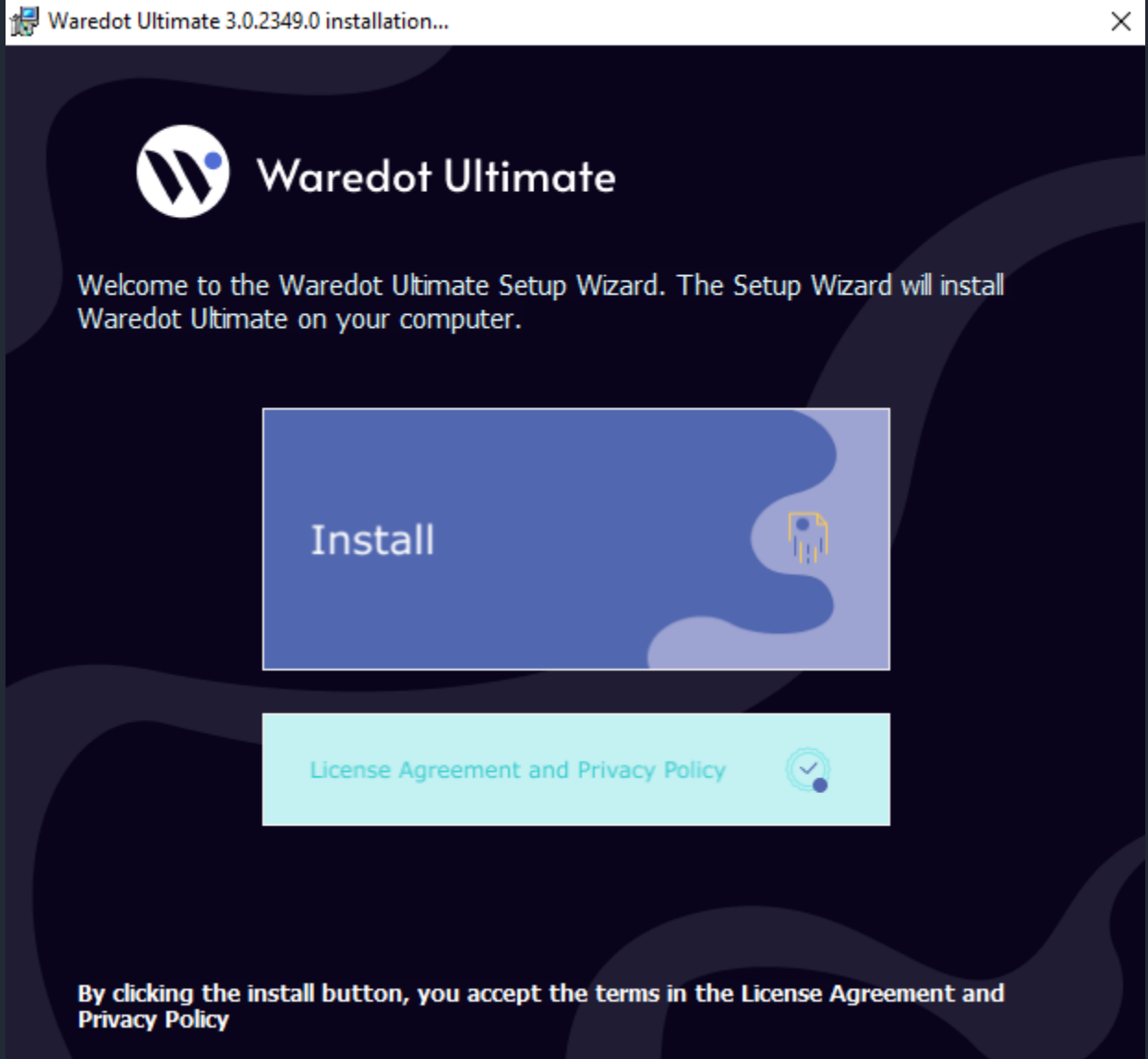
Proper installation of Waredot Ultimate is provided by Waredot Ultimate Installation Wizard. You just need to follow the wizard.

Preparing to install



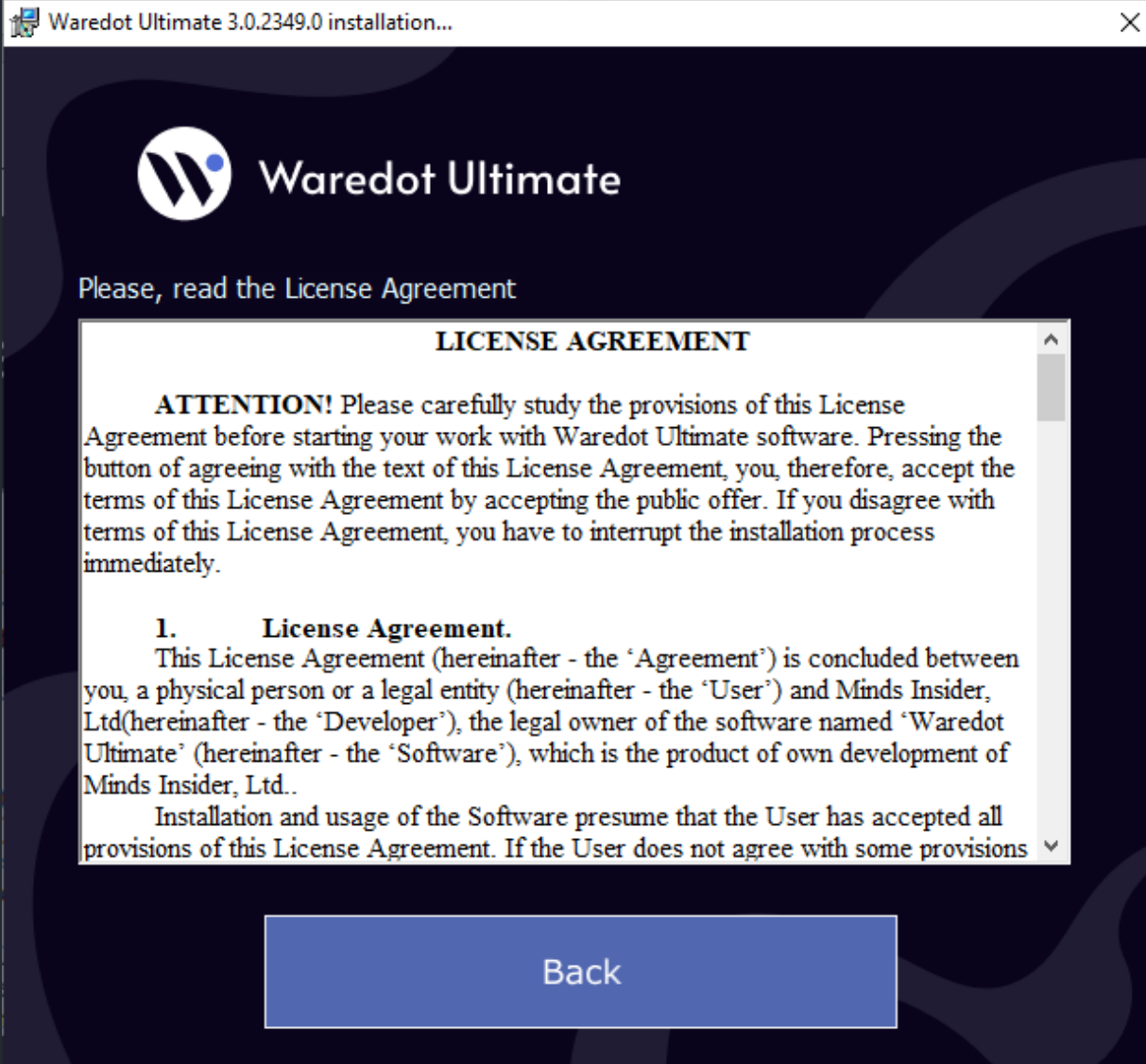
After you will see a Wizard that will install ProtoDefense Internet Security on your PC. The “Install” button will run immediate installation. By clicking the “Install” button you automatically agree with the License agreement.





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 ProtoDefense Internet Security with other antivirus software can cause to system errors. We recommend you to delete all other antivirus programs manually before installing of ProtoDefense Internet Security.

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.



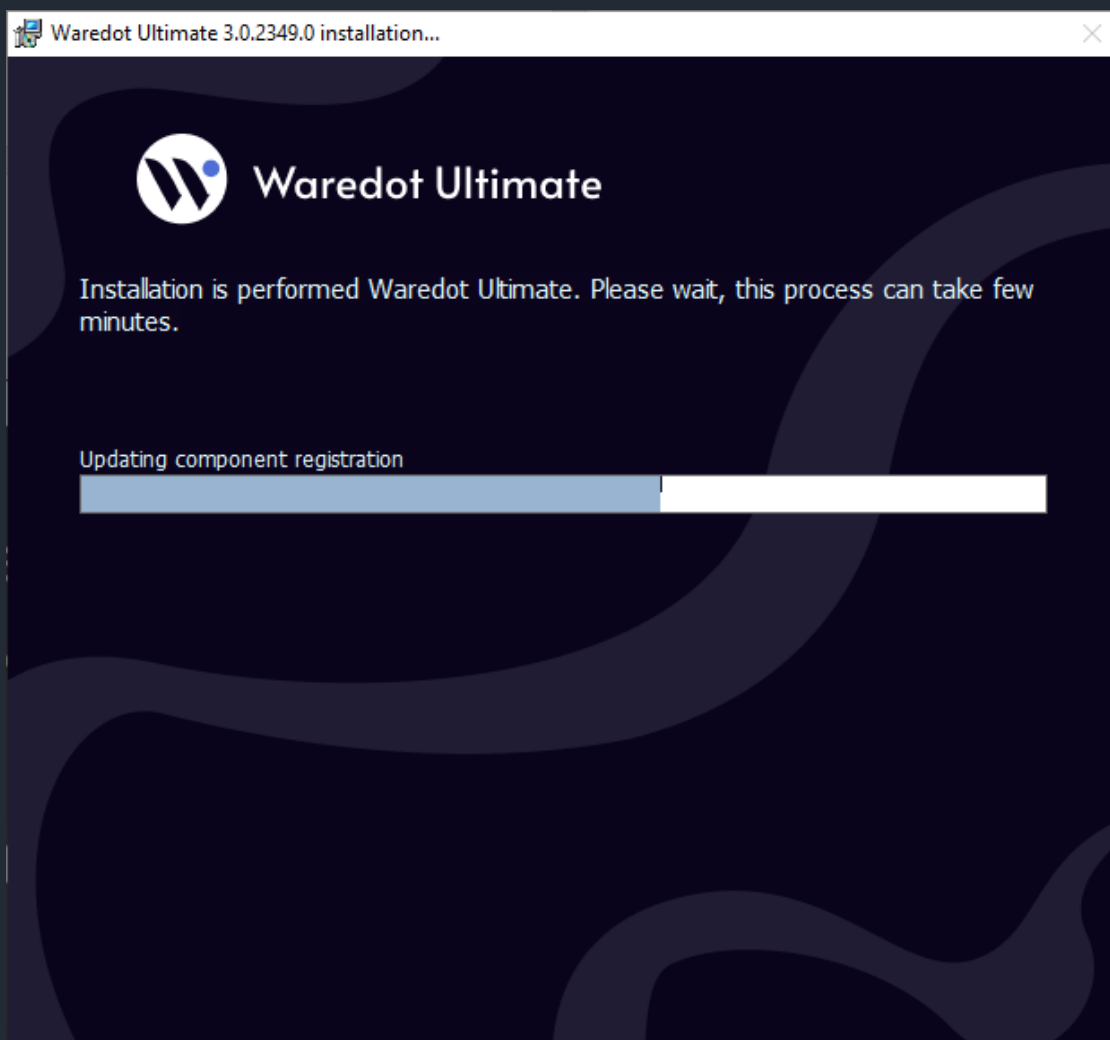
Also, before installing ProtoDefense Internet Security you should remove its previous version.

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

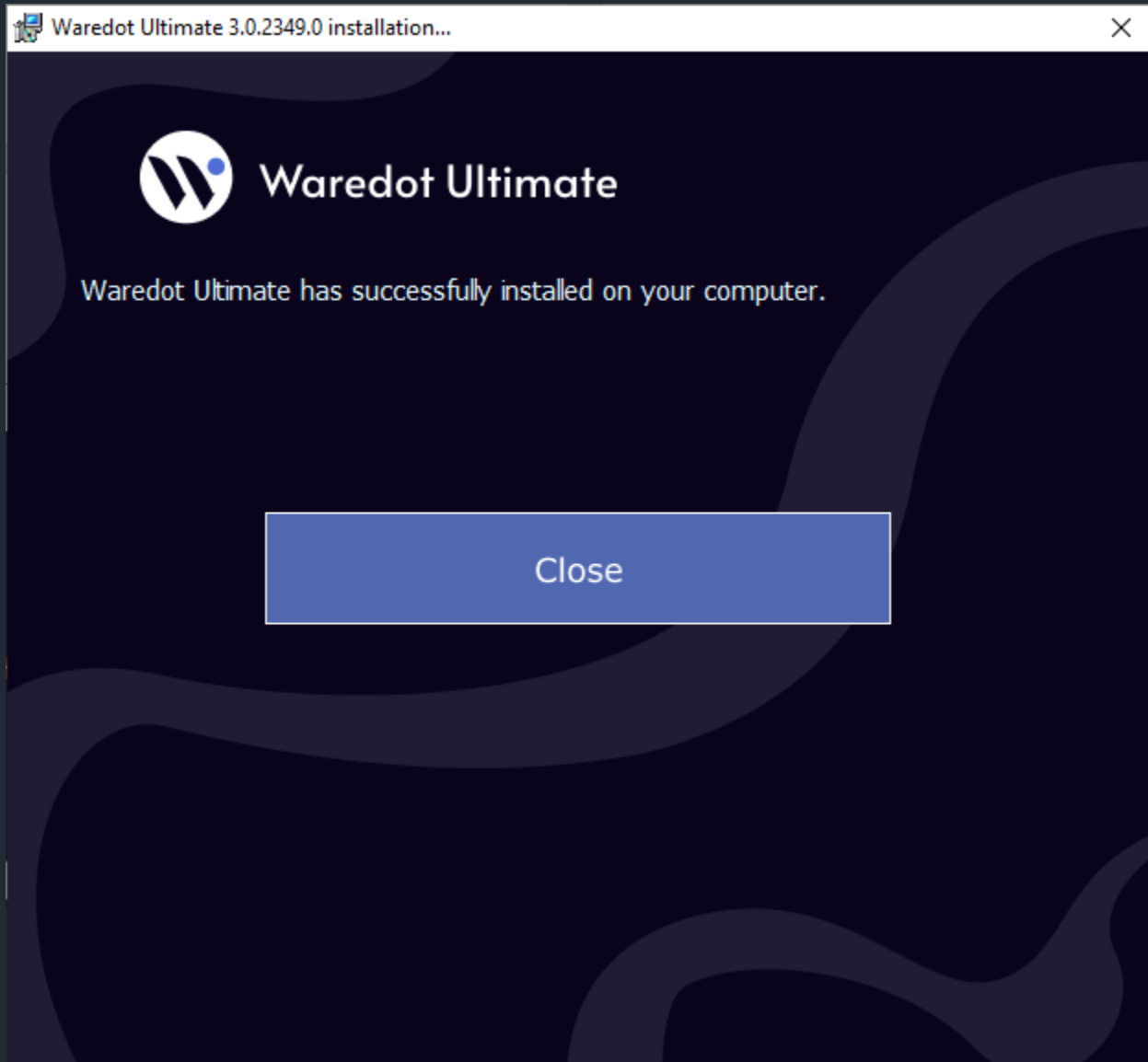
1. Click **Start**, click **Control Panel** and double-click **Add or Remove Programs**.
2. Select an antivirus program to be deleted in the list of installed programs and click **Remove**.
3. For implementation of changes follow the instructions on screen.

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.



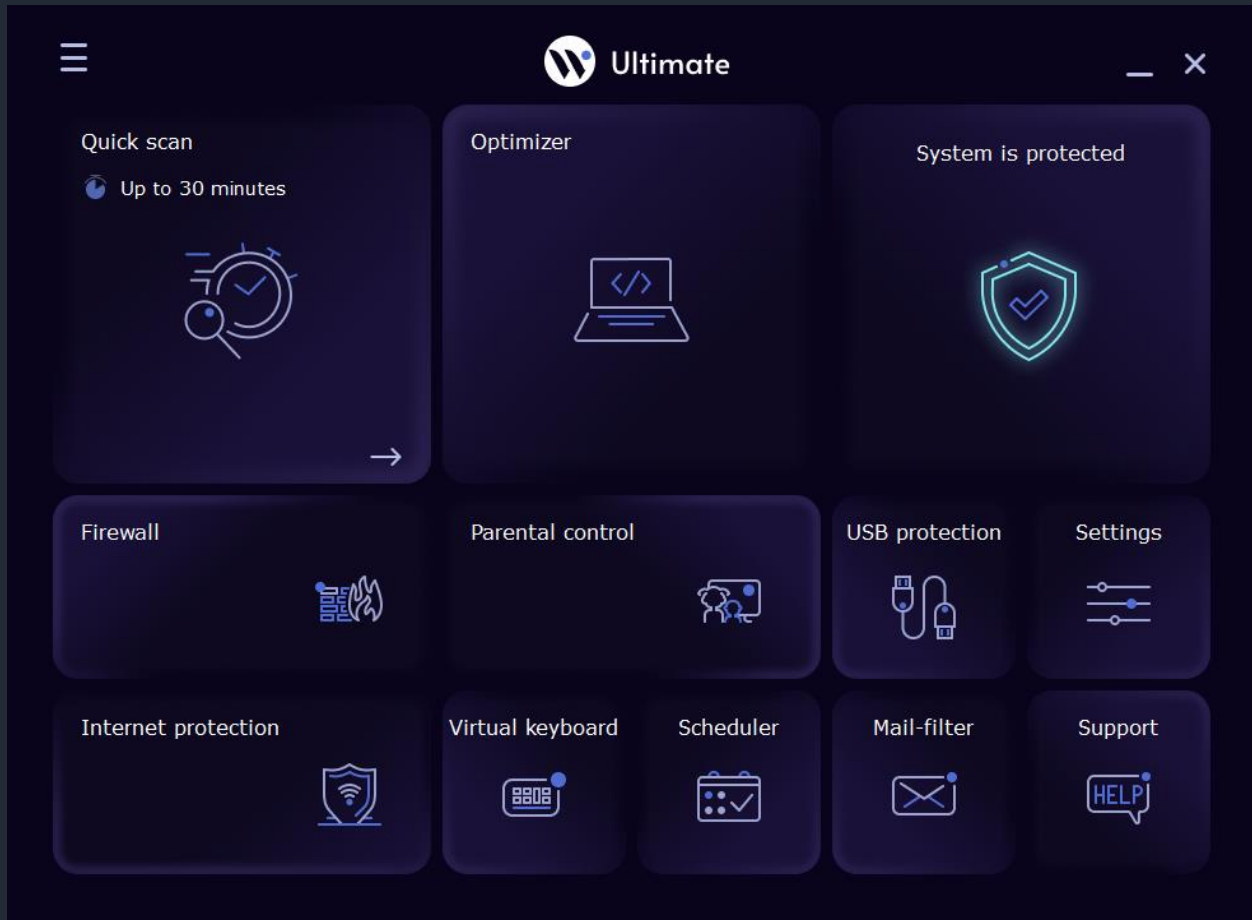
After successful completion of the installation process you will see a window with the next message. Click "Close" button to complete install and run the program.



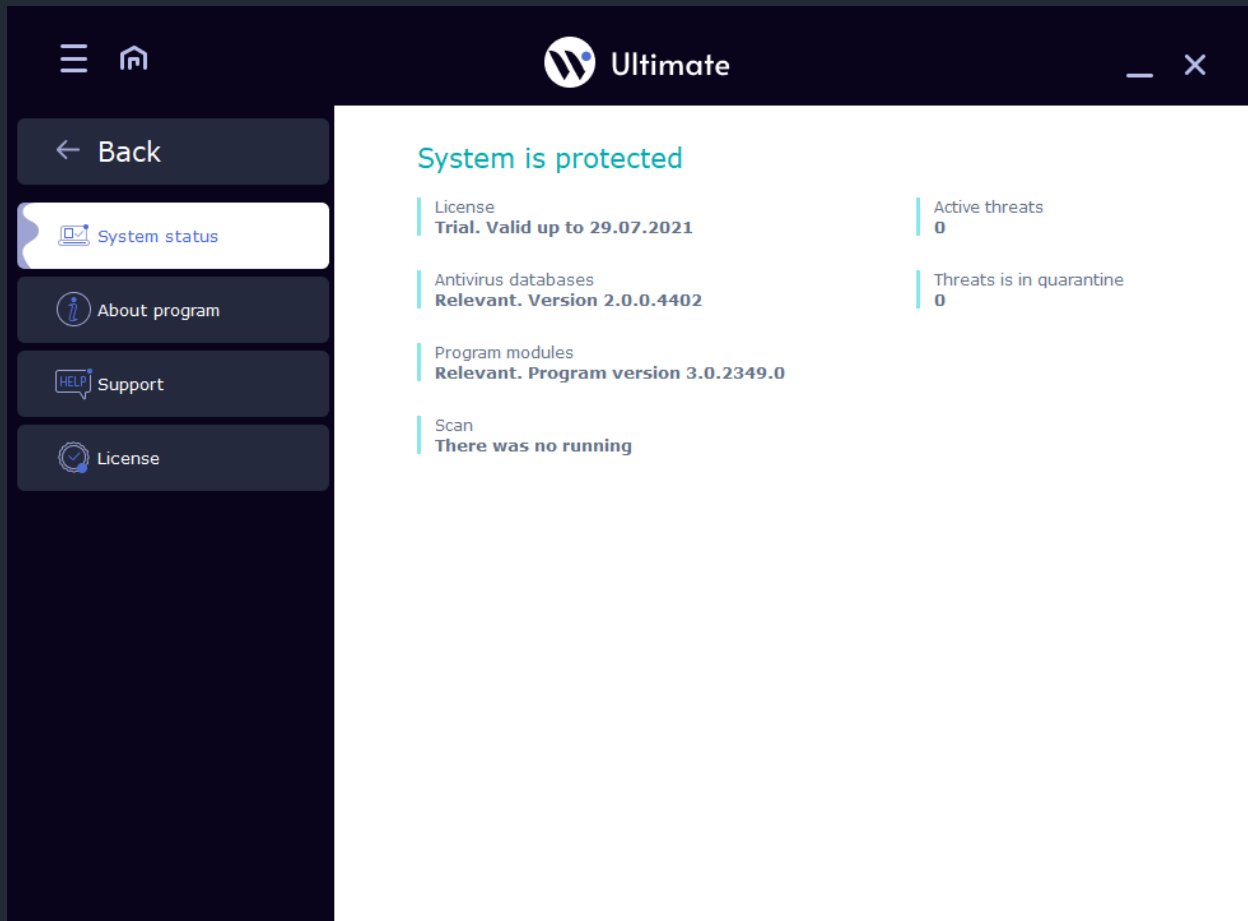
System Status

Waredot Ultimate 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:

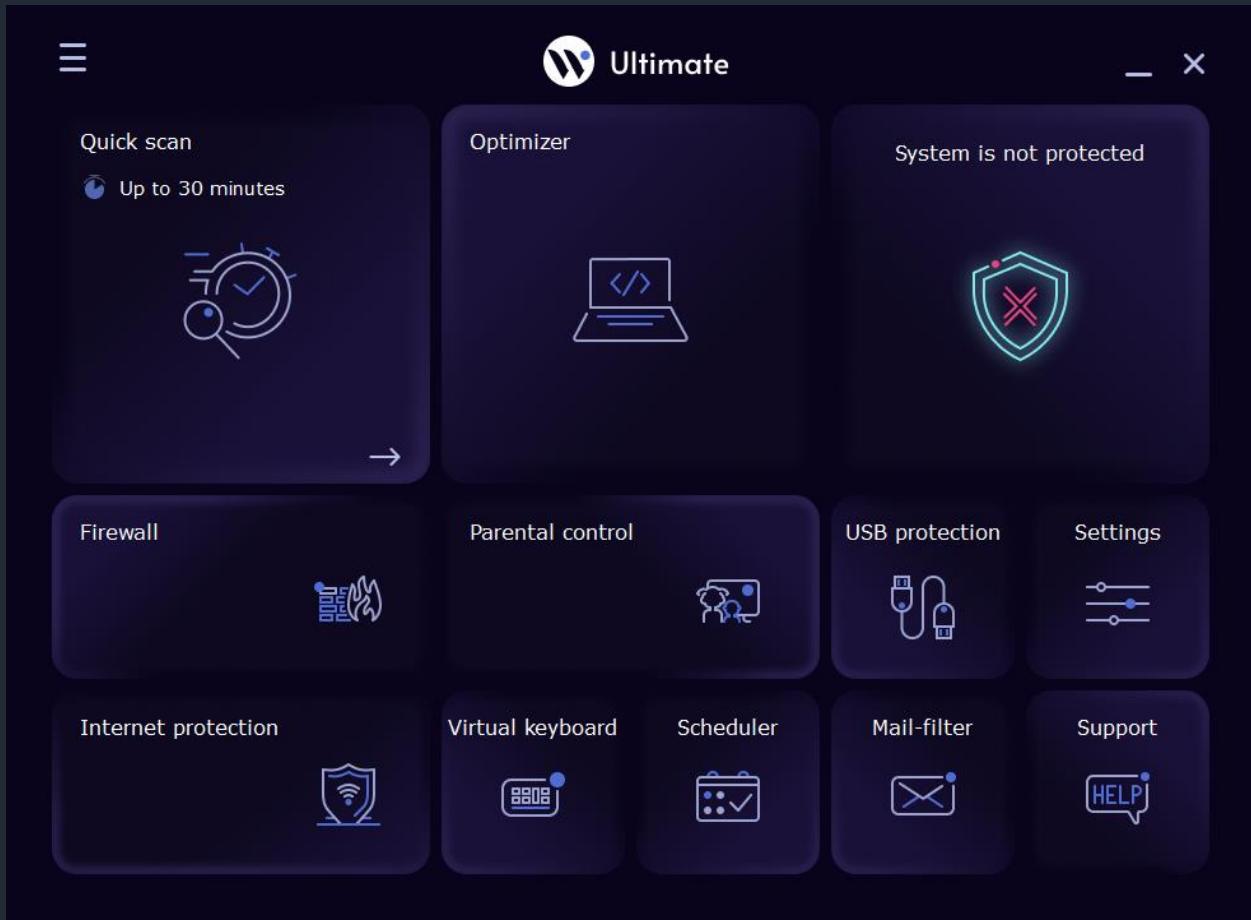


Graphical representation of the system status is presented by Waredot Ultimate in 2 colors.

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.



Red 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:

System is not protected

License
Trial. Valid up to 29.07.2021

Active threats
0

Antivirus databases
Relevant. Version 2.0.0.4402

Threats is in quarantine
0

Program modules
Relevant. Program version 3.0.2349.0

Scan
There was no running

Issue 1 / 1

Guard

Guard is necessary for real-time protection of your system. Perhaps you turned it off yourself. We recommend you turn Guard on for full protection of your PC.

To turn Guard on click on "Fix" at the bottom of the window or turn it in the settings of program.

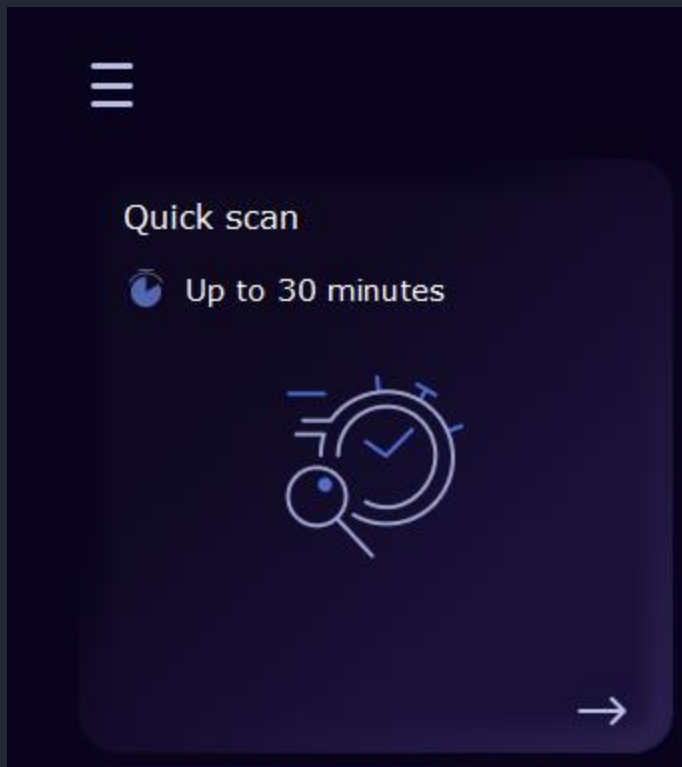
Detailed Resolve

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

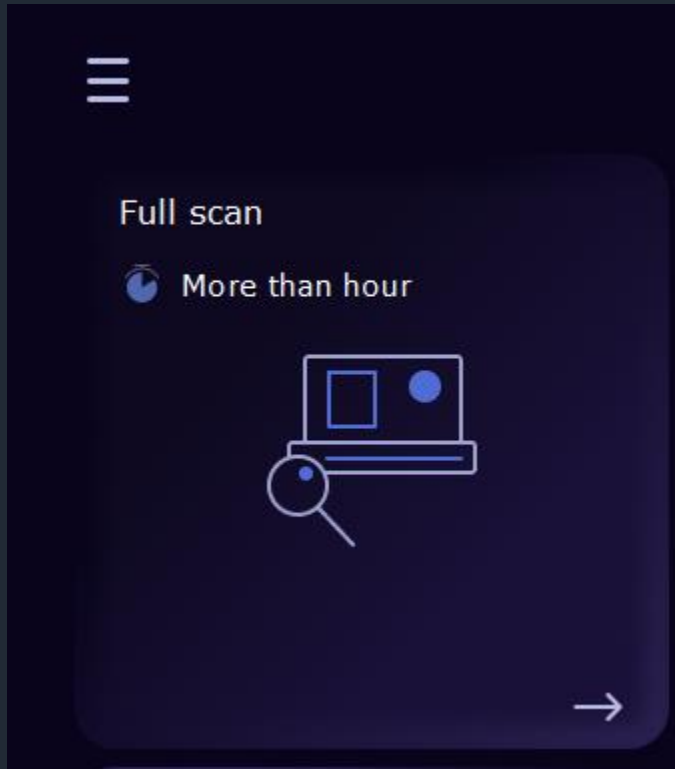
Waredot Ultimate has three scan modes which are available in the main window: **Quick**, **Full** and **Custom Scan**. Each set is provided with certain parameters of the mode. You can choose type of Scan using pointer in the right corner at the bottom of the Scan button.

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.

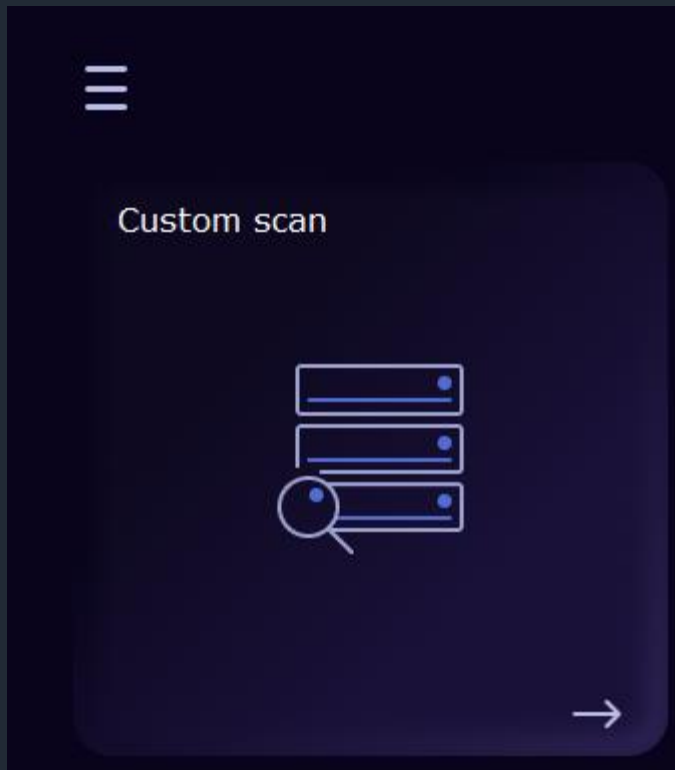


Full Scan – total system check. Thorough scanning of the system. The following items are scanned: system memory, objects that run on startup, backup storage systems, mail bases, hard and removable drives.

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.

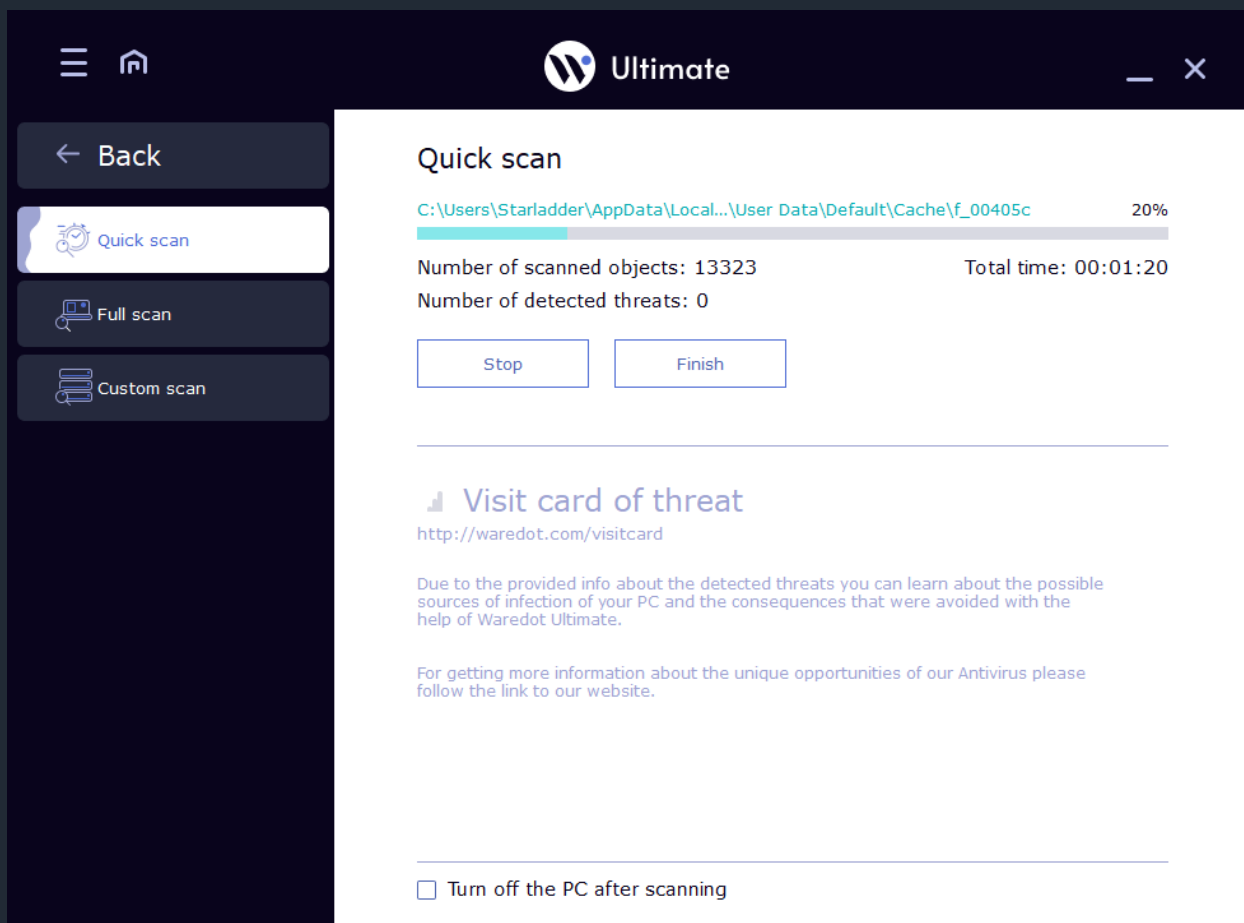


After the scan will be complete you will receive a report with its results: total time of scanning and detailed information about the number of scanned and infected objects.

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



When this process be completed, Waredot Ultimate 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 Ultimate:

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.

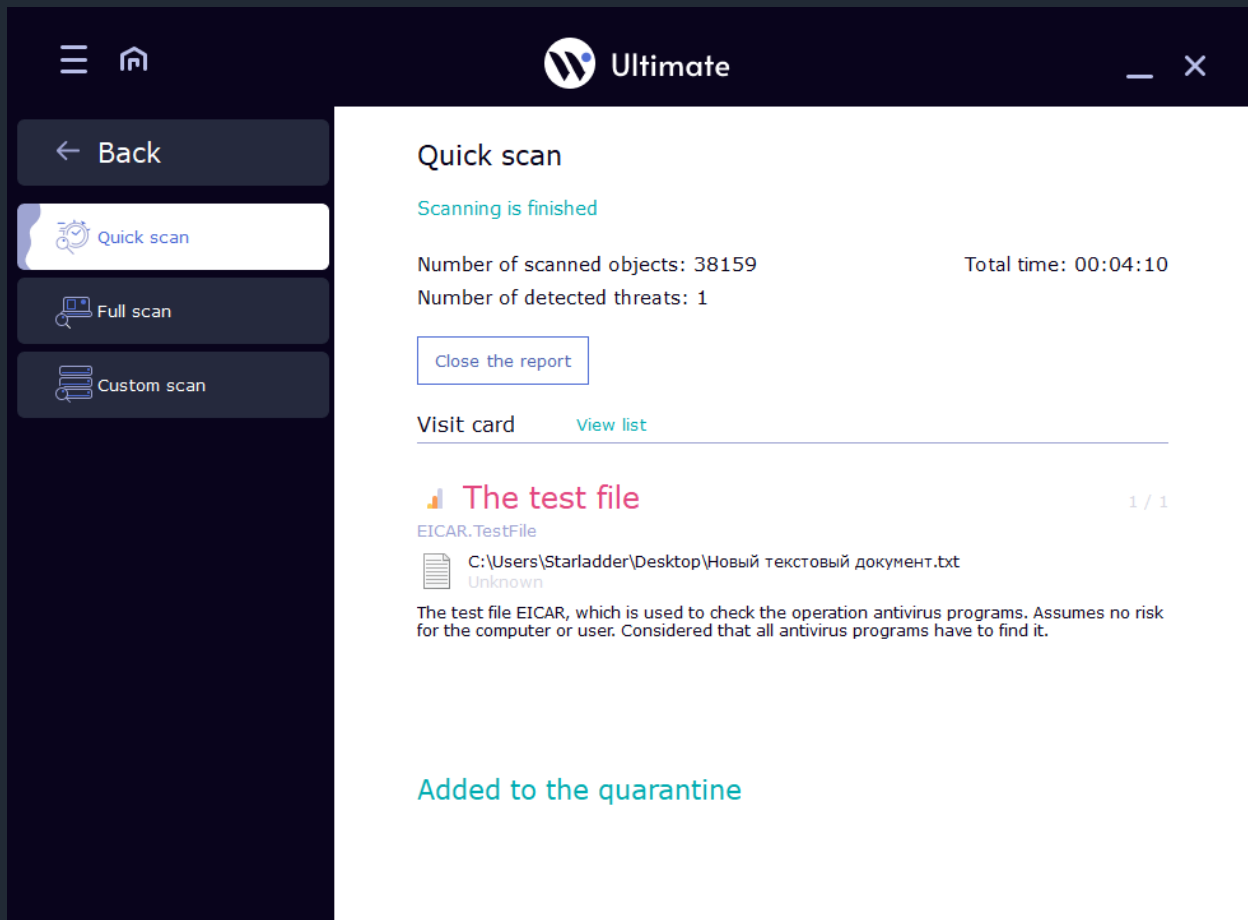
If you do not have time or you do not want to wait for the scan is complete, you can use an option that is placed at the bottom of the window – "Turn off the PC after scanning."



When Waredot Ultimate Detects Threats

Waredot Ultimate 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 Ultimate 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 Ultimate 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 Ultimate and stays in Active threats until user will choose and apply the other action for this threat. If Waredot Ultimate 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 Ultimate is turned on this PC.

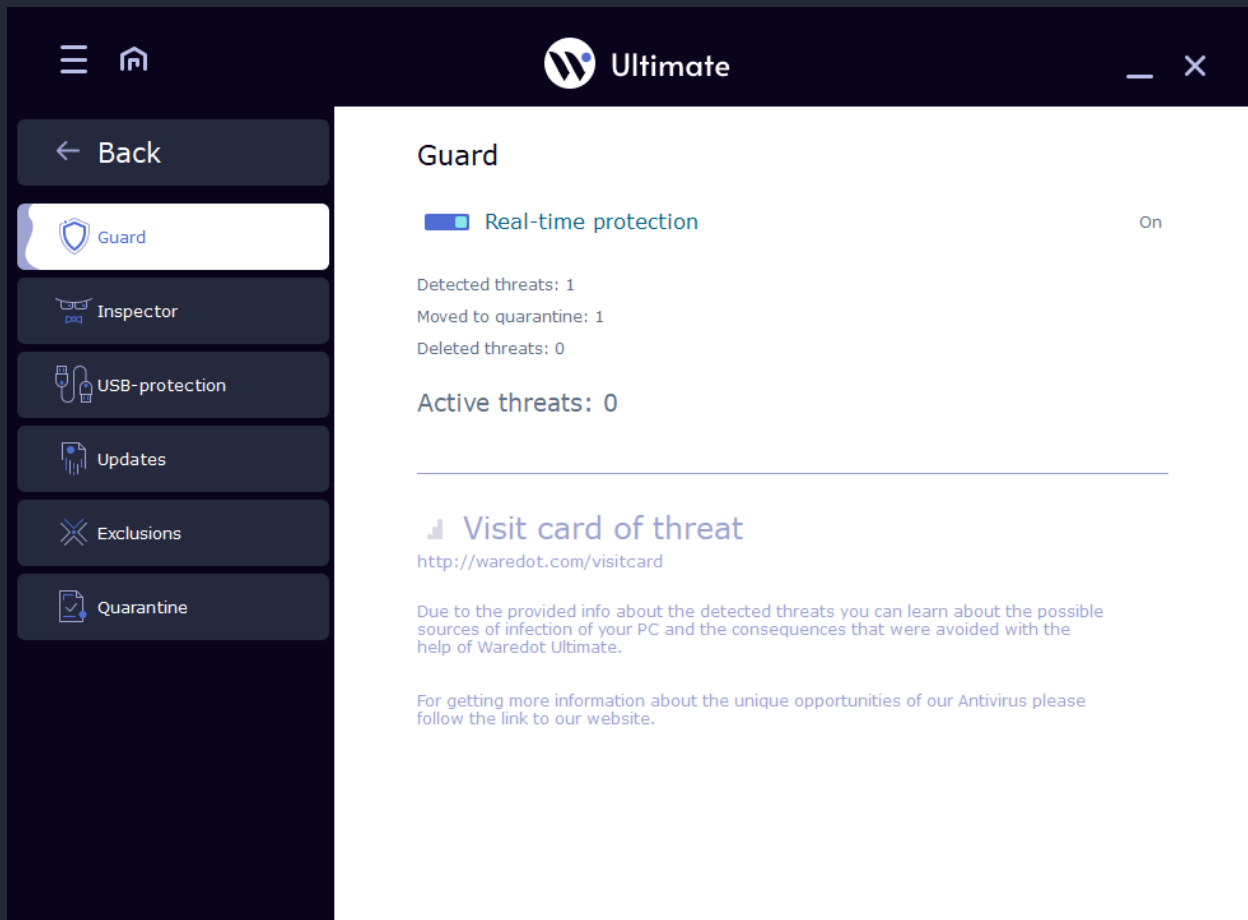
Delete – this action initializes the deleting of the infected file or threat. After deleting user will not be able to restore this file. If user may use this infected file, we recommend to user to apply the action Quarantine to this file and keep these file in Quarantine until it will be needed. Before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



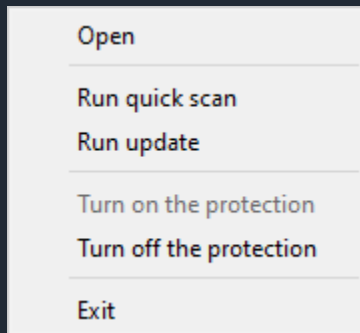
Modules of the Antivirus Protection

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 Ultimate icon in the taskbar notification area or go to the item Turn on the protection.

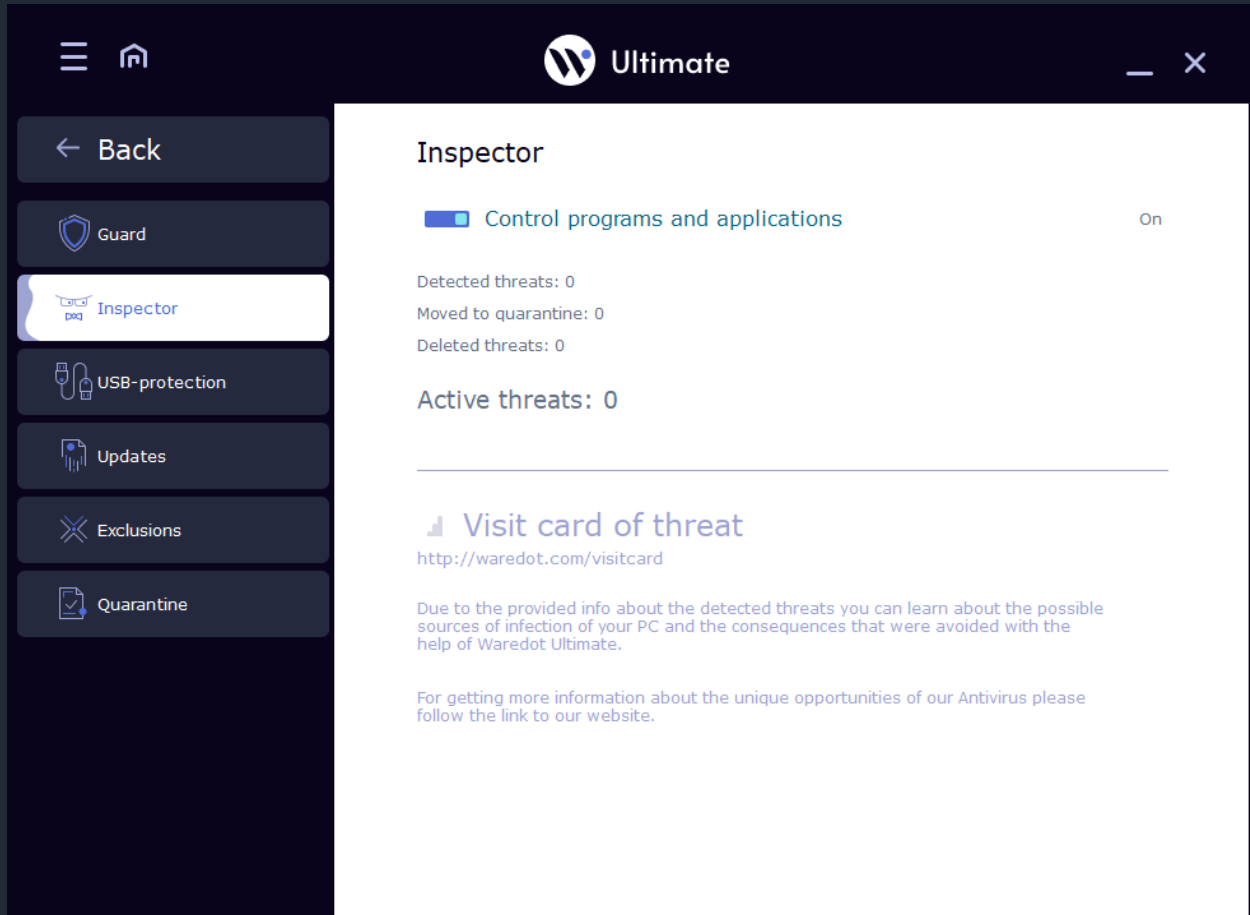


Guard on tab “Settings” – allows you to choose the action which will be applied in the case of detection of threat by Waredot Ultimate.



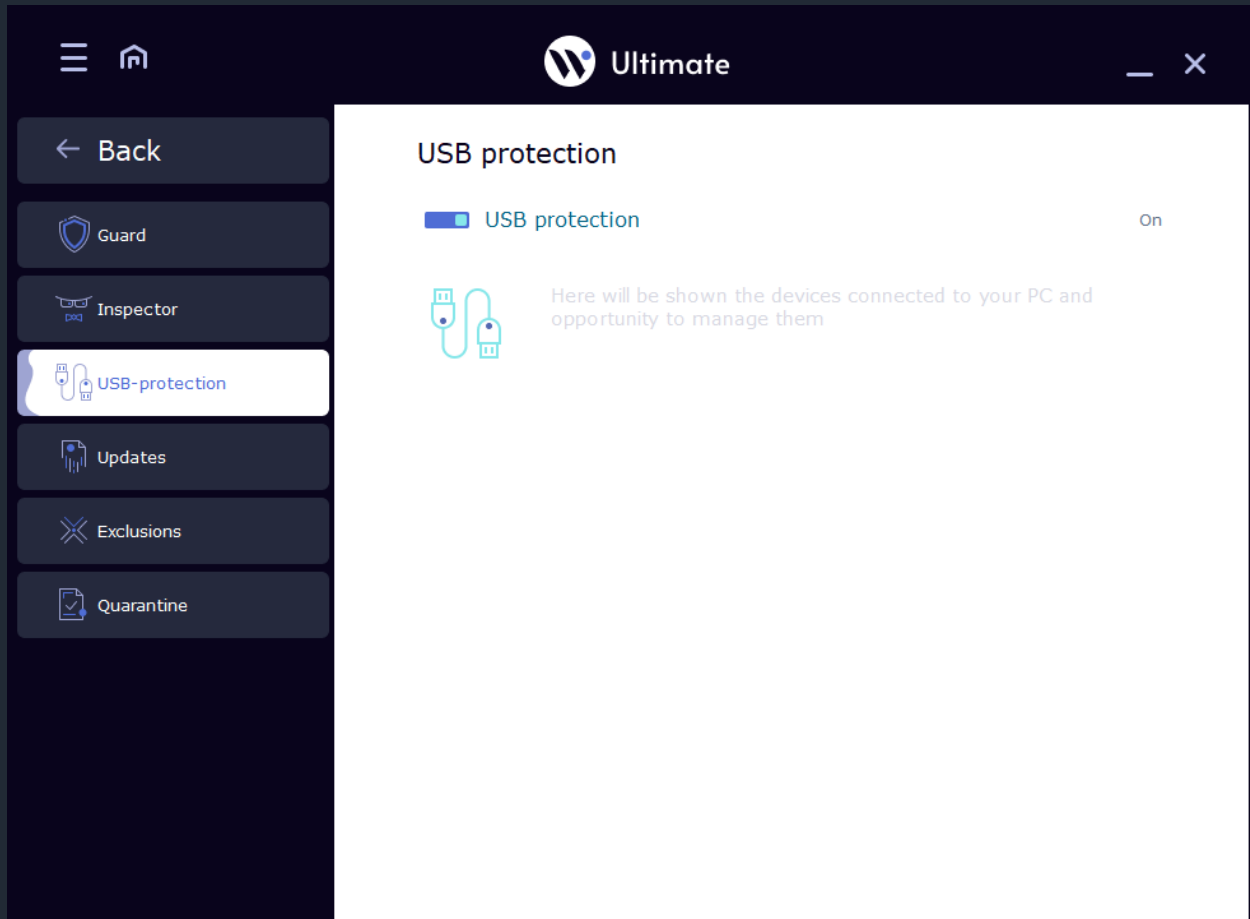
Inspector (Behavioral analyzer, HIPS) - One of the most important modules of all range of antiviruses ProtoDefence is the presence of so-called behavioral analyzer (HIPS).

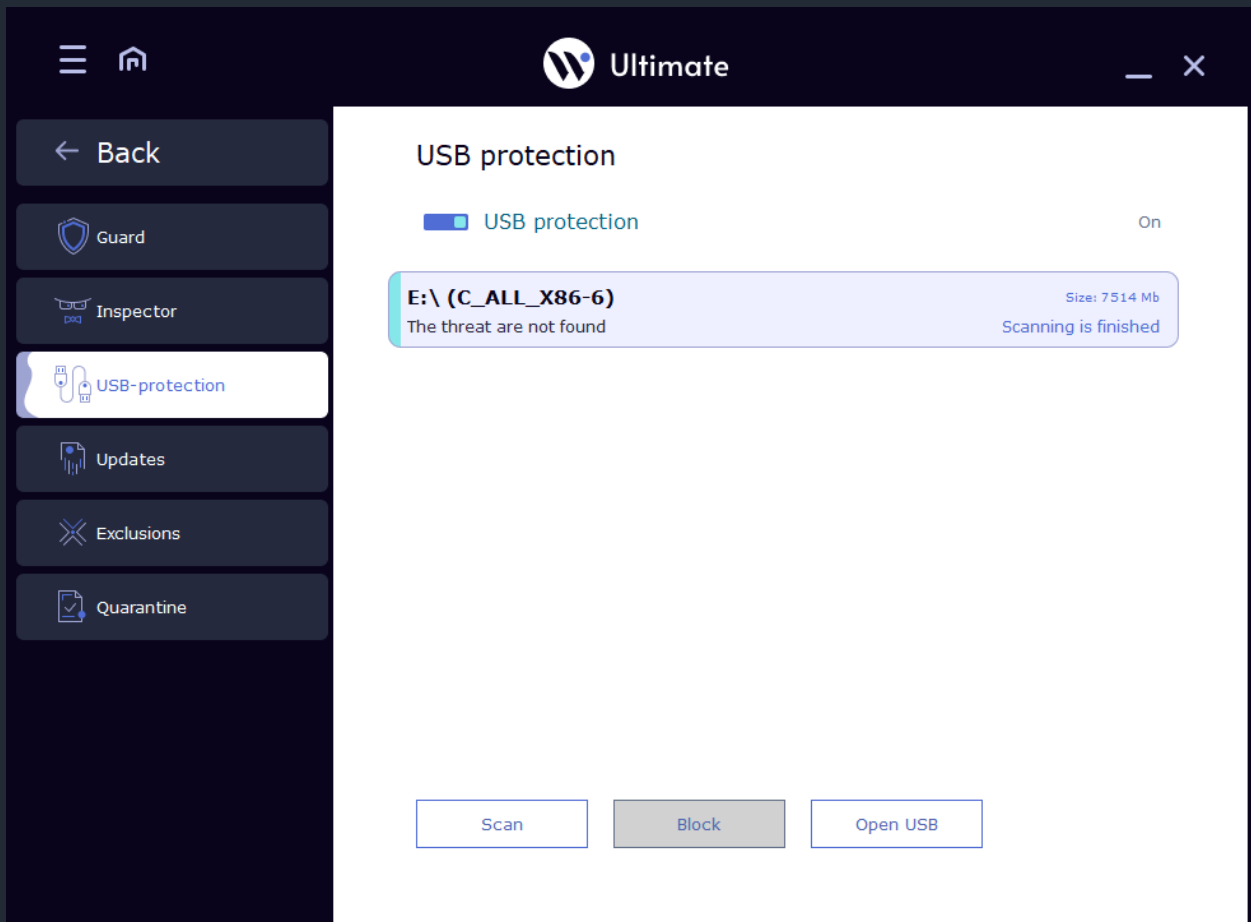
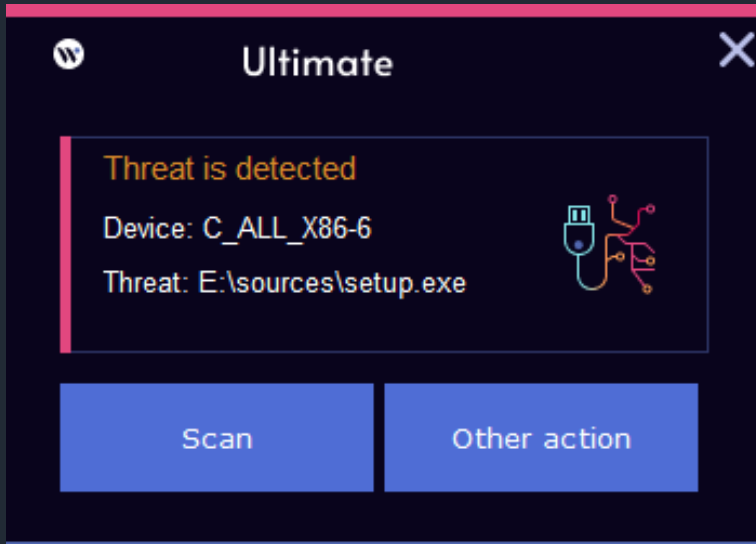
This technology allows to scan and analyze of programs, to determine likelihood of malicious behavior. If HIPS will notice that some program performs actions that could potentially harm PC, it will be blocked even before its launch.



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 ProtoDefence 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.

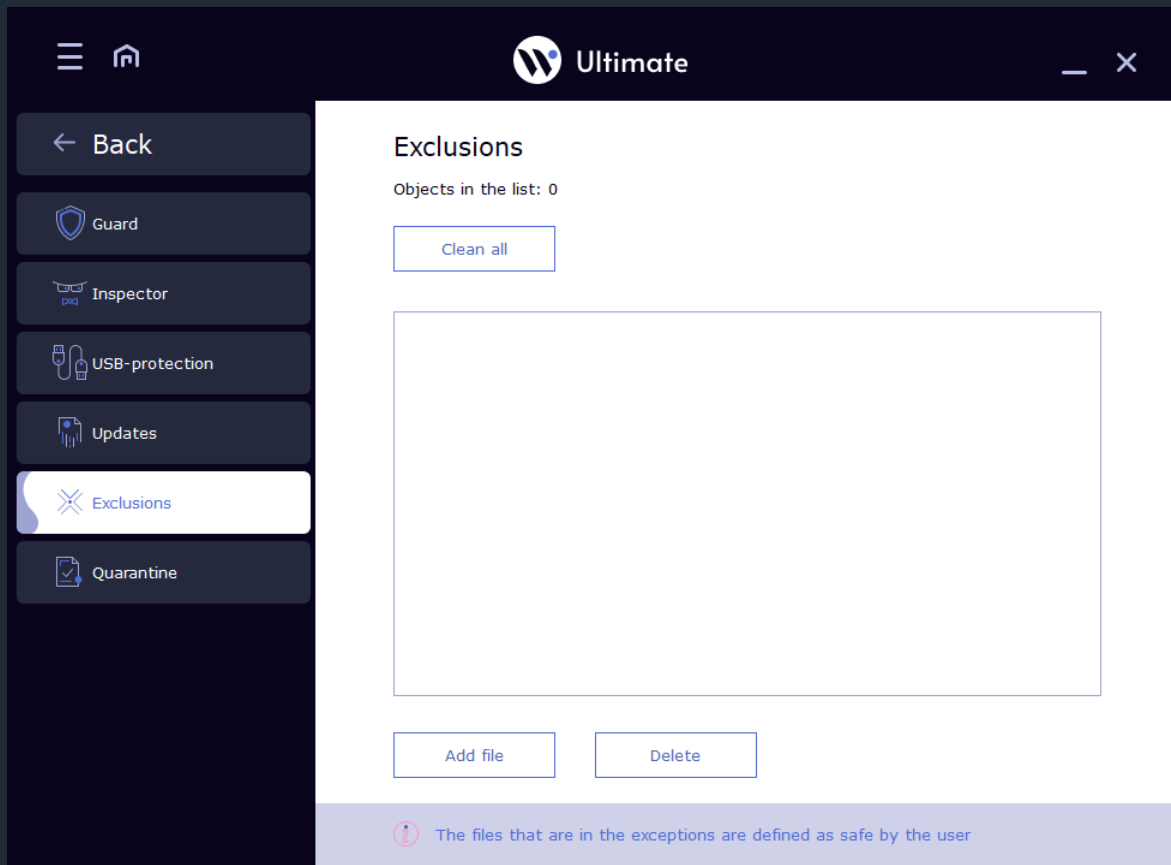
When a new USB-drive is connected, ProtoDefence detects it, performs a brief analysis and informs the user about the evaluated level of security of the disc. In the case of detection of the viruses or any suspicious objects on the flash drive, antivirus immediately prompts the user to remove them.





Exclusions tab contains files which were marked as exclusions by Waredot Ultimate. It means that Waredot Ultimate 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 Ultimate, 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 Ultimate. 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 Ultimate because all files in Exclusions are not scanned by Waredot Ultimate till they stay in Exclusions.

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

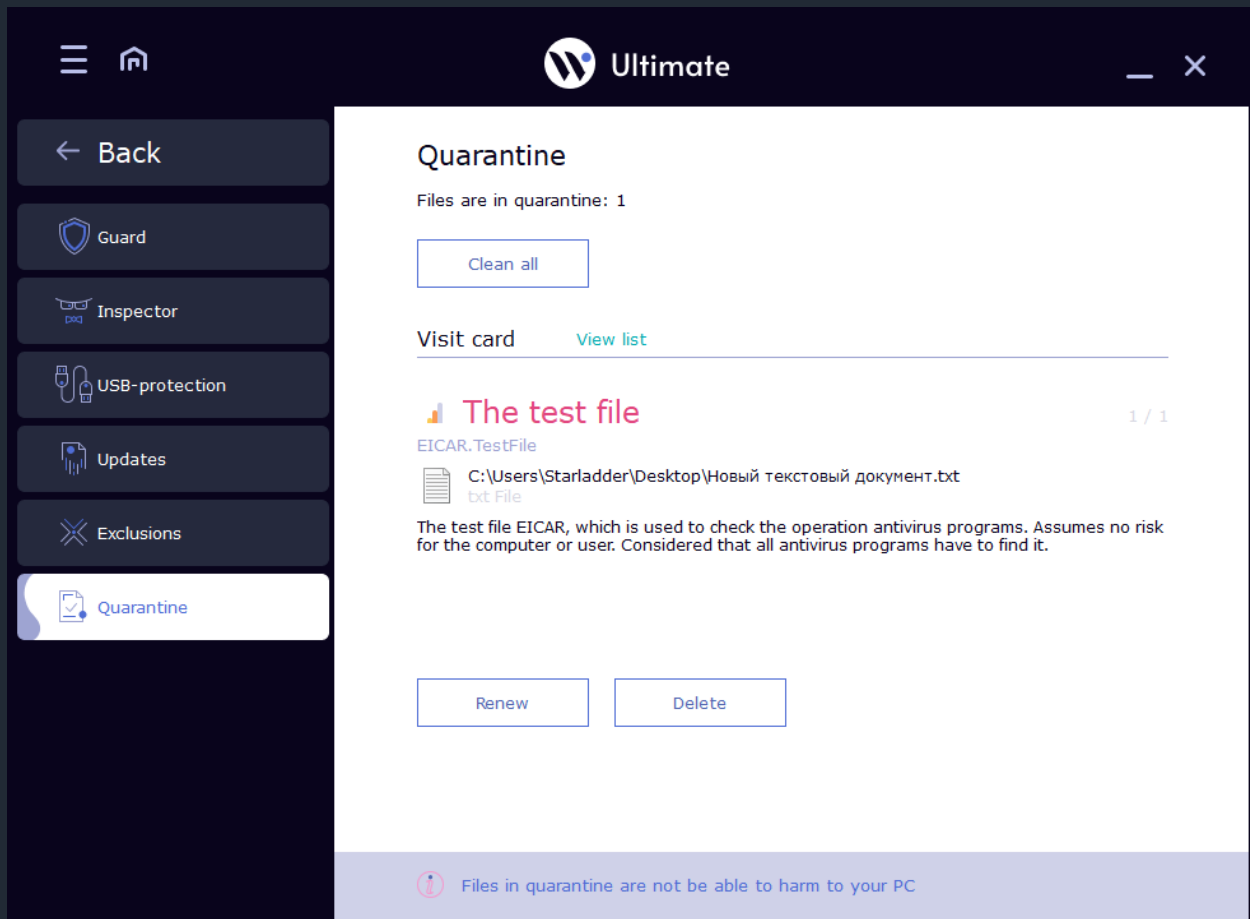
Button “Clear all” – allows user to clear whole list of the Exclusions of Waredot Ultimate with a single click of this button.



Quarantine tab contains the files which were marked by **Waredot Ultimate** 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 Ultimate 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 Ultimate:

- **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 Ultimate.

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

Please, note: after applying the action “Renew” the file will be automatically marked as safe for Waredot Ultimate and it will be added to the Exclusions of Waredot Ultimate. This file will stay in the Exclusions list of Waredot Ultimate 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 Ultimate. 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.

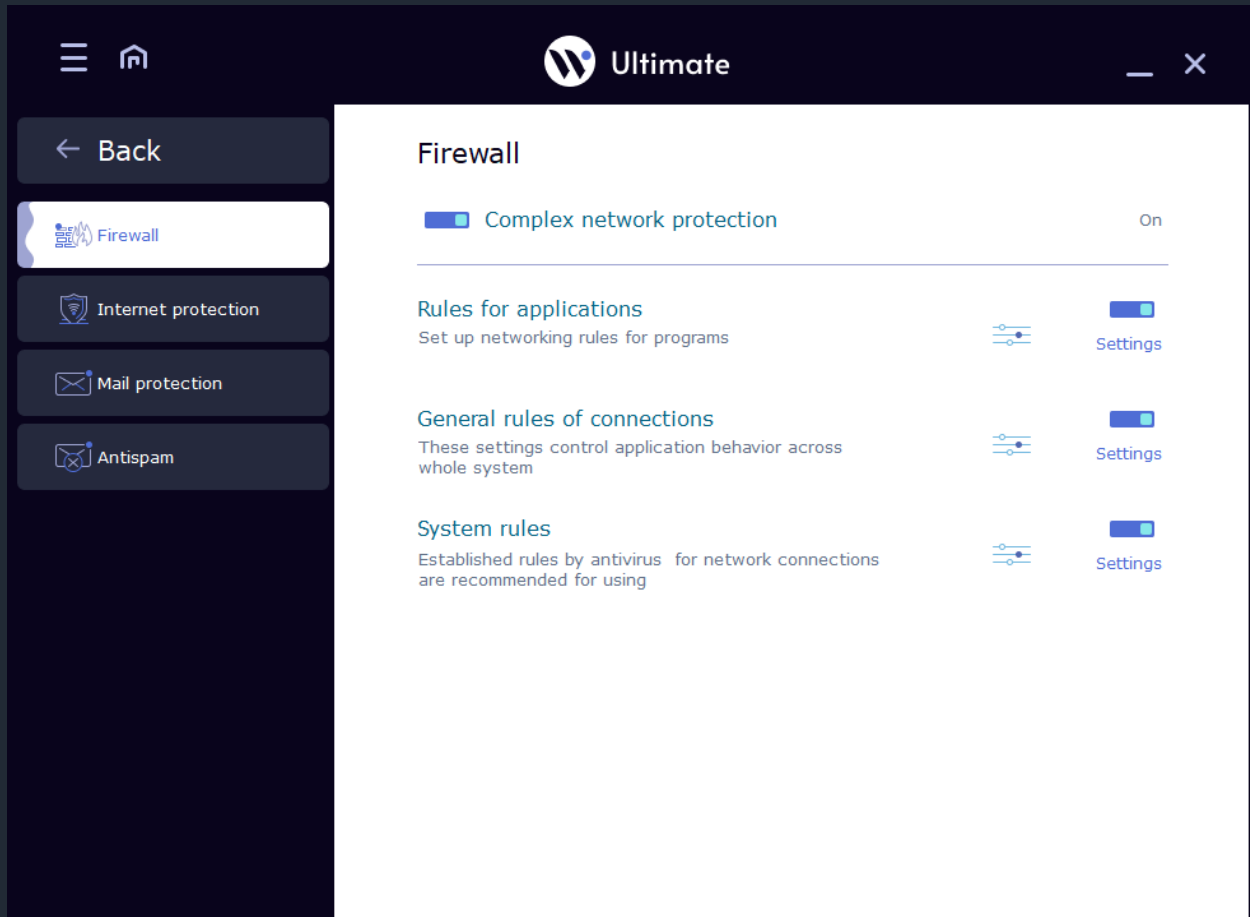
Button “Clear all” – allows user to clear whole list of the Quarantine of Waredot Ultimate with a single click of this button.



Modules of the Network Protection

Network Protection Includes:

Firewall – this module controls applications’ access to the network and provides protection against external attacks. The firewall keeps track of all applications that attempt to access the network - both incoming and outgoing traffic. By default, the firewall allows applications only outgoing traffic. This allows to protect the system from attempts to access to it from the outside, since any incoming requests will be blocked.



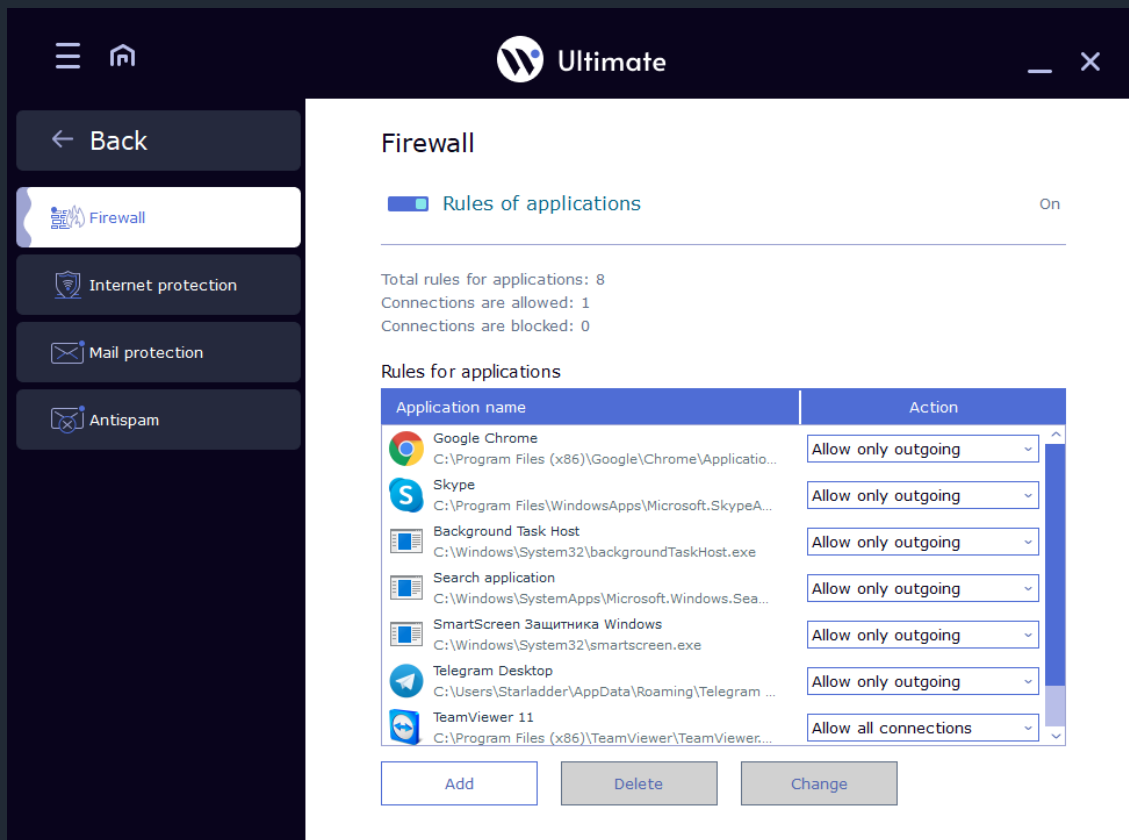
The Automatic Operative Mode

For users who do not have certain knowledge and skills to work with a firewall and its settings, has been implemented the automatic operative mode. In this mode automatically creates rules allowing outgoing traffic only for applications that require the access to the network for their work. This allows to optimally configure the security of the system without any action from the user.

Interactive mode is for experienced users.

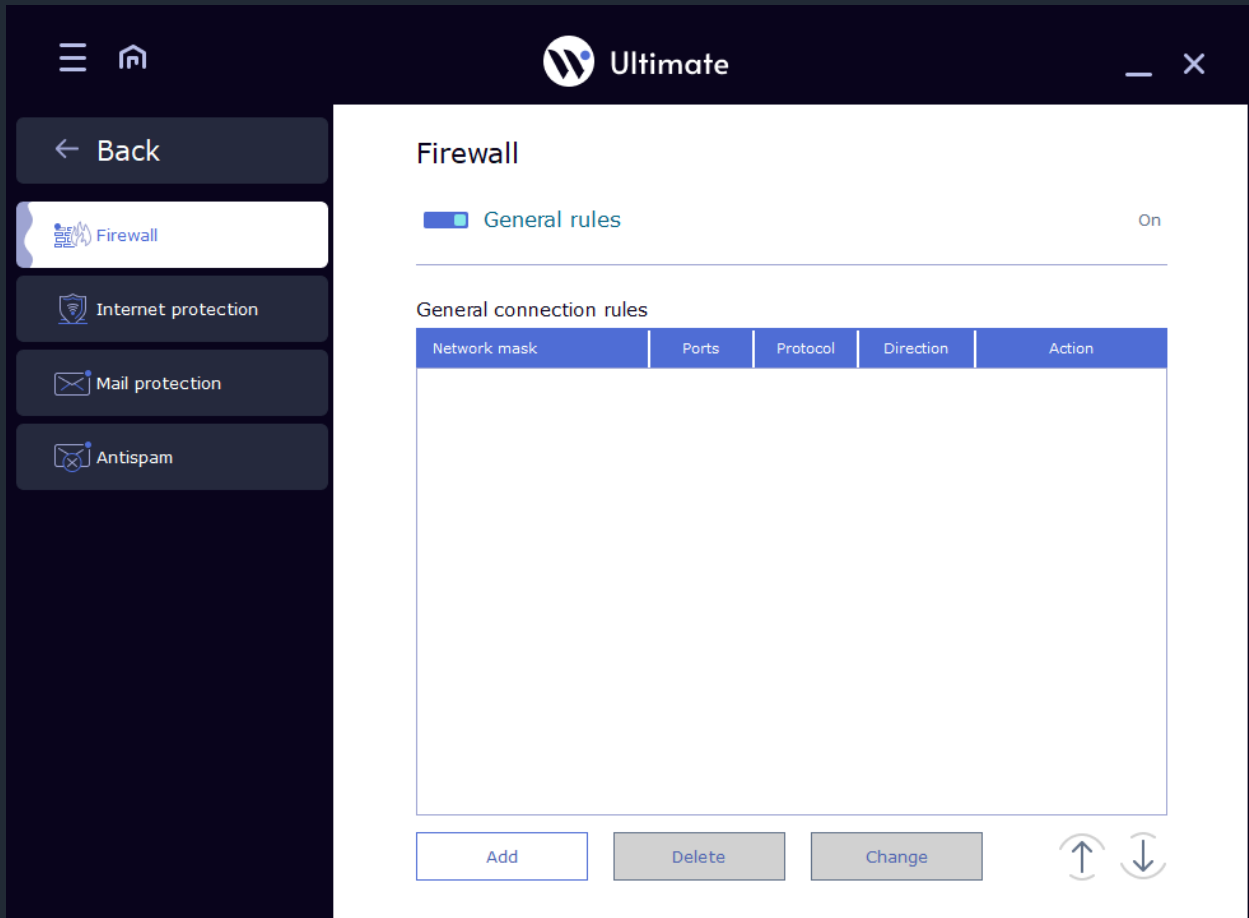
If the user knows how to create firewall rules correctly he can use an interactive mode of this module. In this mode user has **4 options**:

- **Block all** - completely blocks incoming and outgoing traffic for all applications;
- **Allow all** - allows all incoming and outgoing traffic;
- **Allow only outgoing** - allows the application to have only outgoing traffic;
- **Create a separate rule** - allows to fully customize individual access parameters:
 - To enable or disable a specific address (single address, range of addresses, the IP-addresses mask);
 - To open or close specific ports (or to apply the rule to all ports for the application, to select the direction of traffic for these settings, to specify the protocol).



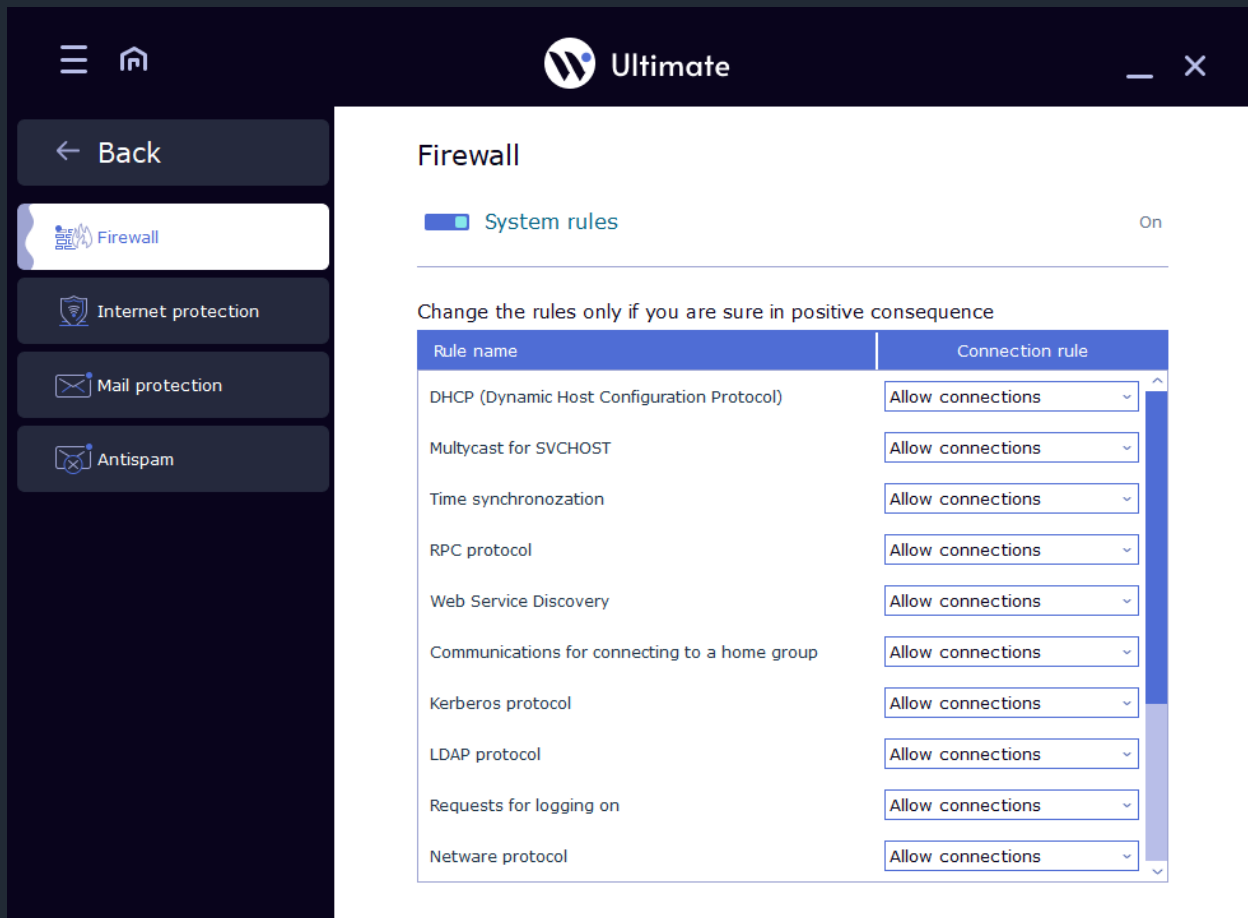
The ability to set general settings for all applications in the system

Waredot Ultimate is able to set general settings for all applications. *For example: the user requires that all applications had access to a particular server. To do this in settings must be a rule that will allow access to a specific IP-address and to a specific port. And no longer will be necessary to create separate rules of access to this server for each application.*



Built-in set of rules

The program has a built-in database containing all necessary rules to allow or to block (defined by the user) standard system services and protocols (NetBios, DHCP, DNS etc.) for work with the network. With their help, user can allow or block network activity on such protocols, leaving aside the intricacies of their work.



← Back

Firewall

Internet protection

Mail protection

Antispam

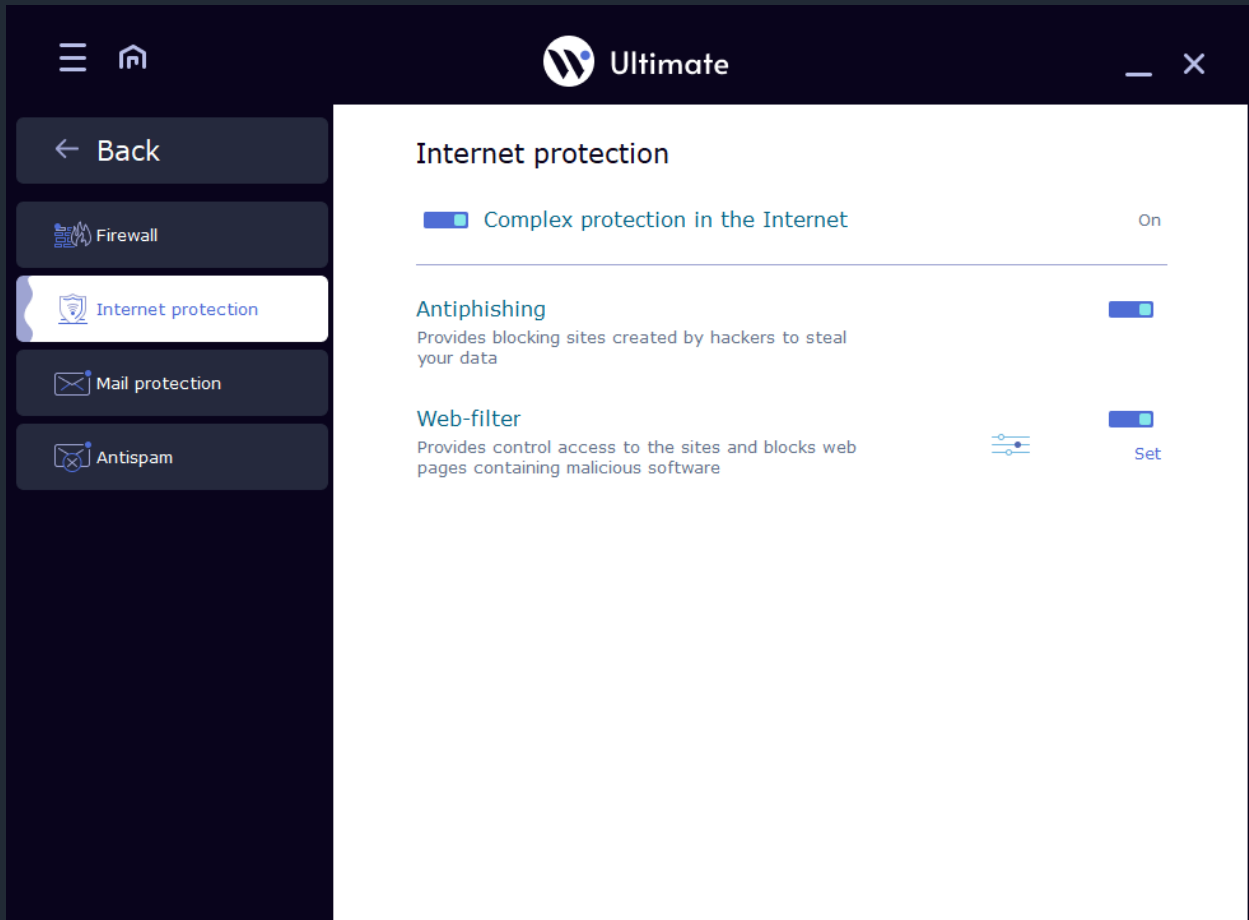
Firewall

System rules On

Change the rules only if you are sure in positive consequence

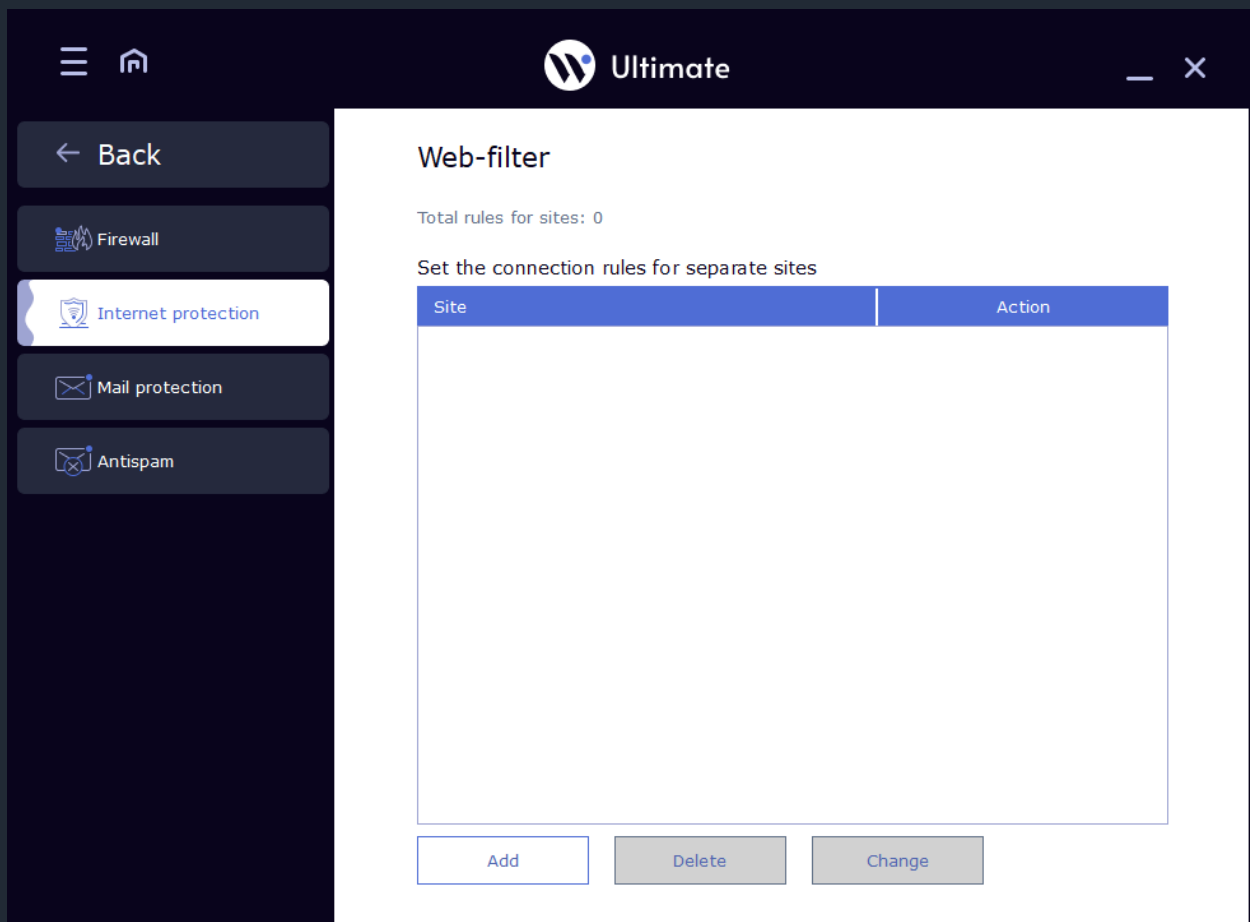
Rule name	Connection rule
DHCP (Dynamic Host Configuration Protocol)	Allow connections
Multicast for SVCHOST	Allow connections
Time synchronozation	Allow connections
RPC protocol	Allow connections
Web Service Discovery	Allow connections
Communications for connecting to a home group	Allow connections
Kerberos protocol	Allow connections
LDAP protocol	Allow connections
Requests for logging on	Allow connections
Netware protocol	Allow connections

Internet protection provides complex protection in the Internet. It includes Antiphishing module and Web-filter. **Antiphishing module** - allows to avoid the visiting sites that have phishing activity, steal user data and are used by cybercriminals for illegal enrichment.

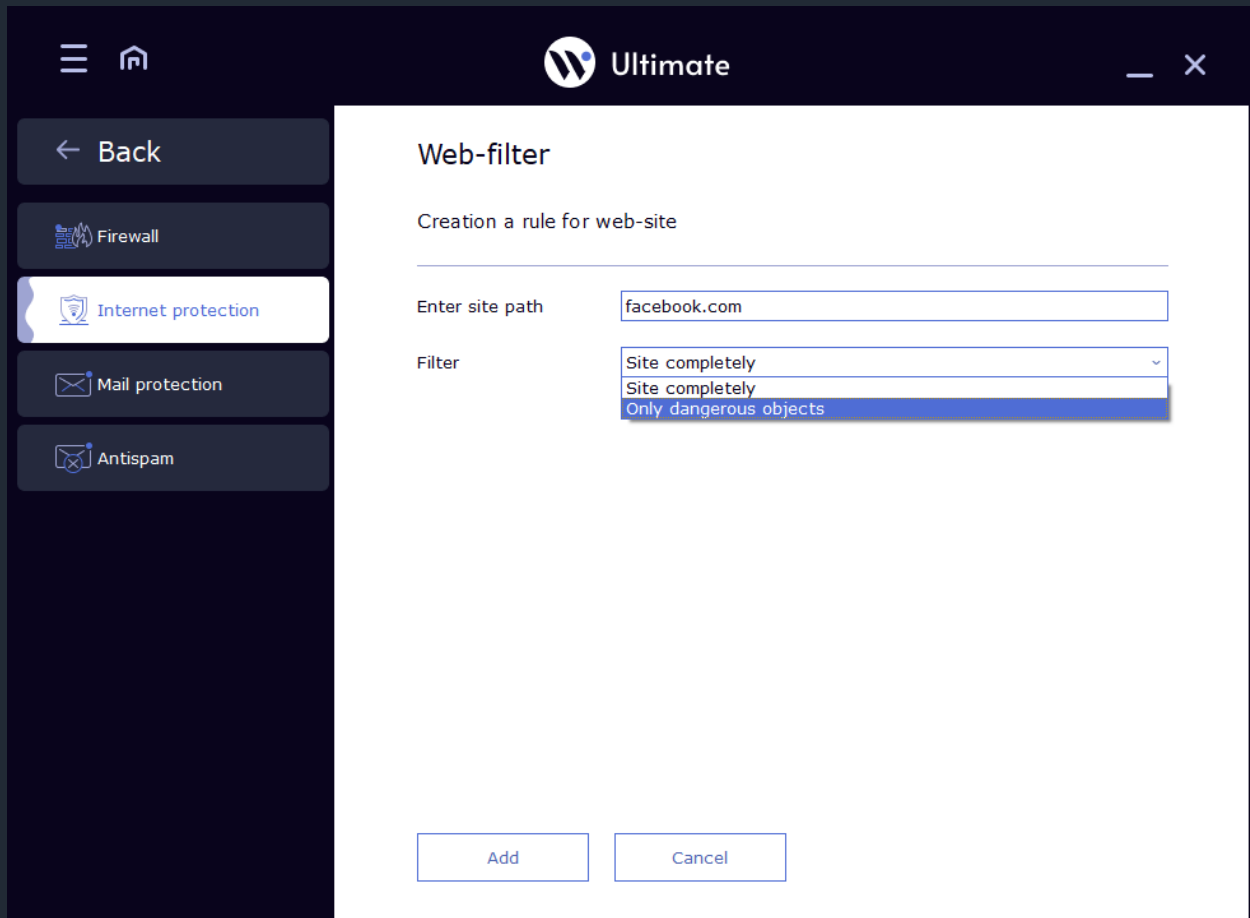


WEB-filter can block dangerous sites and potentially dangerous content from suspicious sites. Waredot Ultimate has the ability to block access to potentially dangerous sites, stopping them from loading when viewed in a browser. In this case, the user sees a message: ACCESS TO THE PAGE BLOCKED.


Some sites are added to the base of Waredot Ultimate as suspicious, or sites that have malicious content. If a site is in this list, you will be able to visit it, to view the pages, images, but you will not be able to download from this resource any programs, files, documents and other files that may harm your computer.





In addition to the built-in data base of blocked sites, Web-filter allows user to create own list of sites that he considers undesirable by any reason. To this personal base applied the same rules that apply to the built-in base. For adding new web-site click the button “Add” in main window of WEB-filter. In this window you should to enter URL of web-site and select filter then click “Add”.



← Back

 Firewall

 Internet protection

 Mail protection

 Antispam

Web-filter

Total rules for sites: 1

Set the connection rules for separate sites

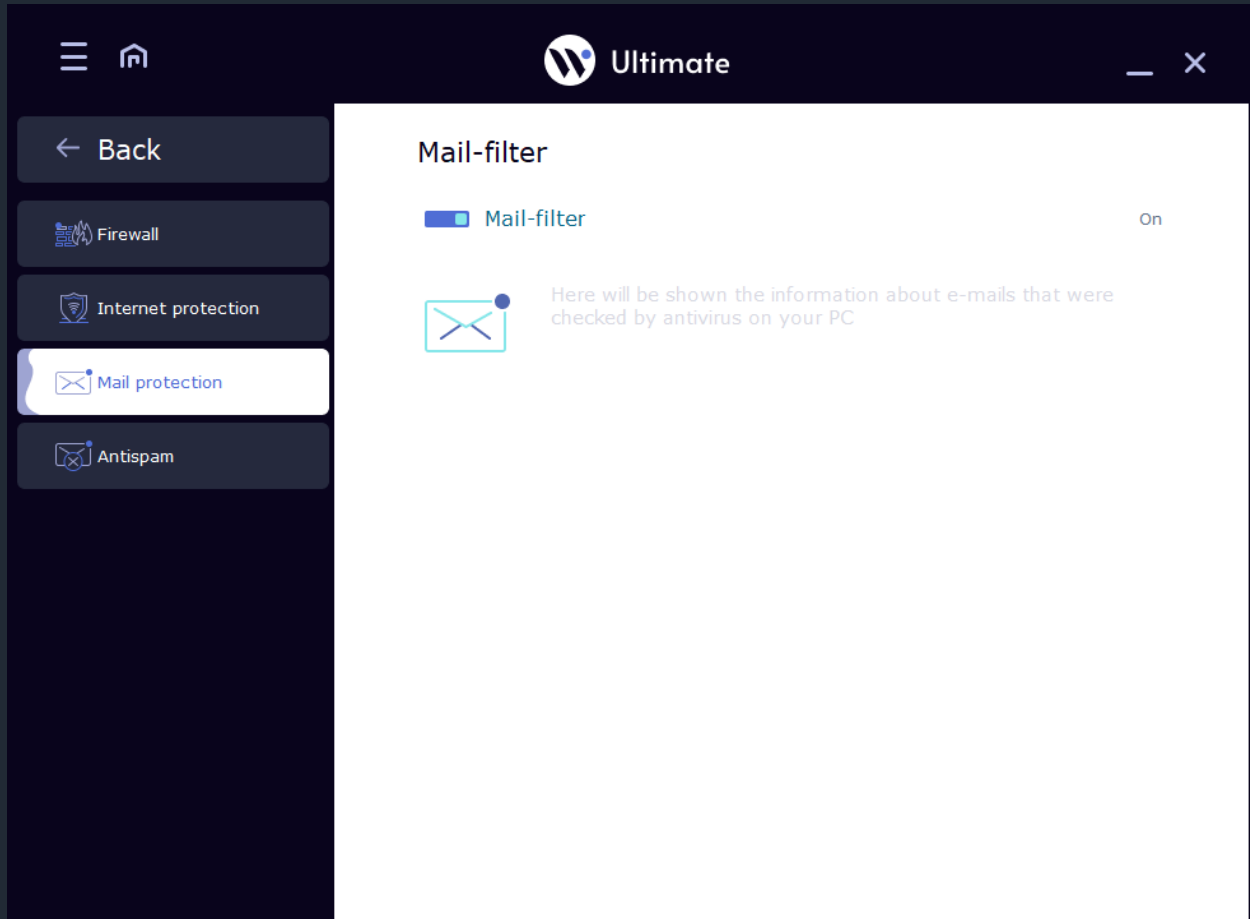
Site	Action
facebook.com	<div style="border: 1px solid #ccc; padding: 2px;"><p>Site completely ▾</p><p>Site completely</p><p>Only dangerous objects</p></div>

Add

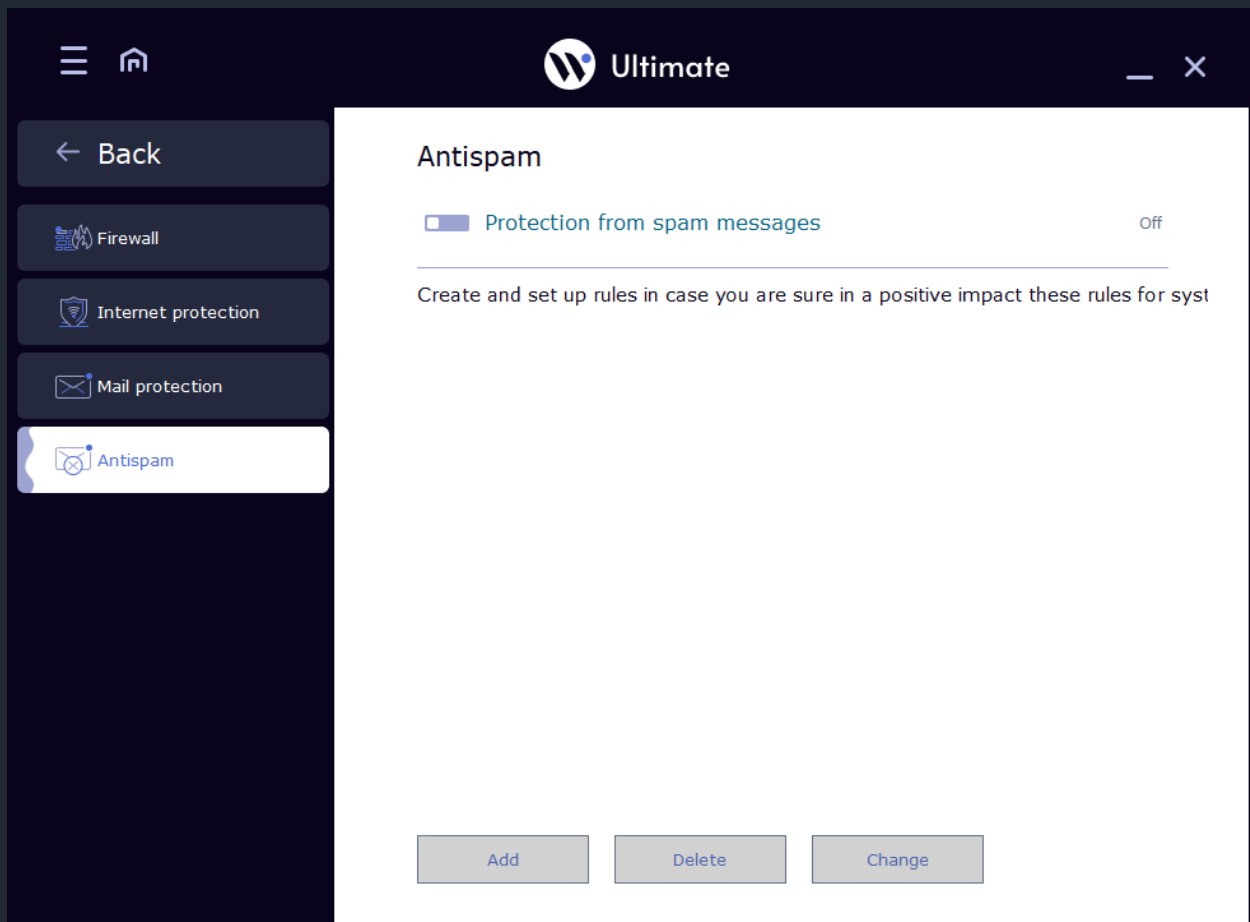
Delete

Change

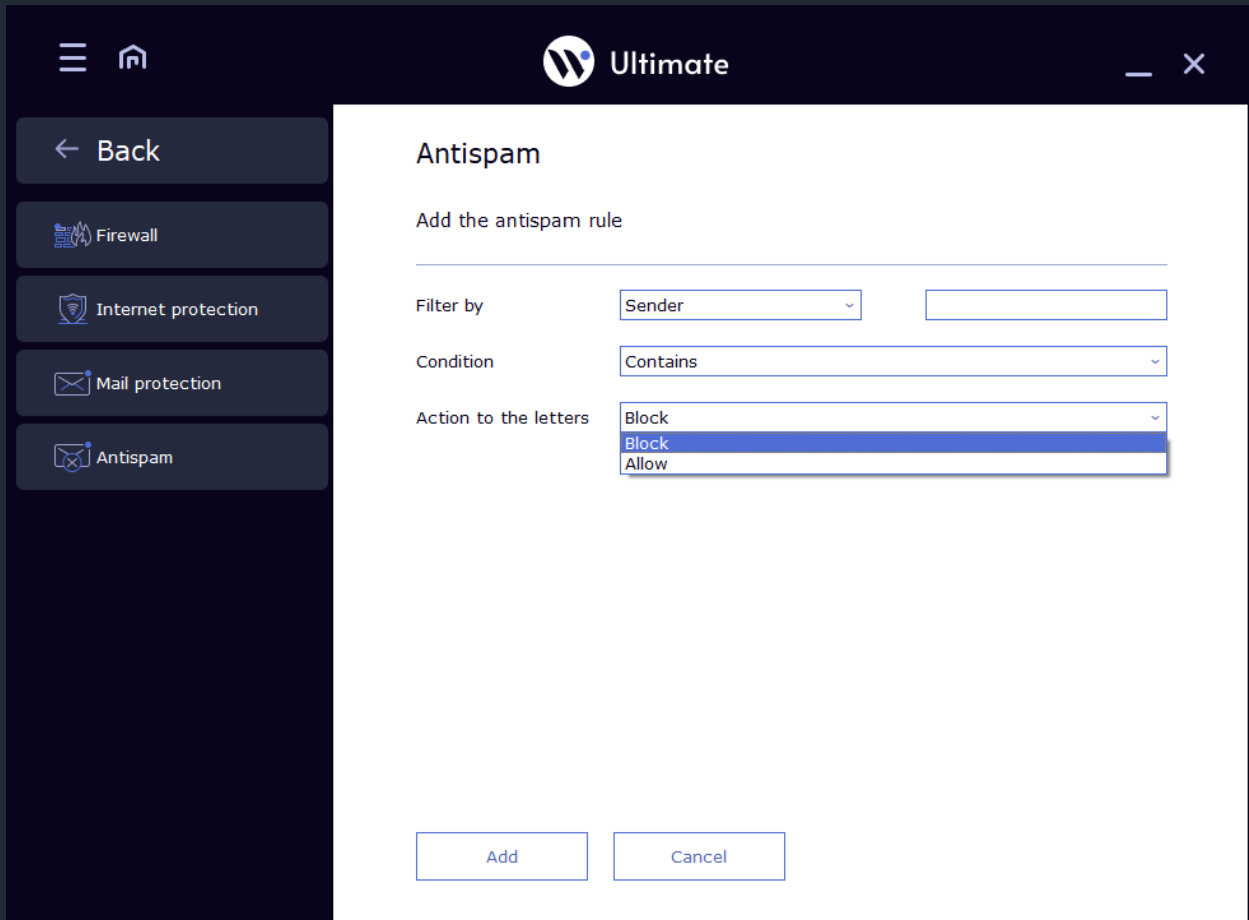
Mail filter checks all incoming and outgoing email messages for malicious objects, thus avoiding possible infiltration of threats in the system by means of e-mail.



Antispam module is built on the principle of proactive technologies. They allow to set up a "black list" of e-mail addresses and websites that have been seen in spam mailings and phishing activity.



For example, Antispam allows to make flexible adjustment of blocked messages. You can set the filter by sender, recipient, title, or subject. This will significantly reduce the probability of receiving unwanted emails.



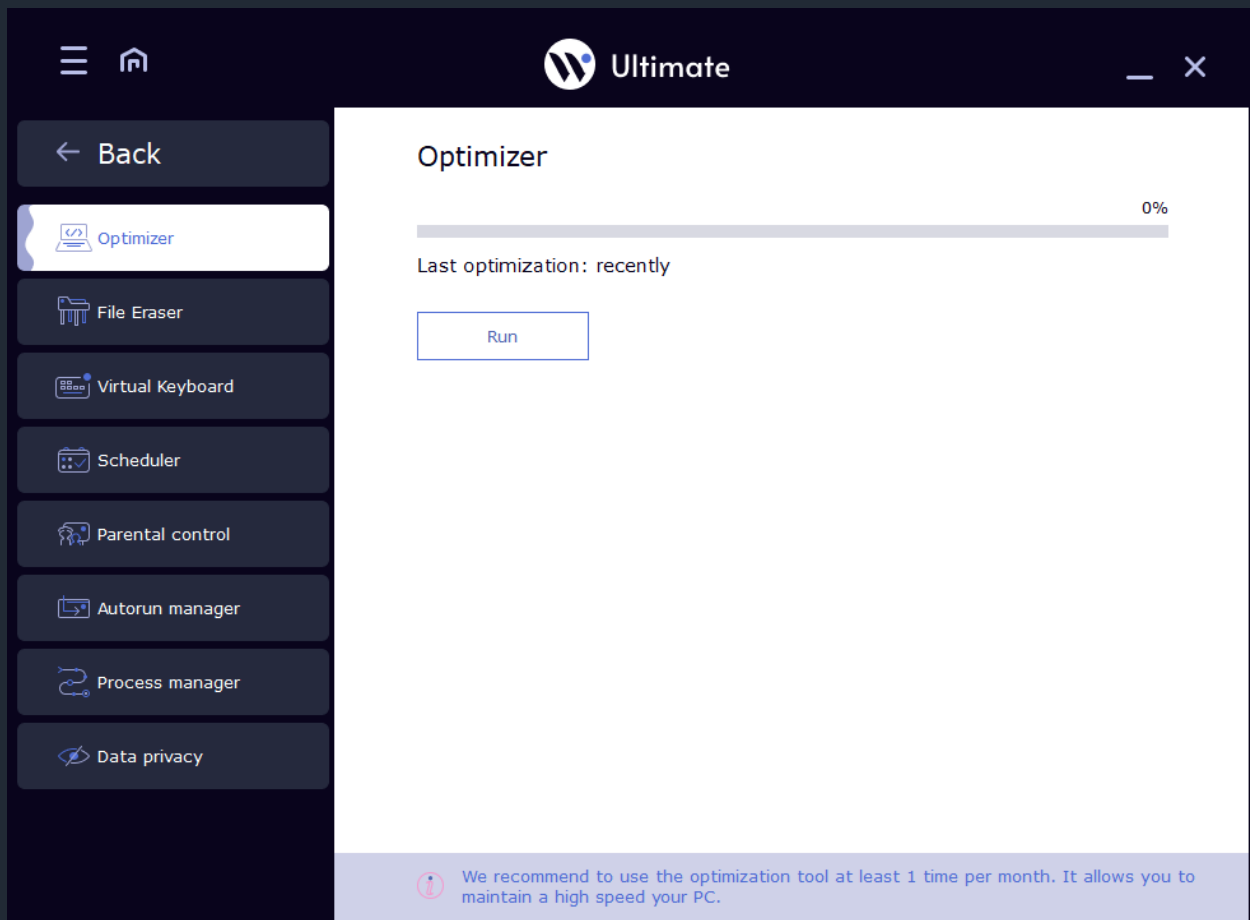
Tools

Waredot Ultimate contains the **next Tools:**

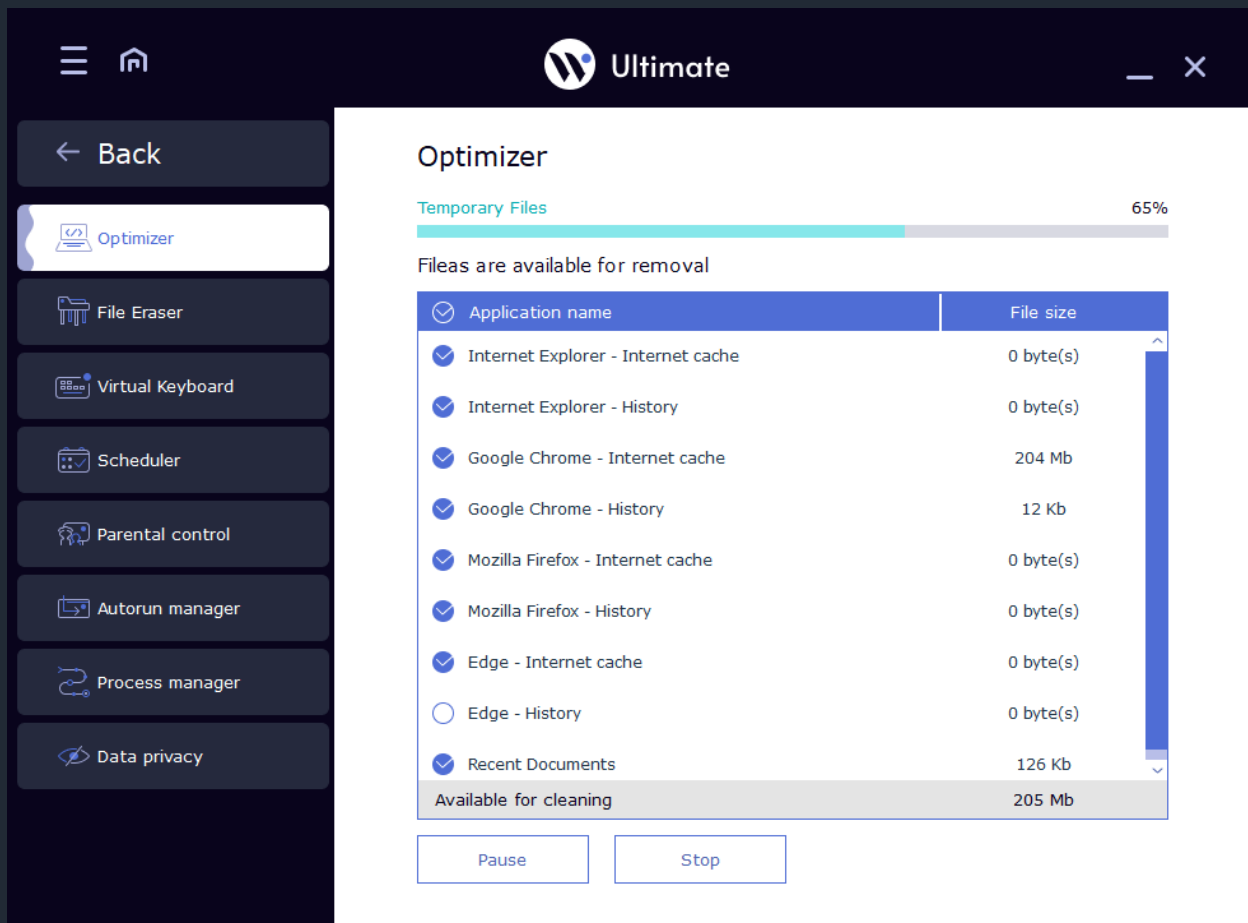
Optimizer is a tool that speeds up your PC. The software module allows to find unnecessary files and programs that overload operating system, and to remove them.

The principle of its work is based on check of certain computer memory locations where temporary files are stored. Optimization are subject such categories files as browsers' cache, search history, which they store, files of updates of operating system, "service" files etc.

Please click the button "Run" for beginning the optimization.

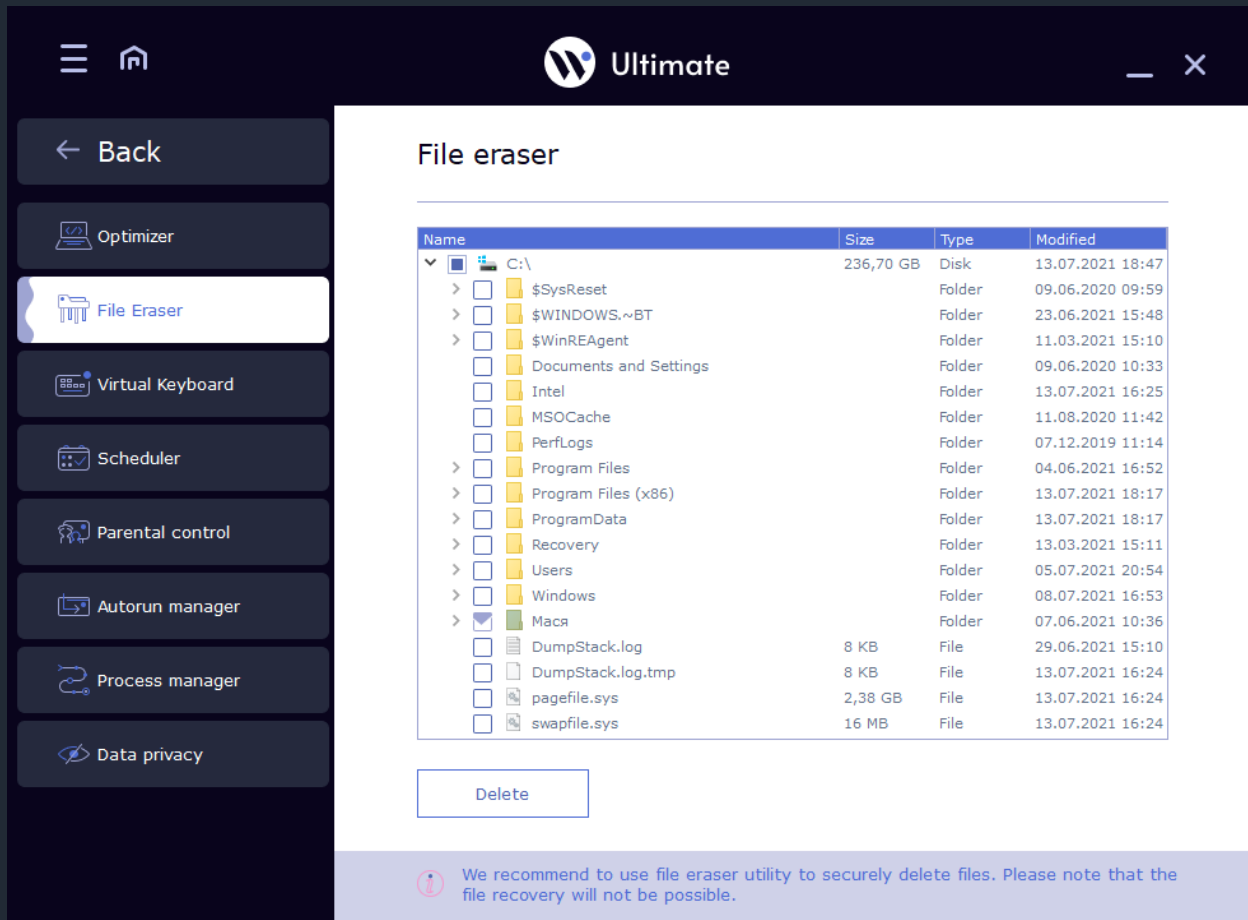


After scanning, the tool displays a list of all files, which are offered to be removed, the size each of them, and the total volume of memory that will be released. The decision about removing is made directly by user.

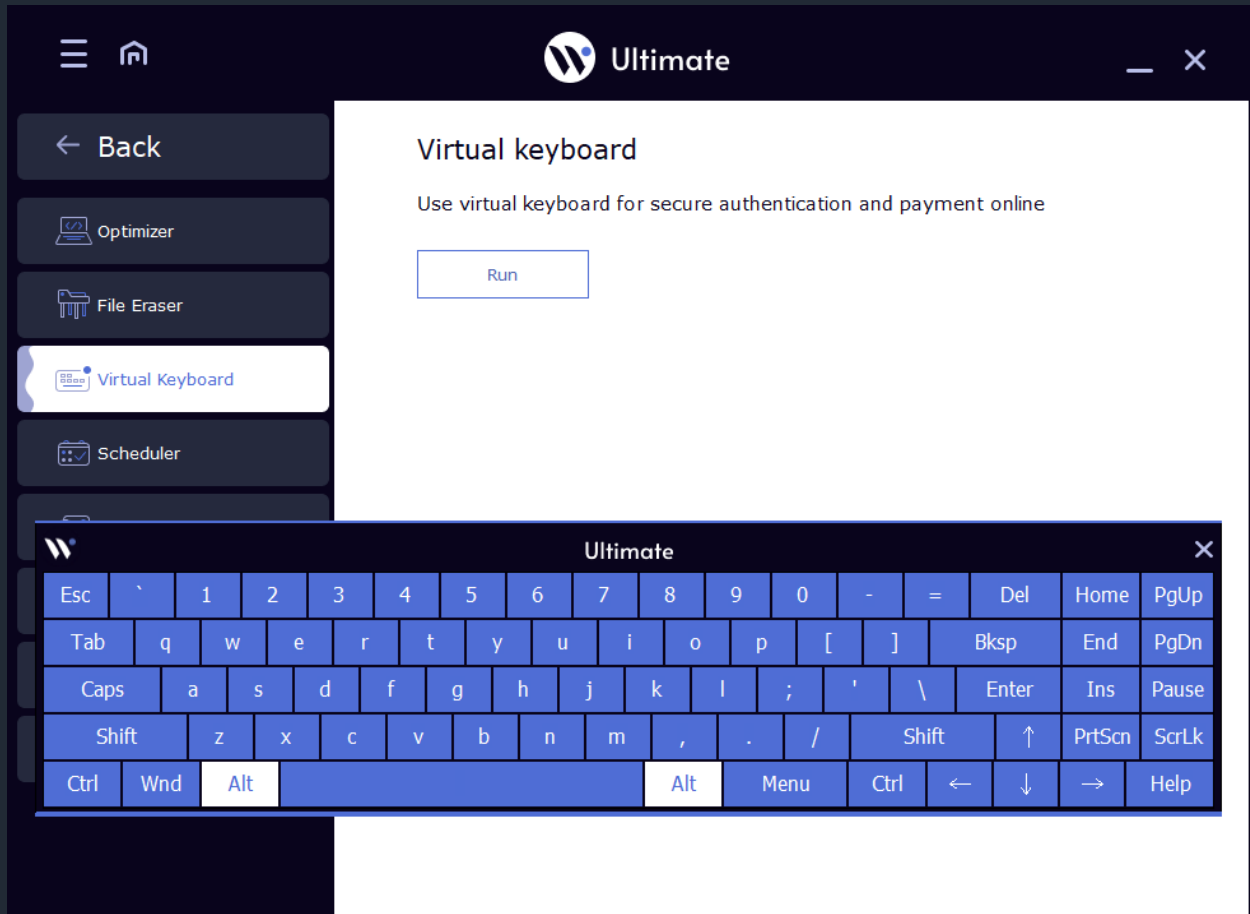


File Eraser is a special program that allows to safely remove the most unwanted or confidential files without the possibility of their recovery.

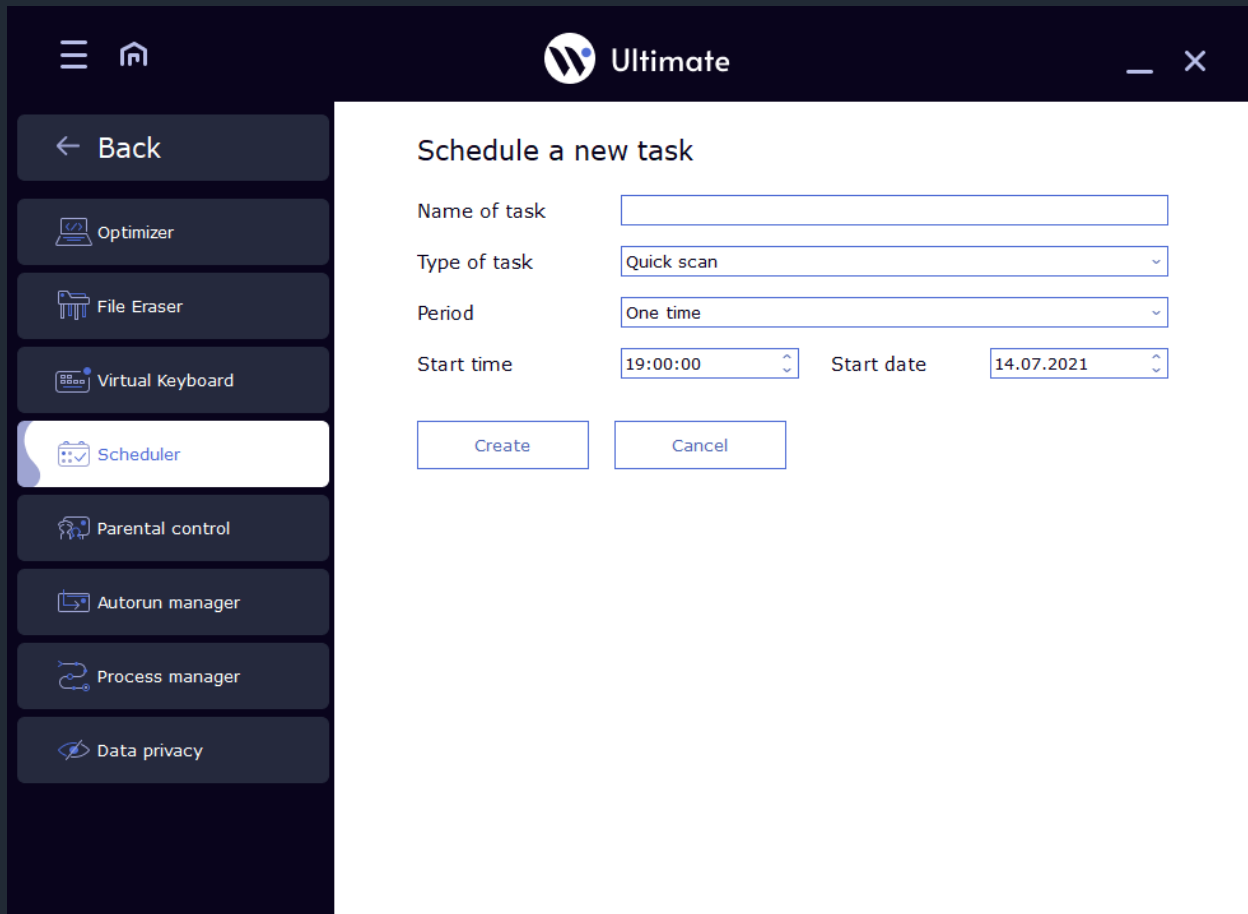
The way of operation of programs-shredders are next: the file that will be removed, is subjected to multi wipe-off. In the fact, it will be filled with meaningless information garbage (random numbers, characters, symbols etc.), which completely distorts its content, without the restoration possibility. After this, it will be removed from the hard drive. Even if such file would ever be found by hackers and they would try to restore it, they would not receive any benefit from such actions.



Virtual keyboard allows to prevent interception of confidential data. Using it, you can specify the details of your account in social networks, email, banking, etc., without the risk that they can be intercepted and stolen by hackers. The virtual keyboard can be used for typing in any application, as well as on any Internet resource for a set of confidential information (login, password, banking card, etc.).



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", "monthly". "Time" indicates 24-hour format the time to start the task. "Start Date" - the date for the scan.

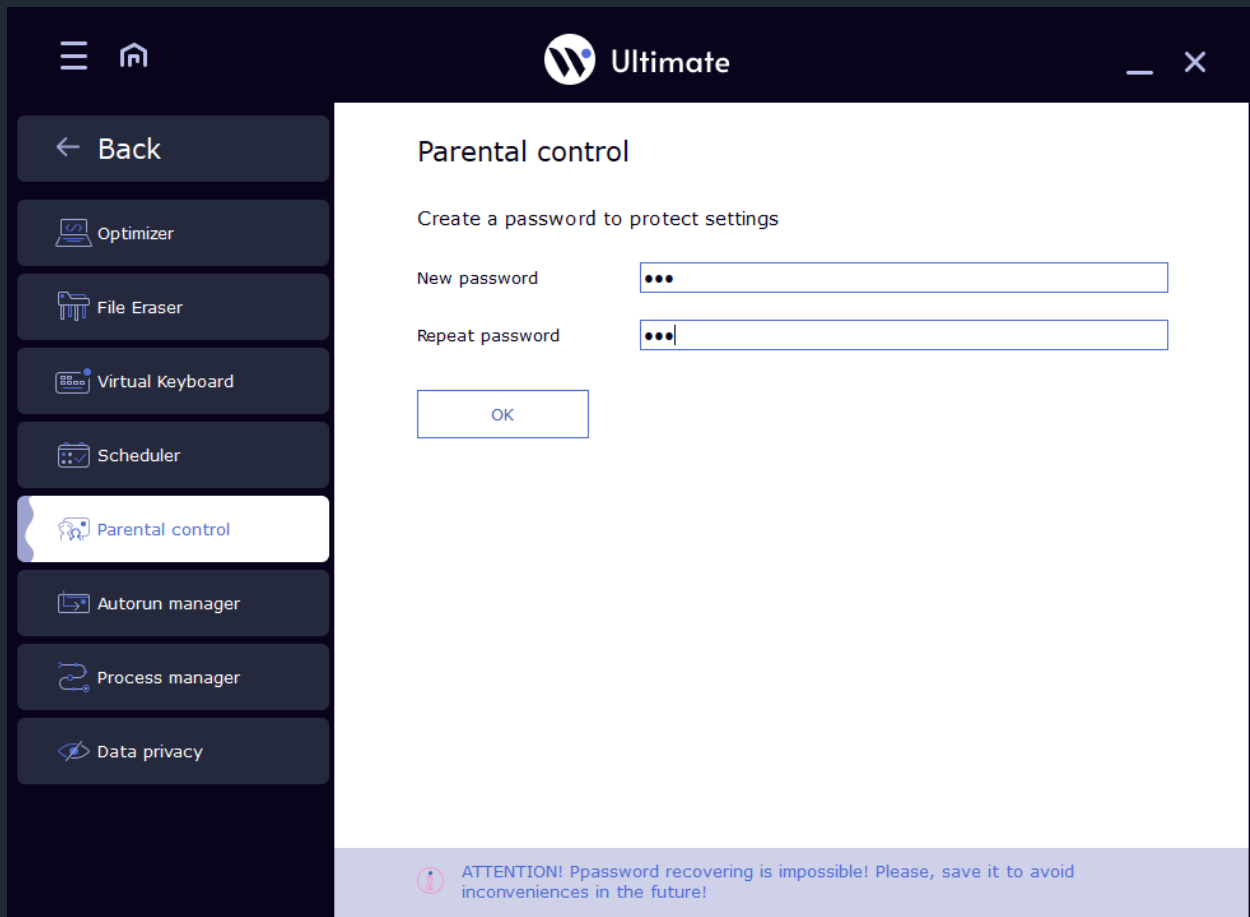


The screenshot shows the 'Ultimate' application interface. On the left is a dark sidebar with a menu containing: 'Back', 'Optimizer', 'File Eraser', 'Virtual Keyboard', 'Scheduler' (highlighted), 'Parental control', 'Autorun manager', 'Process manager', and 'Data privacy'. The main area is a white dialog box titled 'Schedule a new task'. It contains the following fields: 'Name of task' (text input), 'Type of task' (dropdown menu with 'Quick scan' selected), 'Period' (dropdown menu with 'One time' selected), 'Start time' (time picker set to '19:00:00'), and 'Start date' (date picker set to '14.07.2021'). At the bottom of the dialog are 'Create' and 'Cancel' buttons.

Parental Control

This module allows to control visits to websites of the young PC users that their parents find undesirable.

It is important to understand that the essence of the “Parental Control” is to create a safe informational space for the child. Modern programs of parental control are complex filters that prevent minors visits to certain sites, the content of which, according to their parents, is undesirable for viewing.



☰ 🏠 Ultimate — ✕

← Back

🖥️ Optimizer

🗑️ File Eraser

🌨️ Virtual Keyboard

📅 Scheduler

👤 Parental control

📁 Autorun manager

🔄 Process manager

👁️ Data privacy

Parental control

Enter your password

🔒 [change password](#)

OK



☰ 🏠 Ultimate — ✕

← Back

📊 Optimizer

🗑️ File Eraser

🖱️ Virtual Keyboard

📅 Scheduler

👤 Parental control

📁 Autorun manager

🔄 Process manager

🔒 Data privacy

Parental control

Child protection in the network On

Total PC users: 2 change password
Under the control: 2


List of users:

Гость1	✔ Under control
Starladder	✔ Under control

[Remove the control](#) [Change](#)



☰
🏠



— ✕

← Back

📈 Optimizer

🗑️ File Eraser

🖱️ Virtual Keyboard

📅 Scheduler

👤 Parental control

📁 Autorun manager

🔄 Process manager


🔒 Data privacy

Parental control

User: Starladder


Rules of access to the Internet

Select the time, when your child will have access to the Internet


Set


Rules of access to websites by category

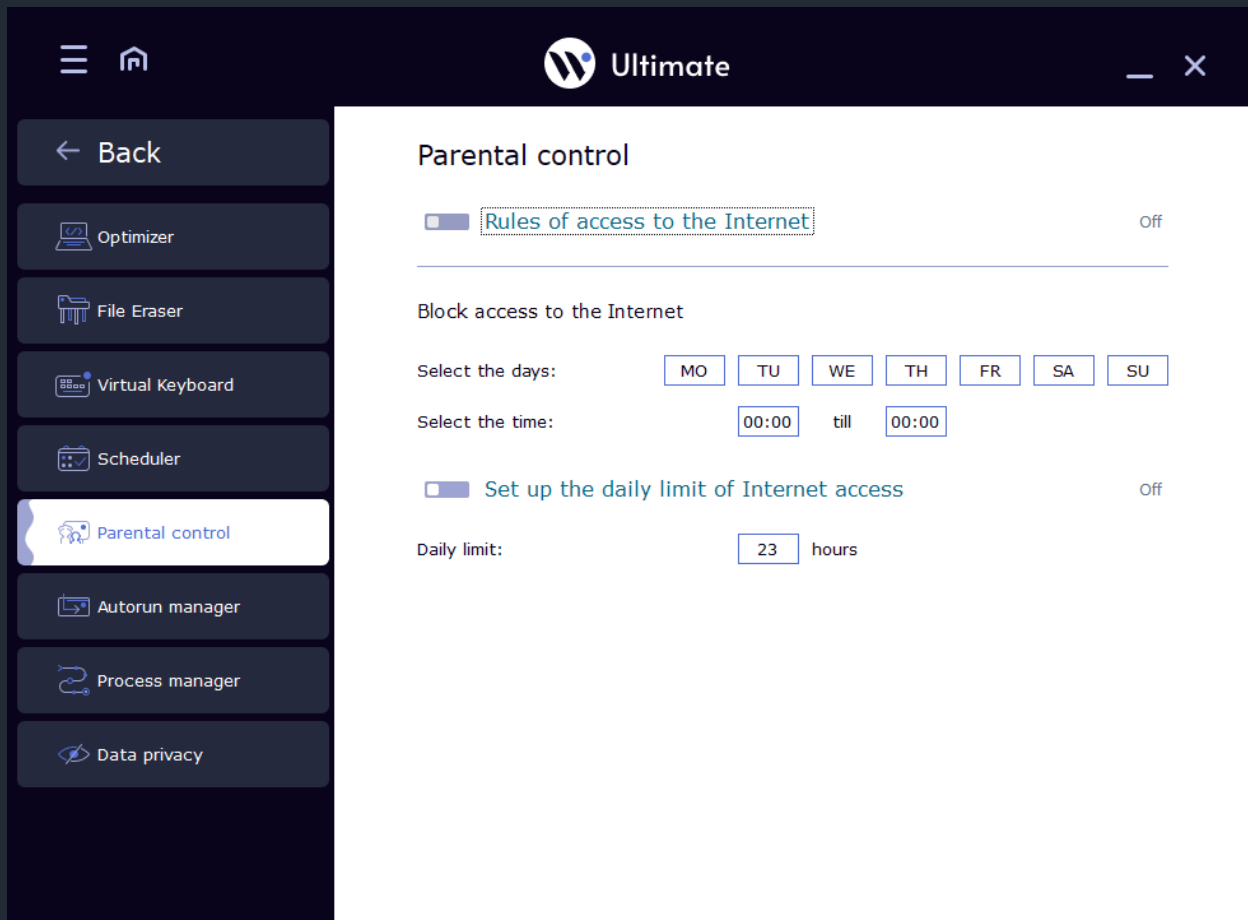
Select categories of sites to which access will be restricted


Set

White and black lists of sites

Allow or deny access to specific sites


Set



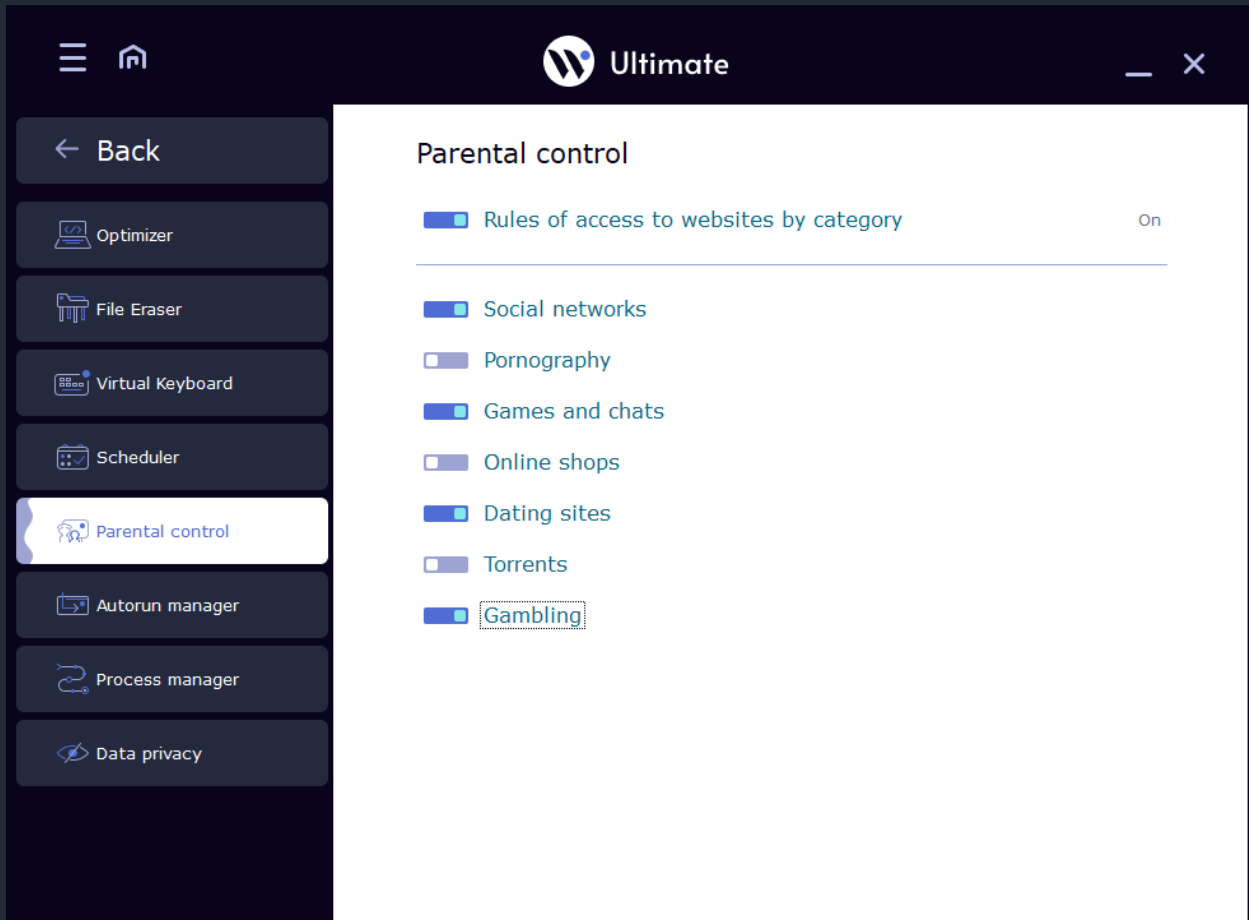
Actions of parental control based on list of network resources, access to which is defined as prohibited.

Functions of “**Parental Control**” that Waredot Ultimate has, include predefined lists of thousands pornographic sites, over 2,000 online gambling sites and over 1,000 resources, where violence and alcohol content is placed.






These resources include the following sites, related to:

- Social networks;
- Pornography;
- Games and Chats;
- Dating sites;
- Torrents;
- Online shops;
- Gambling.


You can choose what categories of web-sites must be blocked by Waredot Ultimate.





In addition, this database can be changed and supplemented manually with administrative rights, allowing you to customize the functionality of the module to make it more flexible and to take into account all the necessary requirements.


   **Ultimate**  


← Back


 Optimizer


 File Eraser


 Virtual Keyboard

 Scheduler

 **Parental control**

 Autorun manager

 Process manager

 Data privacy

Parental control

White and black lists On

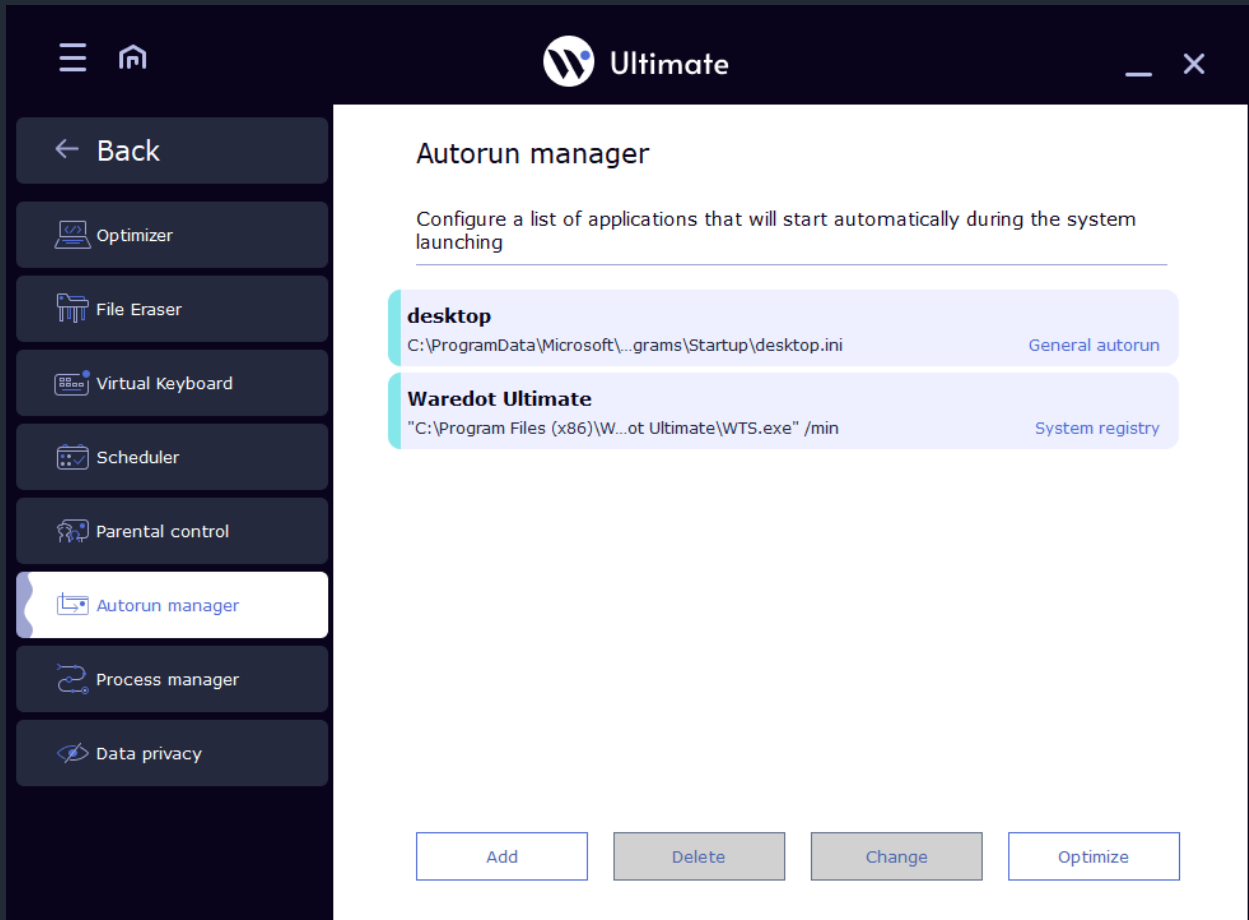
Sites in black list: 0
Sites in white list: 0

Select the list to which you wish to add the site:

Website address:

All Black list White list

Autorun manager allows you to search for programs and services of operating system that are not used by the user, but still automatically uploaded and consume computer resources, and to disable their automatic upload.



Autorun manager is a program that allows you to analyze the applications that are uploaded at startup and to optimize boot time by disabling applications and some system functions that are not used.

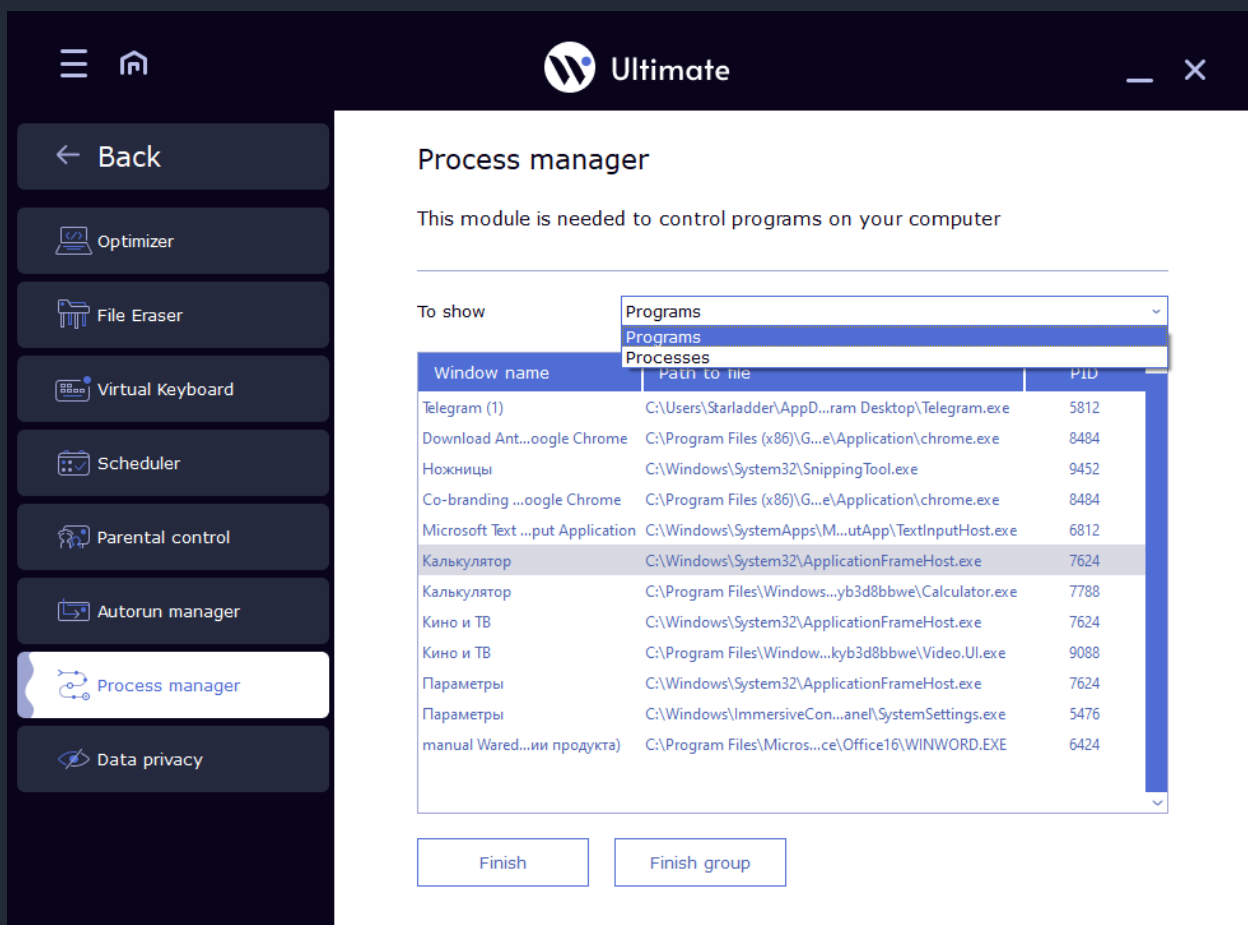
Autorun manager optimization has been designed to increase the speed of your PC.

Process manager, as built-in controller of applications and processes, allows you to control and manage running applications and processes.

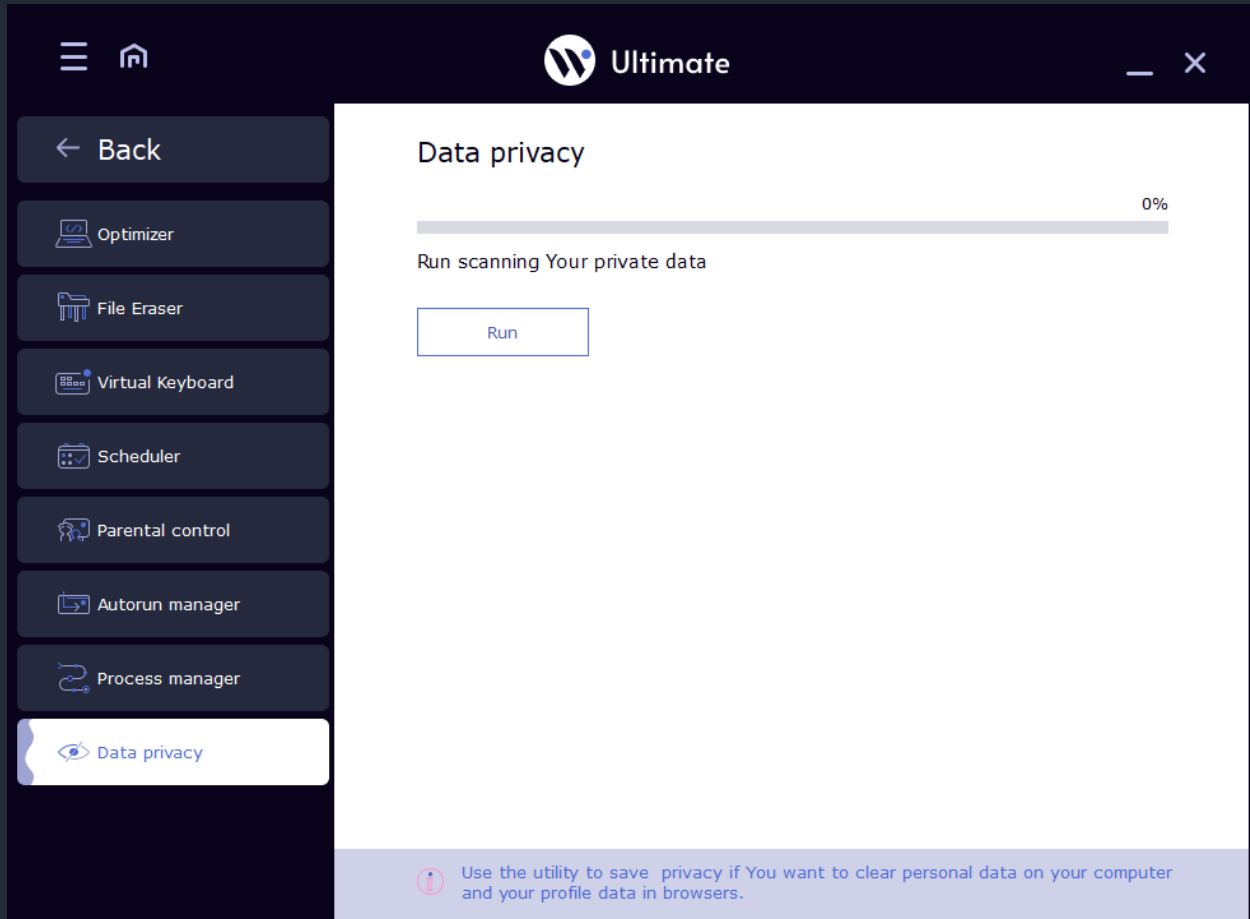
Process manager gives user the information on current working applications and services and also data of resources consumption. Utility allows to forcibly terminate undesirable processes, if they hang, or excessively use memory that could adversely affect the performance of the PC.

Process manager can regulate the work of:

- Applications;
- Processes.

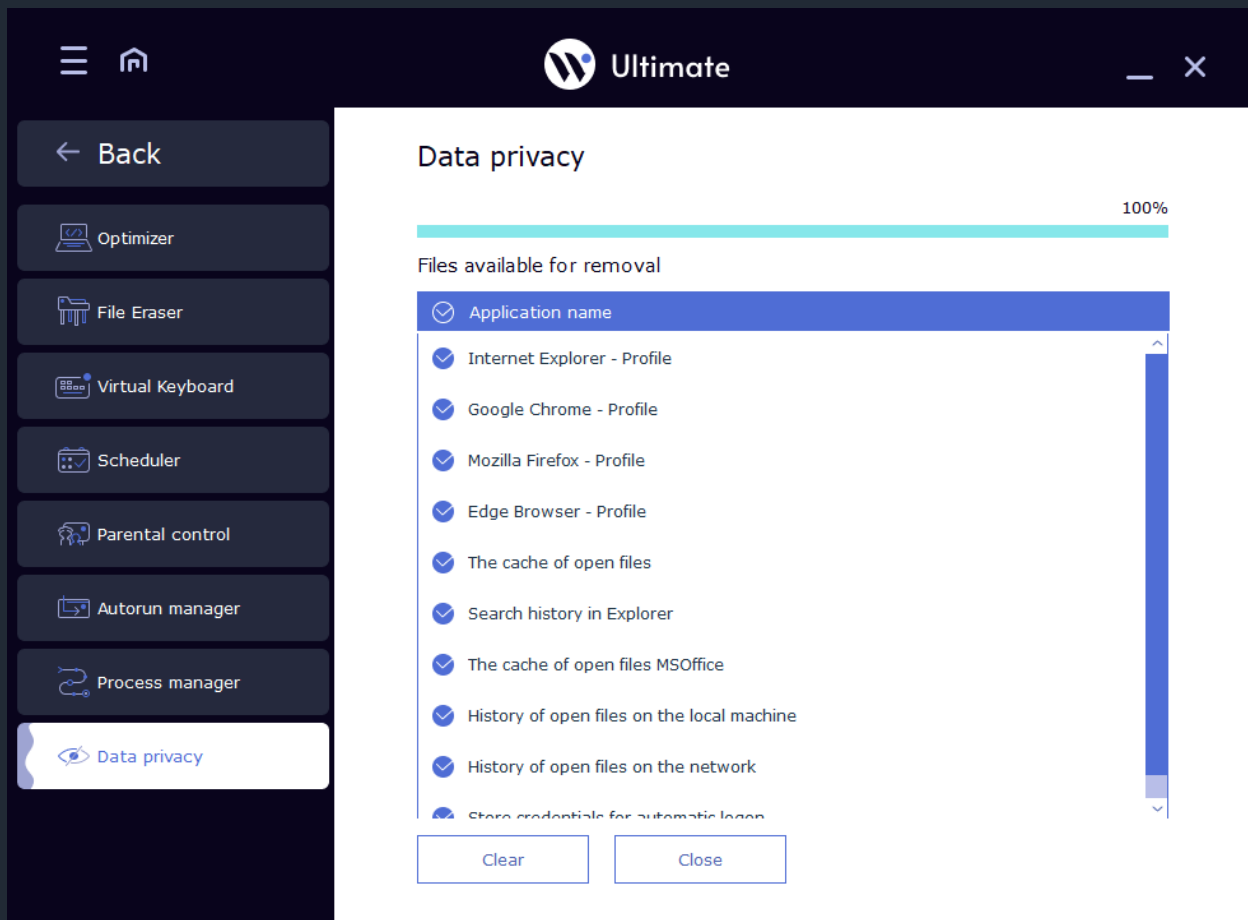


Privacy protection program allows to remove traces of the user's work on PC.



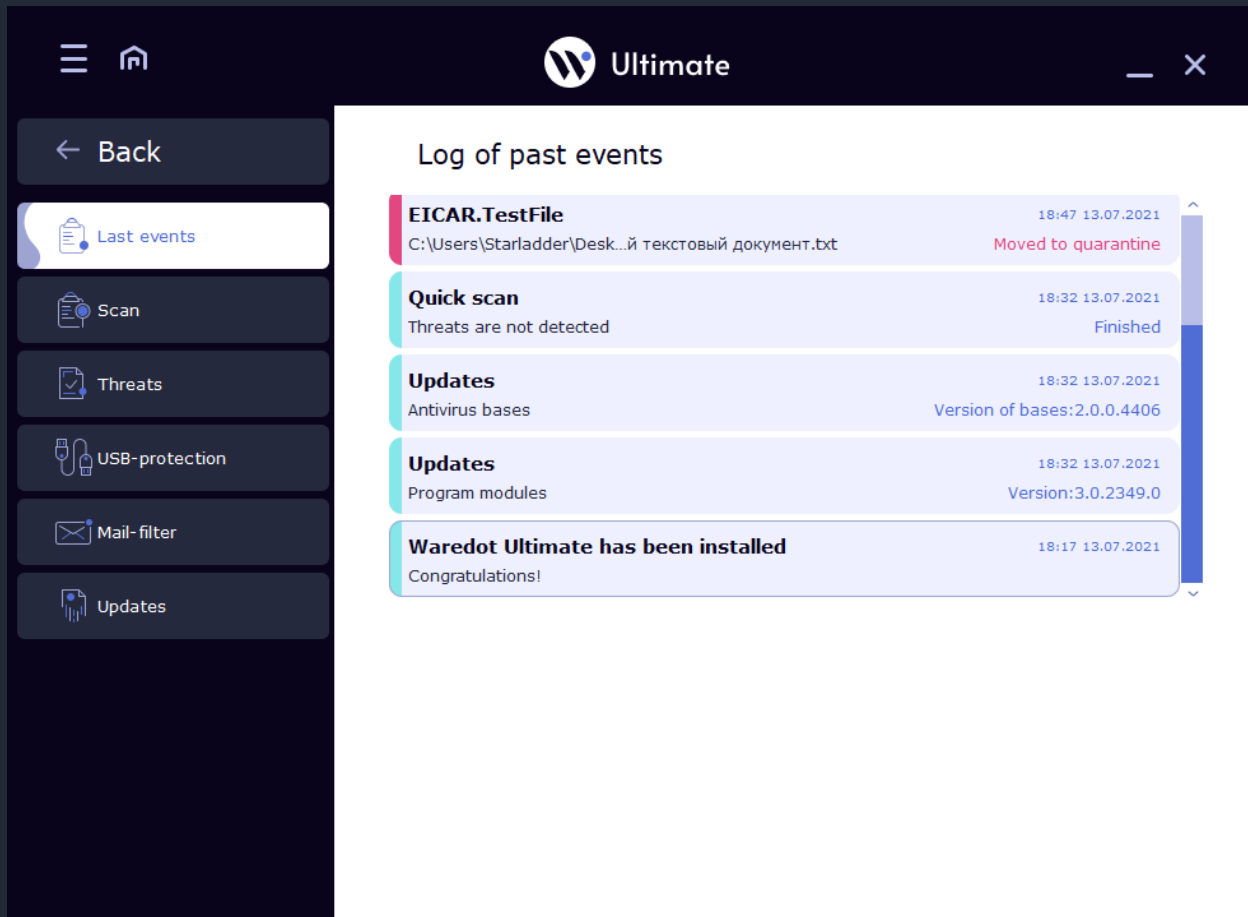
Module searches configuration and temporary files that were created during the operation of the standard software packages, and to perform their clean-up. This module allows to delete the following data:

1. Lists of documents, opened by user;
2. Temporary files;
3. Saved passwords;
4. List of popular programs;
5. Browser history.



Reports

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



The screenshot shows the Wware Ultimate application interface. On the left is a dark sidebar with navigation options: Back, Last events (selected), Scan, Threats, USB-protection, Mail-filter, and Updates. The main area displays a 'Log of past events' window with the following entries:

Event	Time	Date	Status
EICAR.TestFile C:\Users\Starladder\Desk...й текстовый документ.txt	18:47	13.07.2021	Moved to quarantine
Quick scan Threats are not detected	18:32	13.07.2021	Finished
Updates Antivirus bases	18:32	13.07.2021	Version of bases:2.0.0.4406
Updates Program modules	18:32	13.07.2021	Version:3.0.2349.0
Waredot Ultimate has been installed Congratulations!	18:17	13.07.2021	

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 W-ware Ultimate application interface. On the left is a dark sidebar with navigation options: Back, Last events, Scan (highlighted), Threats, USB-protection, Mail-filter, and Updates. The main content area is titled 'Log of past events of scanning' and contains two scan event cards:

- USB scanning** (19:24 13.07.2021): Threats are not detected. Status: Finished.
- Quick scan** (18:32 13.07.2021): Threats are not detected. Status: Finished.

Below these cards is a detailed view for a 'Quick scan' event:

Quick scan		Finished
Time of start	18:30 13.07.2021	
Took time	00:01:37	
Checked objects	14102	
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 Avast Ultimate application interface. On the left is a dark sidebar with navigation icons and labels: Back, Last events, Scan, Threats (highlighted), USB-protection, Mail-filter, and Updates. The main window has a title bar with the Avast logo and 'Ultimate' text. Below the title bar, the heading 'Log of past events with threats' is displayed. Two event cards are shown, each for 'EICAR.TestFile' detected on 13.07.2021 at 18:52 and 18:47 respectively, with the status 'Moved to quarantine'. The path for both is 'C:\Users\Starladder\Desktop\...ый текстовый документ.txt'. A detailed view of the 18:47 event is shown below, listing: Threat name (EICAR.TestFile), Threat level (indicated by a red triangle icon), Date of detection (18:47 13.07.2021), and The path (C:\Users\Starladder\Desktop\...ый текстовый документ.txt).

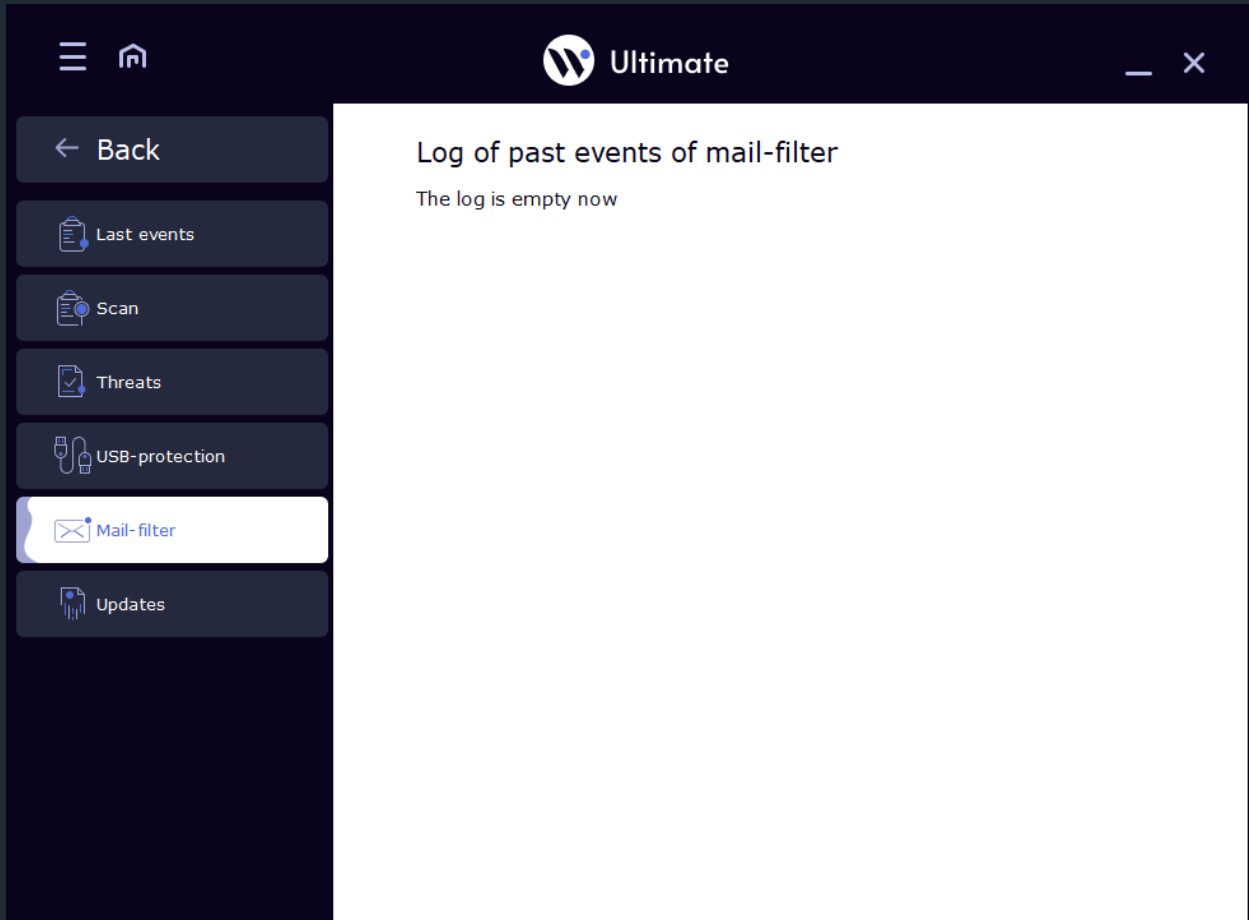


USB-protection - this tab displays the information about scanning USB pen drives, when the scan was started, how long lasted the scanning, how many files were scanned, how many files have been verified as threats, how many threats was added to the quarantine, cured or removed. Information is displayed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

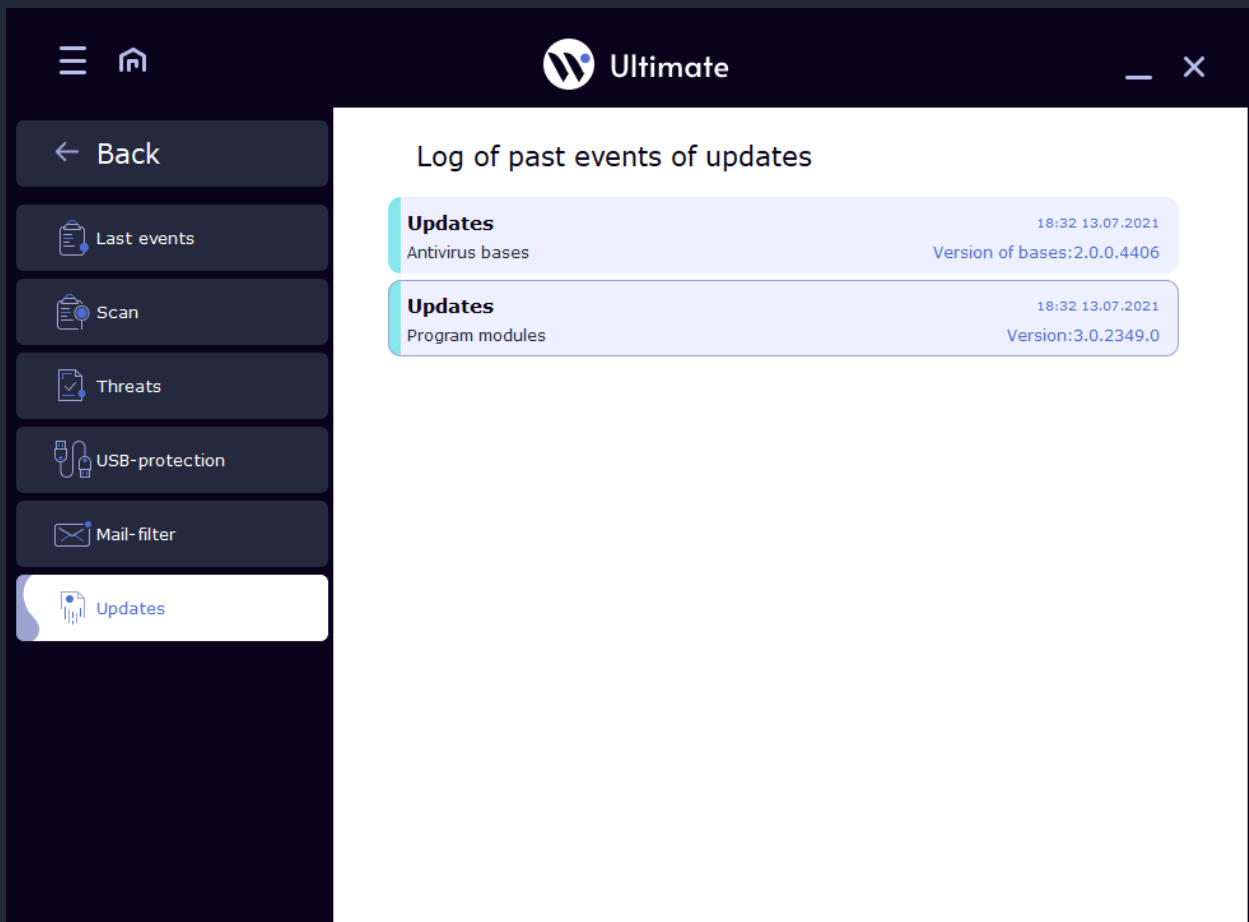
The screenshot shows the 'Ultimate' software interface. On the left is a dark sidebar with navigation options: 'Back', 'Last events', 'Scan', 'Threats', 'USB-protection' (highlighted), 'Mail-filter', and 'Updates'. The main content area is titled 'Log of past events of USB-protection'. It features a summary card for a 'USB scanning' event on 13.07.2021 at 19:24, which is 'Finished' and reports 'Threats are not detected'. Below this is a detailed table for the same event.

USB scanning		Finished
Time of start	19:24	13.07.2021
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 Ultimate

User can set up Waredot Ultimate 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.

3. Settings of **Network Protection**:
 - Inactive – disable all modules of Network protection like Antispam, Firewall, Mail-filter, Antiphishing, Web-filter etc.;
 - Recommended – provides an optimal level of Network protection. All modules of Network protection are turned on except Antispam and checking SSL-connection;
 - Maximum – provides a highest possible level of Network Protection. All modules of Network protection are turned on;
 - User – provides a level of Network Protection according to the settings which were set by user. This mode is turned on in the case user turn on or turn off some modules of Network Protection.



Ultimate

_
×

←
Back

⚙️
Quick settings

⚙️
General settings

🔍
Scan

🛡️
Guard

🔍
Inspector

🔌
USB-protection

✉️
Mail-filter

🔥
Firewall

📧
Antispam

Quick settings

The level of protection:

Minimum
Average
Maximum
User

User-defined settings individually

Notification mode:

Quiet
Recommended
Detailed
Interactive
User

Displays the main message

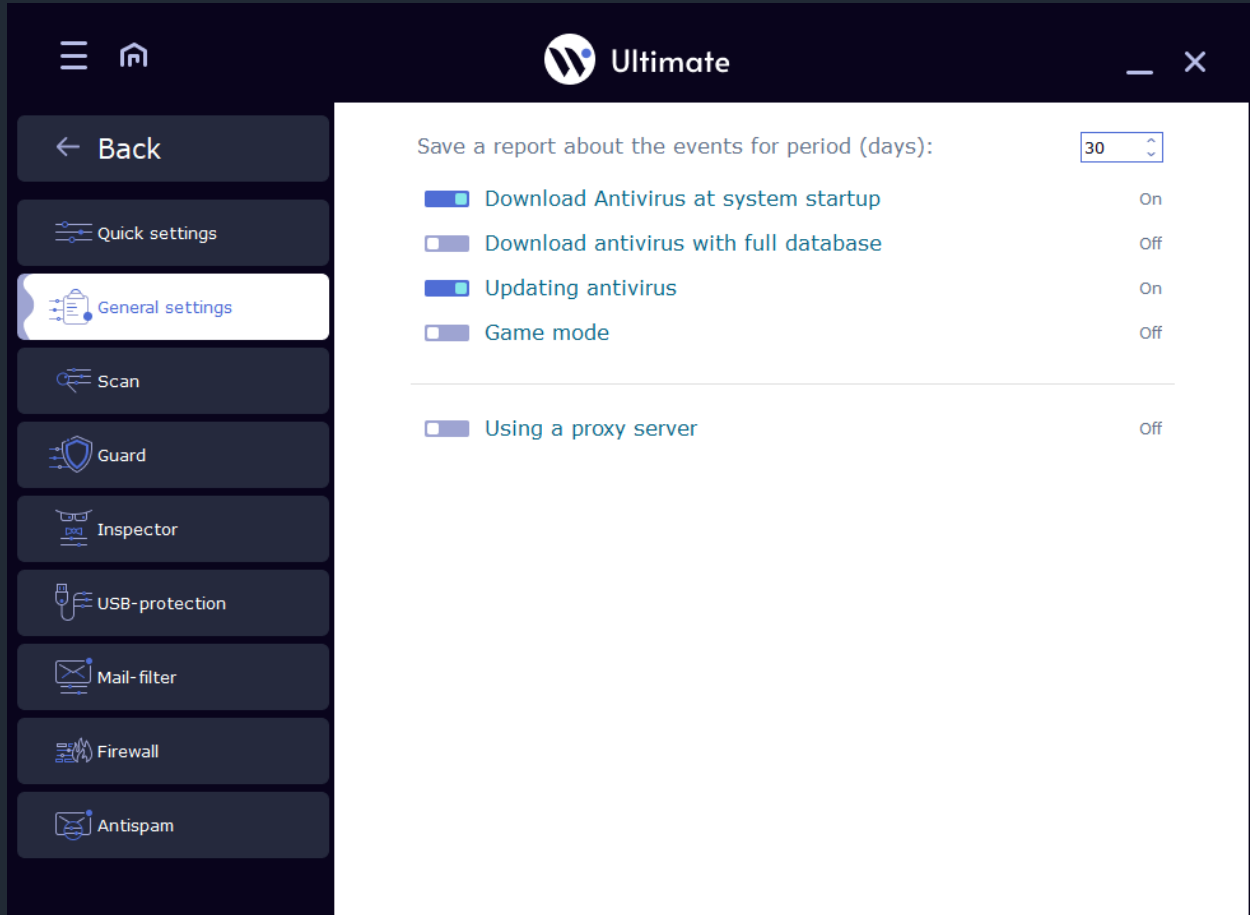
Network Protection:

Inactive
Recommended
Maximum
User

Provides optimal level firewall

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.

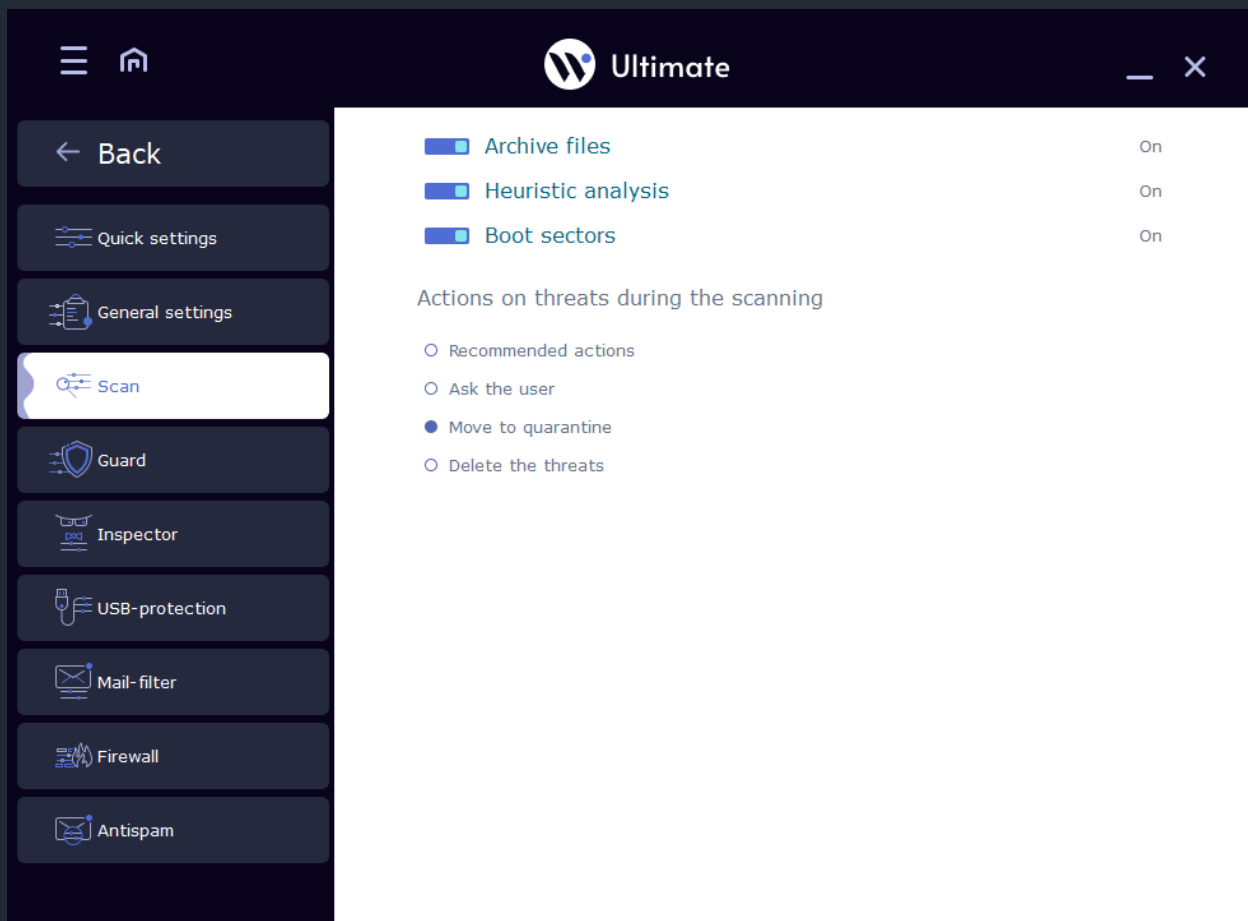
Actions on threats during the scanning:

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;

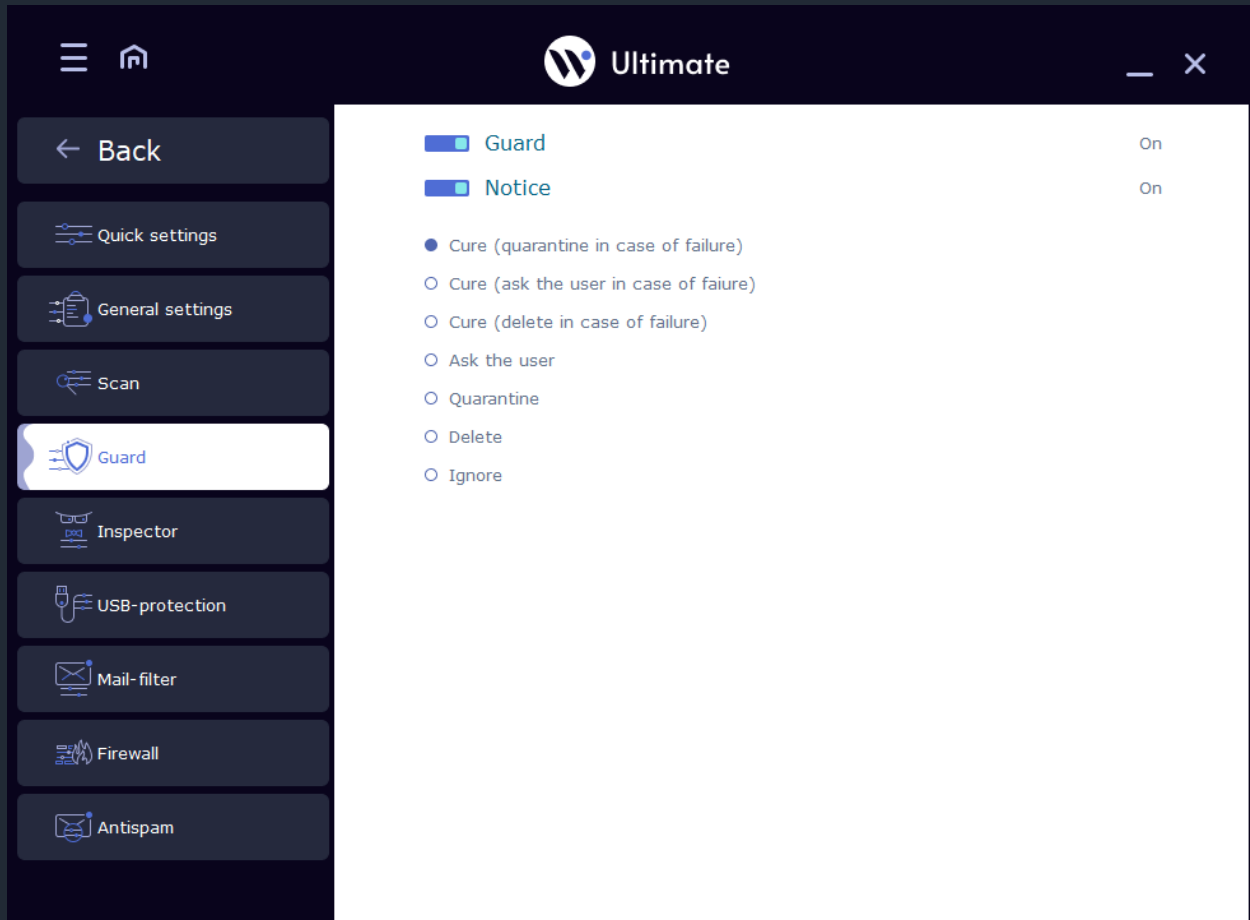
Move to quarantine – move all detected threats to quarantine of Waredot Ultimate;

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



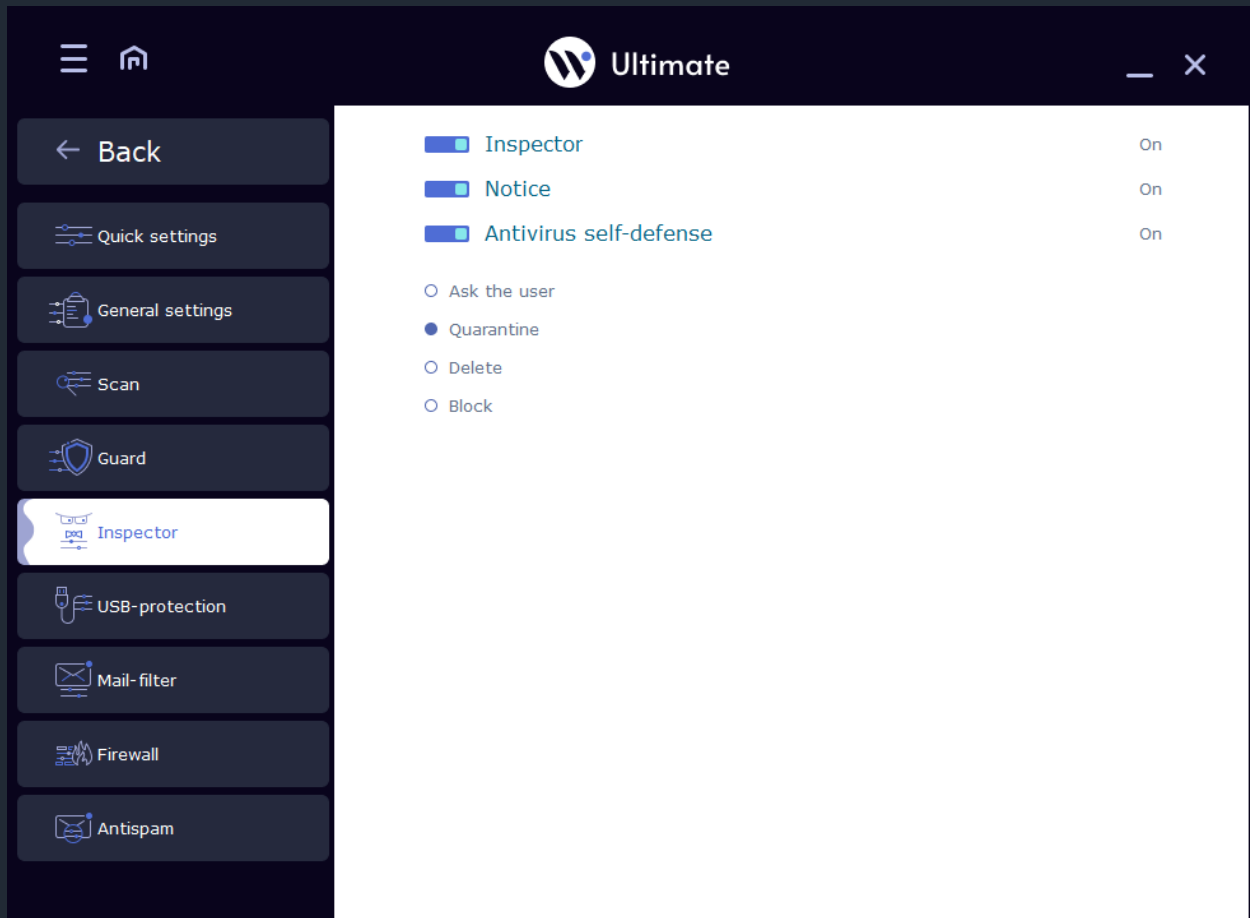
Guard (File Monitor) - continuously monitors the system for threats.

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.

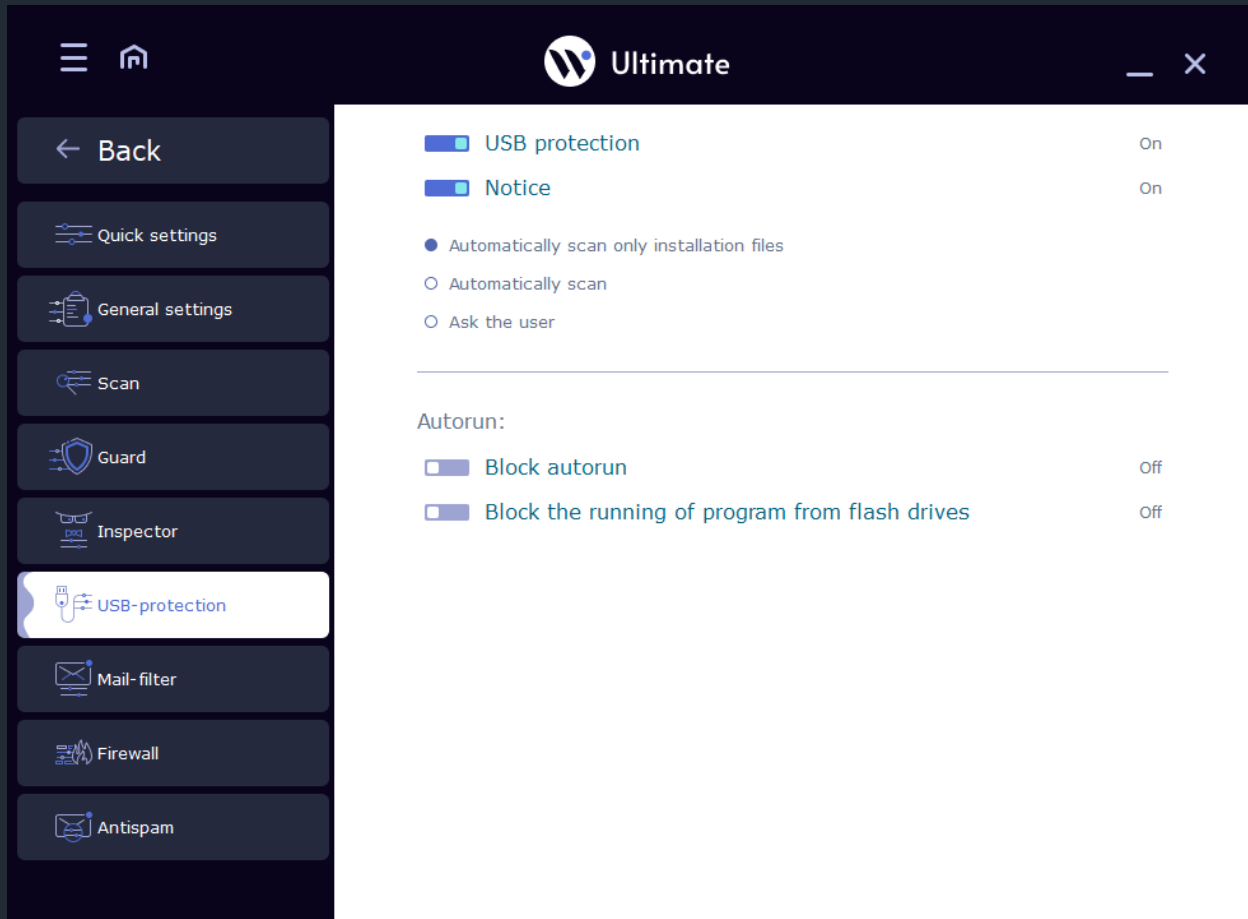
In the Settings on Inspector tab user can turn on or turn off the monitoring of the behavior of the files and programs in the real time; turn on and turn off the notifications of it; turn off and turn on Antivirus self-defense; set and change the default action for the detected threats.



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.

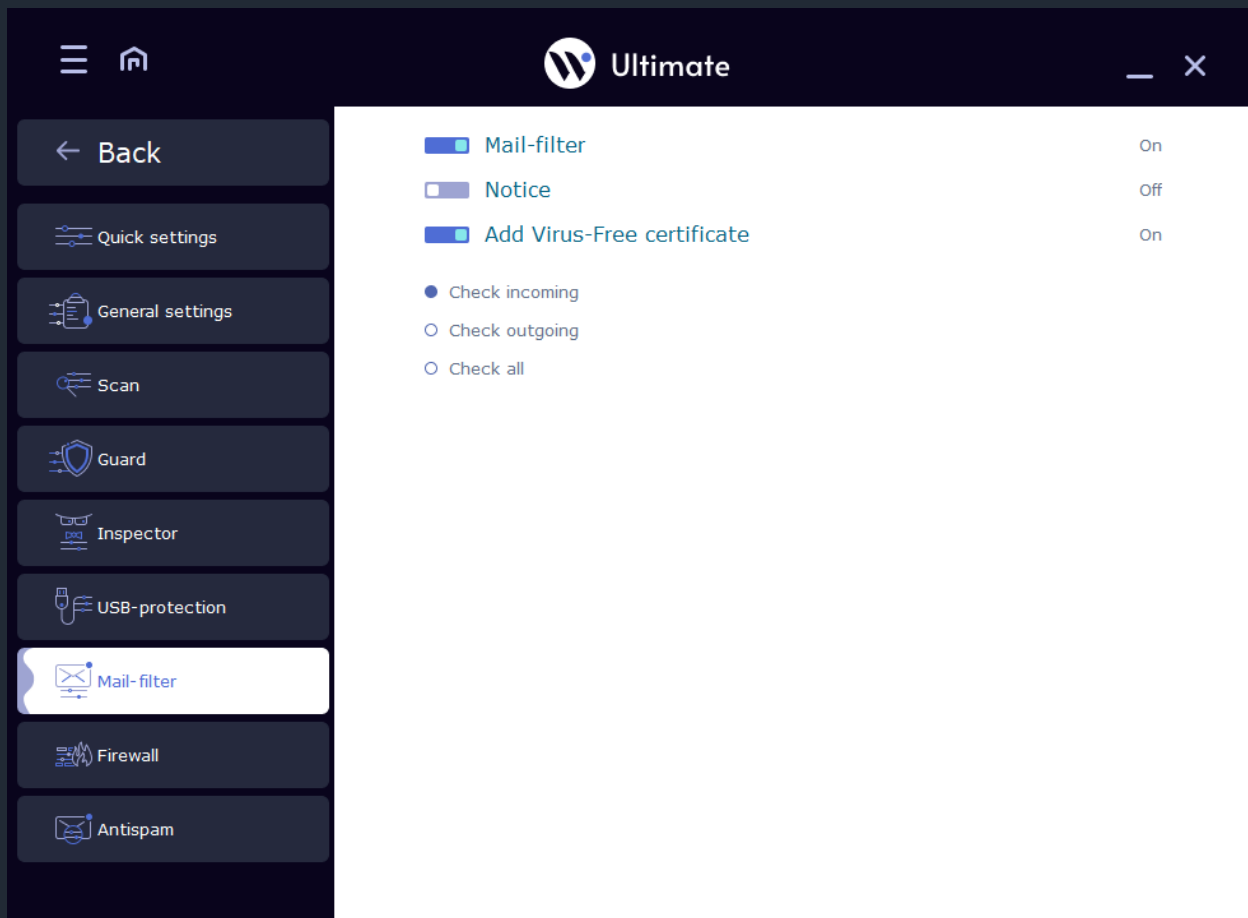


Mail – filter - scans email for threats.

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 Ultimate.

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.



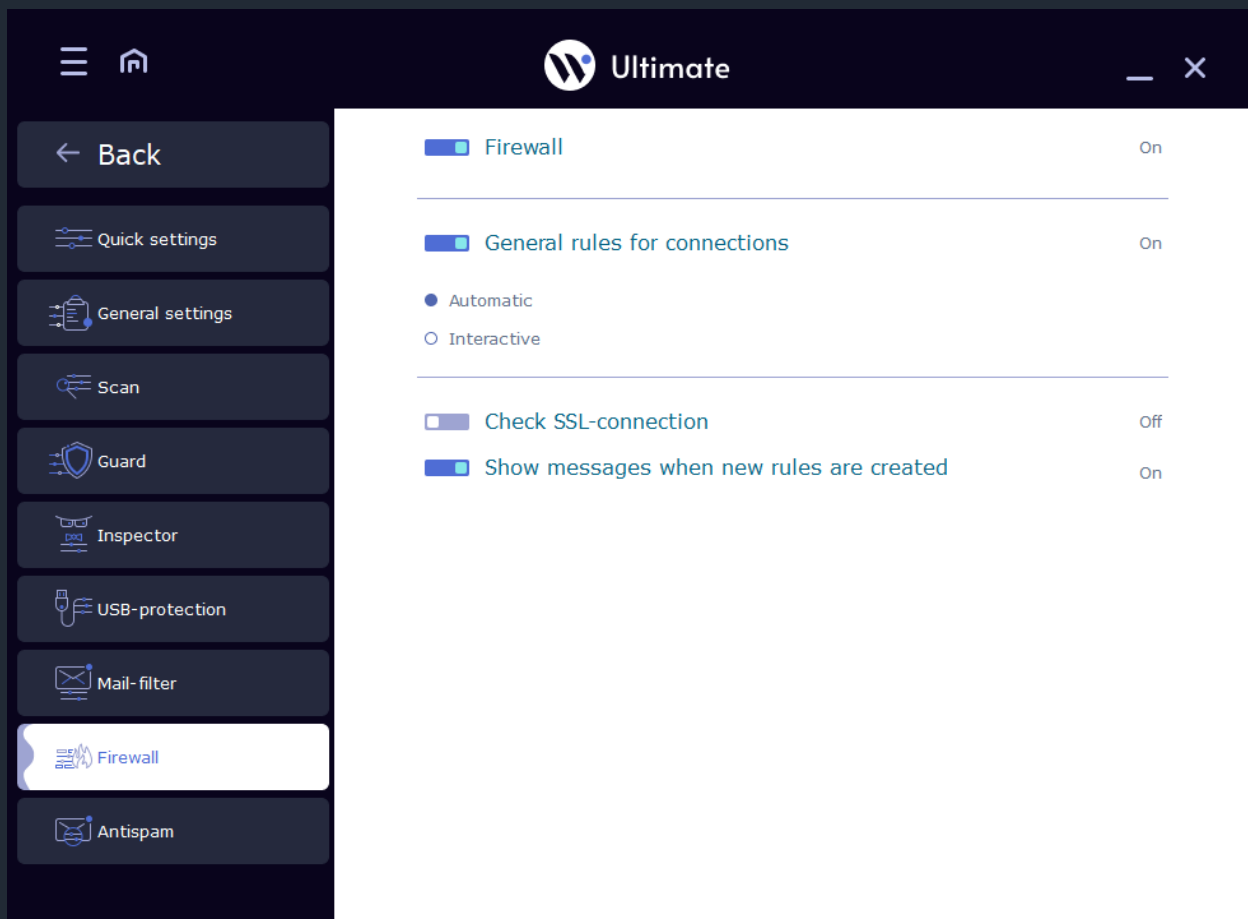
Firewall - sets the rules of incoming and outgoing connections for programs installed on your PC.

In the Settings on Firewall tab user can turn on or turn off the Firewall; set the General rules for connections:

- Automatic - Waredot Ultimate set the rule for every program according to our base of the optimal rules.
- Interactive – in this mode Waredot Ultimate shows the dialogue during every new connection of the program from user’s PC to the Internet. In this dialogue user have to choose the rule for every new connection manually.

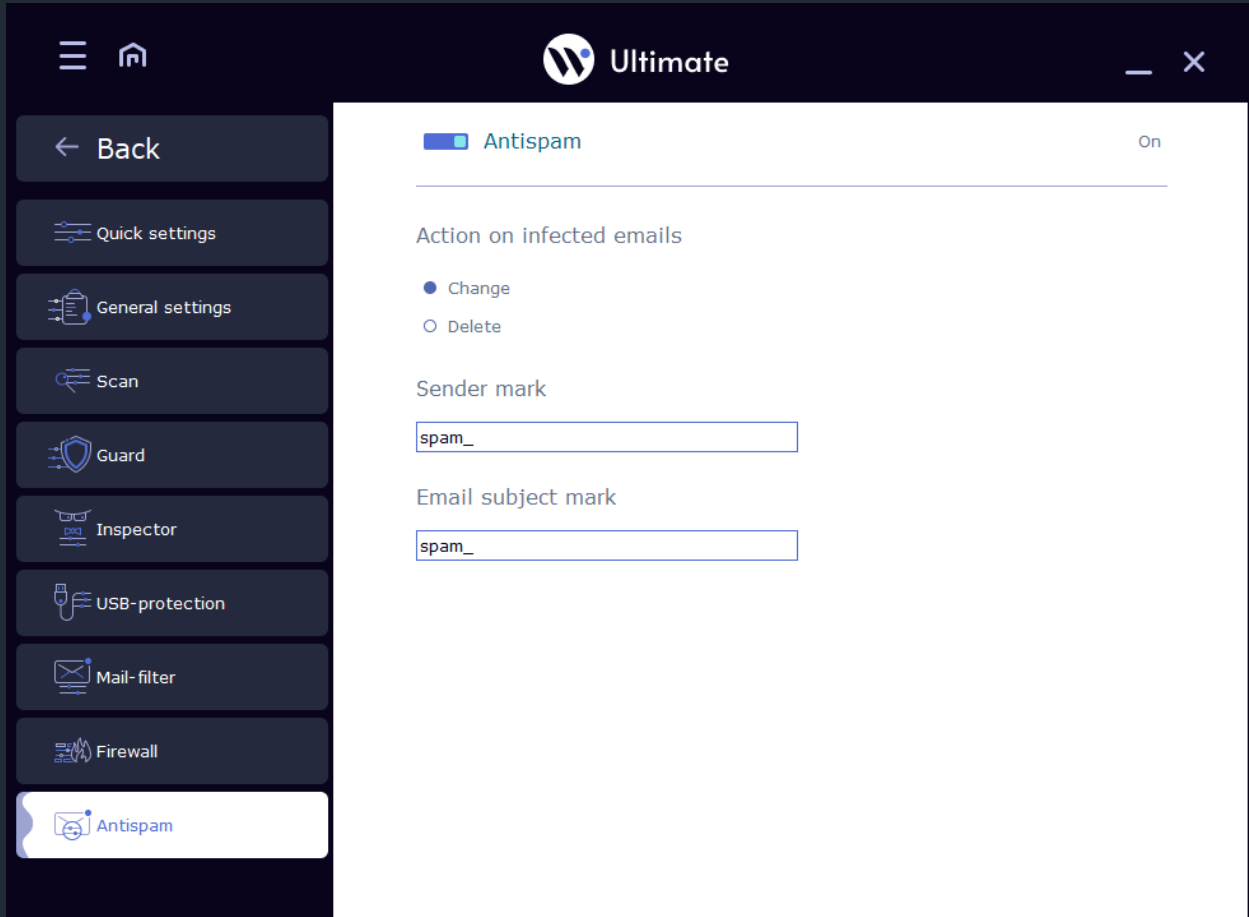
Check SSL-connection – set to check the SSL certificates.

Show messages when new rules are created – set to show the notifications after creation the rule for some software by the Firewall.



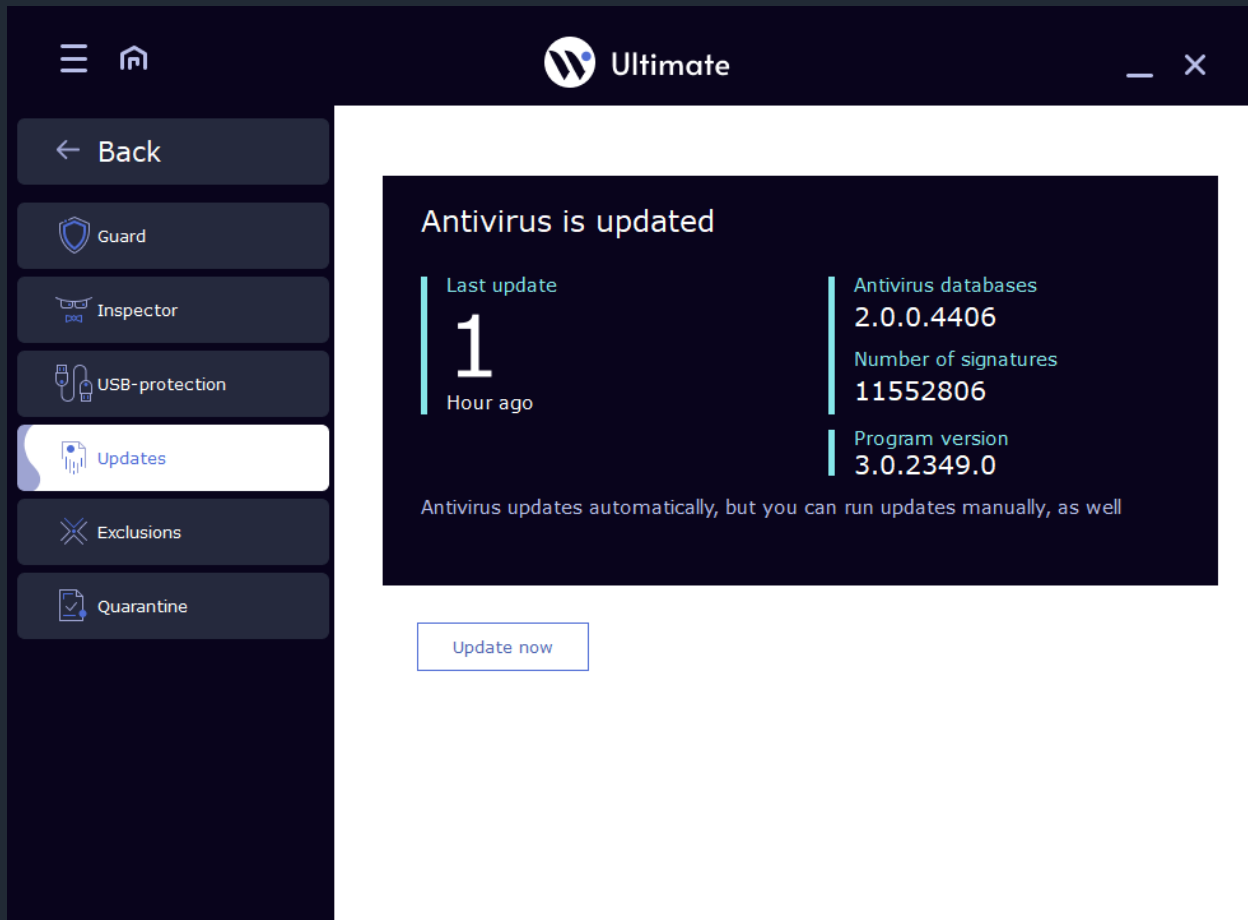
Anti-spam - blocks penetration of spam messages on the user's PC.

In the Settings on Anti-spam tab user can turn on or turn off Anti-spam protection; change the default action on the emails which contain any malware and set the marks for the emails.



Databases and Program Modules Updates

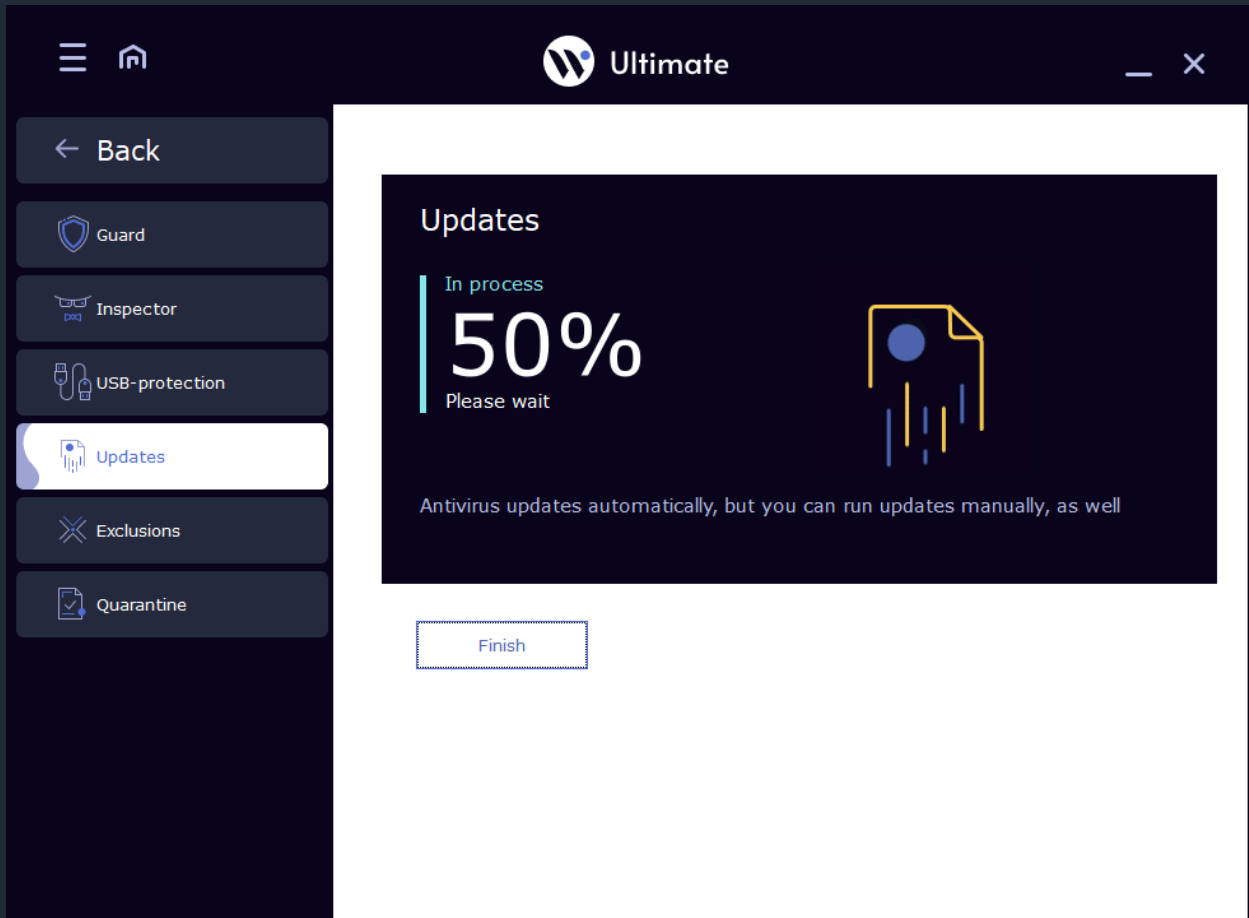
The effectiveness of antivirus product depends on how regularly virus databases are updated. Regular automatic update of databases is critically needed to keep the optimal level of protection of your computer.

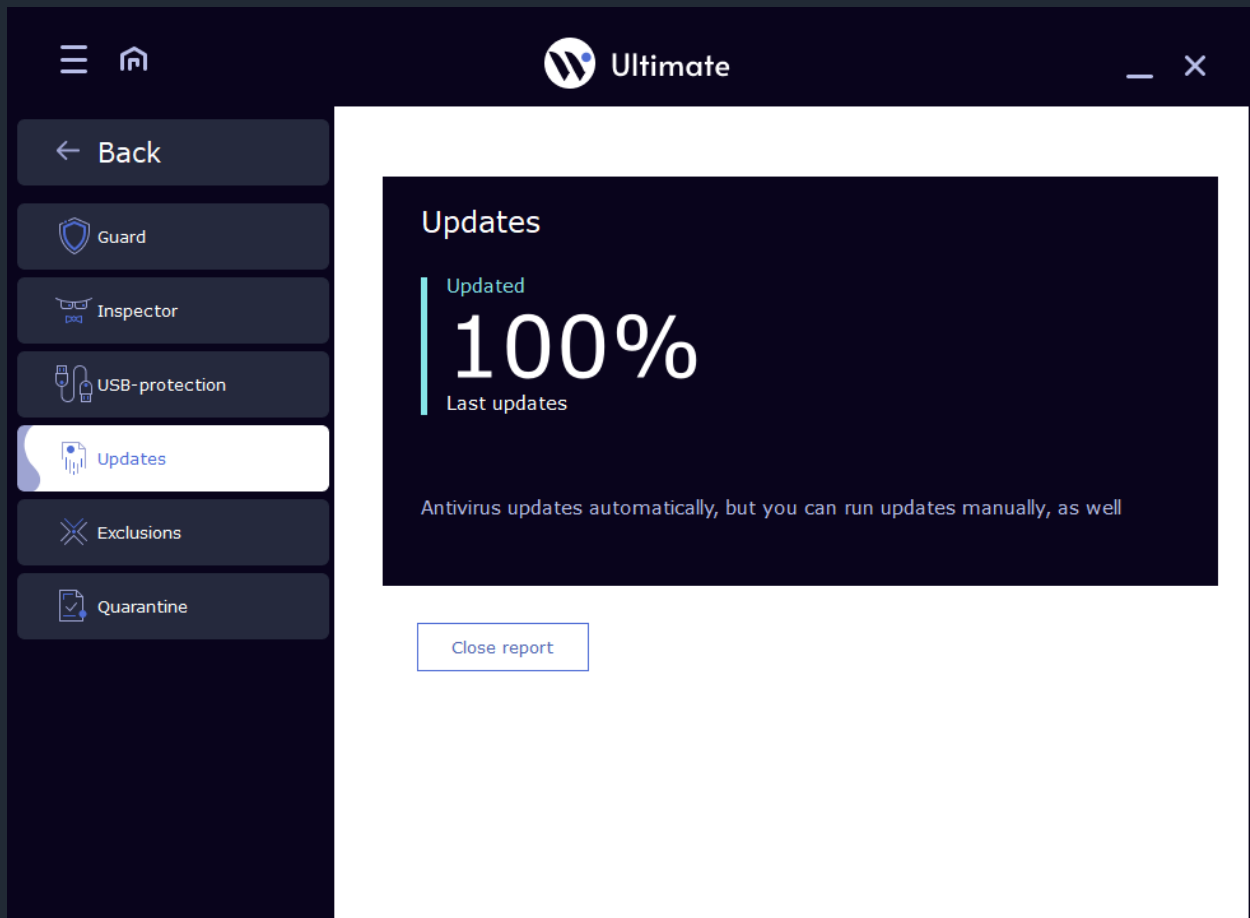


Updating takes place in two stages:

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





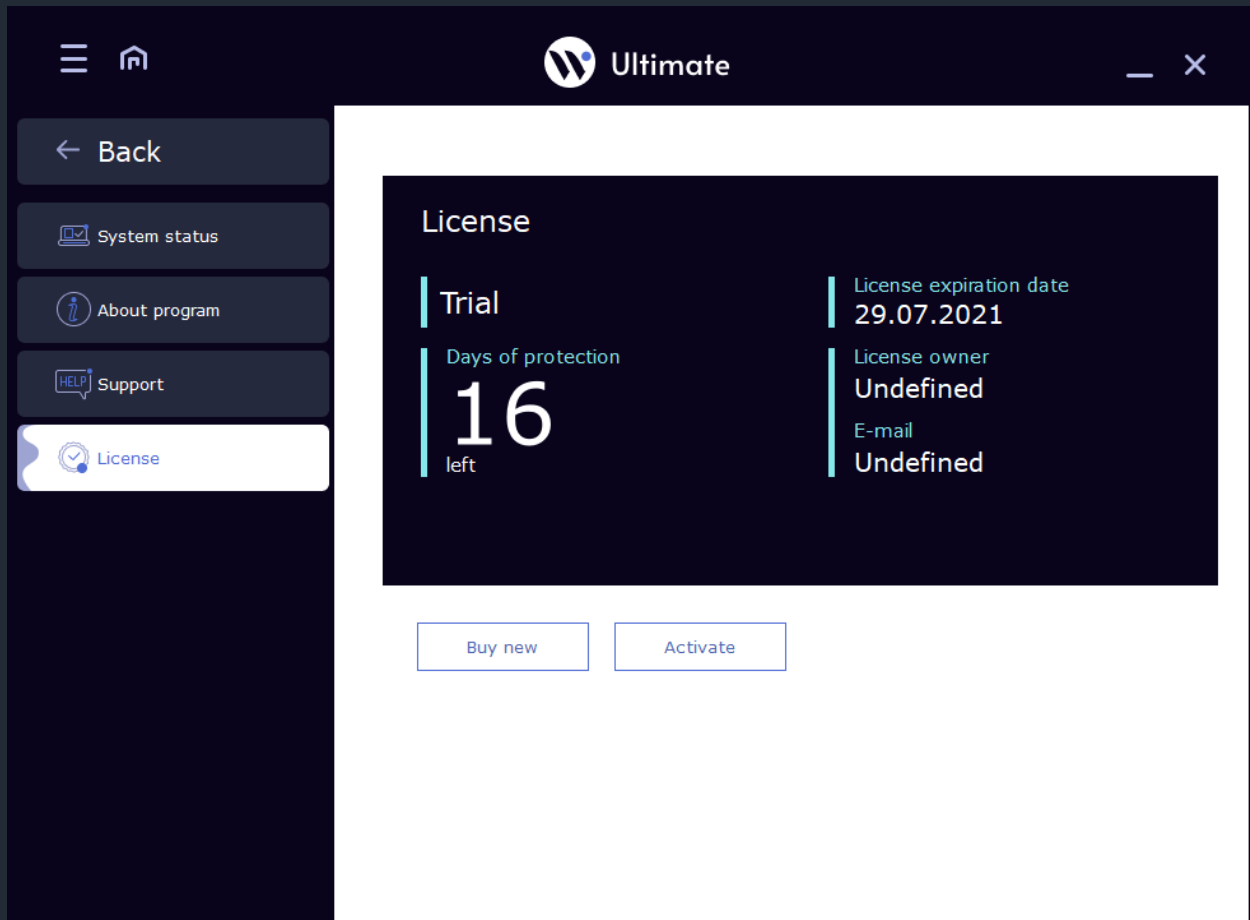


Specialists of our Antivirus Laboratory promptly react to new threats, update the antivirus bases and bases of malware. Typically, virus updates are issued 1-2 times a day. In case of epidemics our Antivirus Laboratory prepares updates in accelerated mode to protect users.

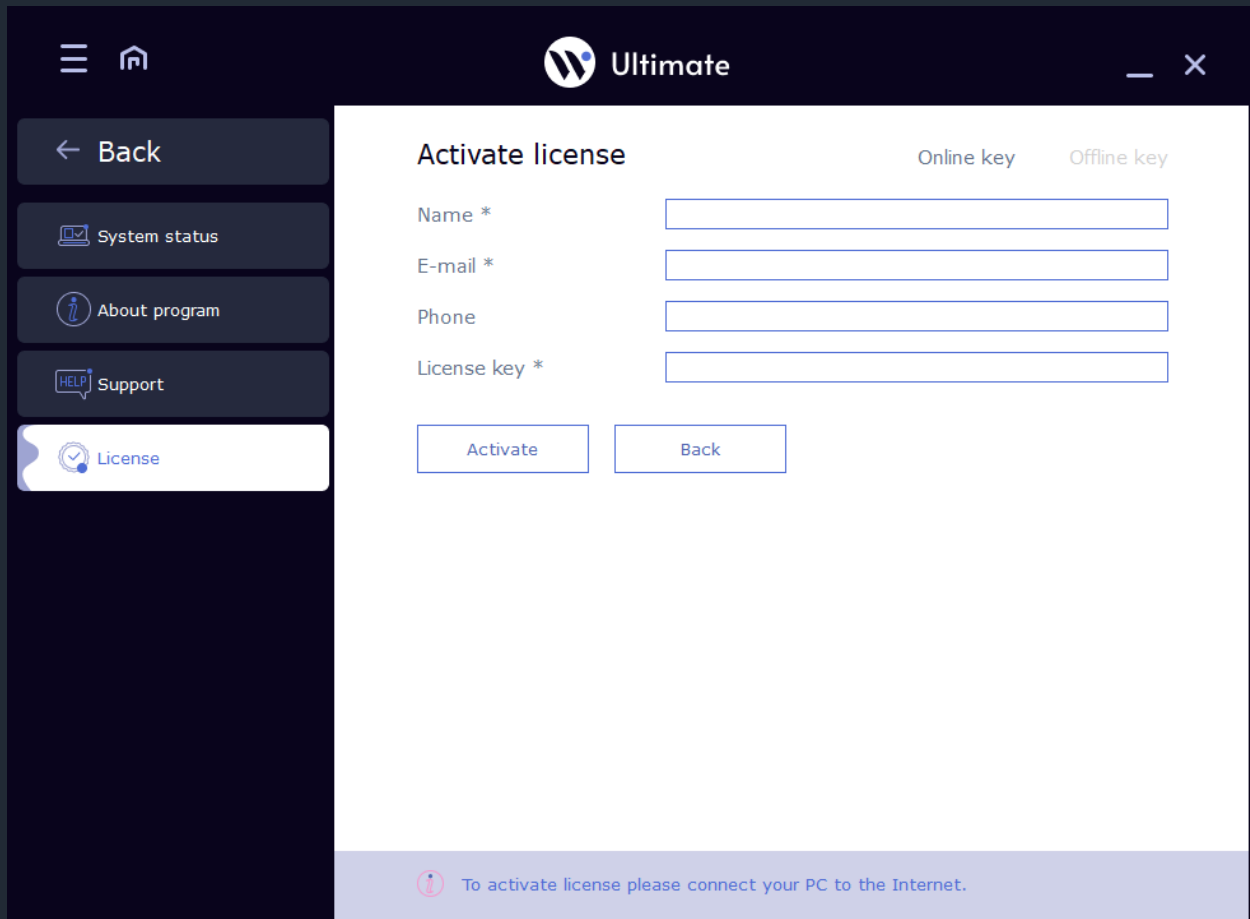
For users who do not have regular access to the Internet, it is possible to use off-line updates of antivirus.

Waredot Ultimate Registration

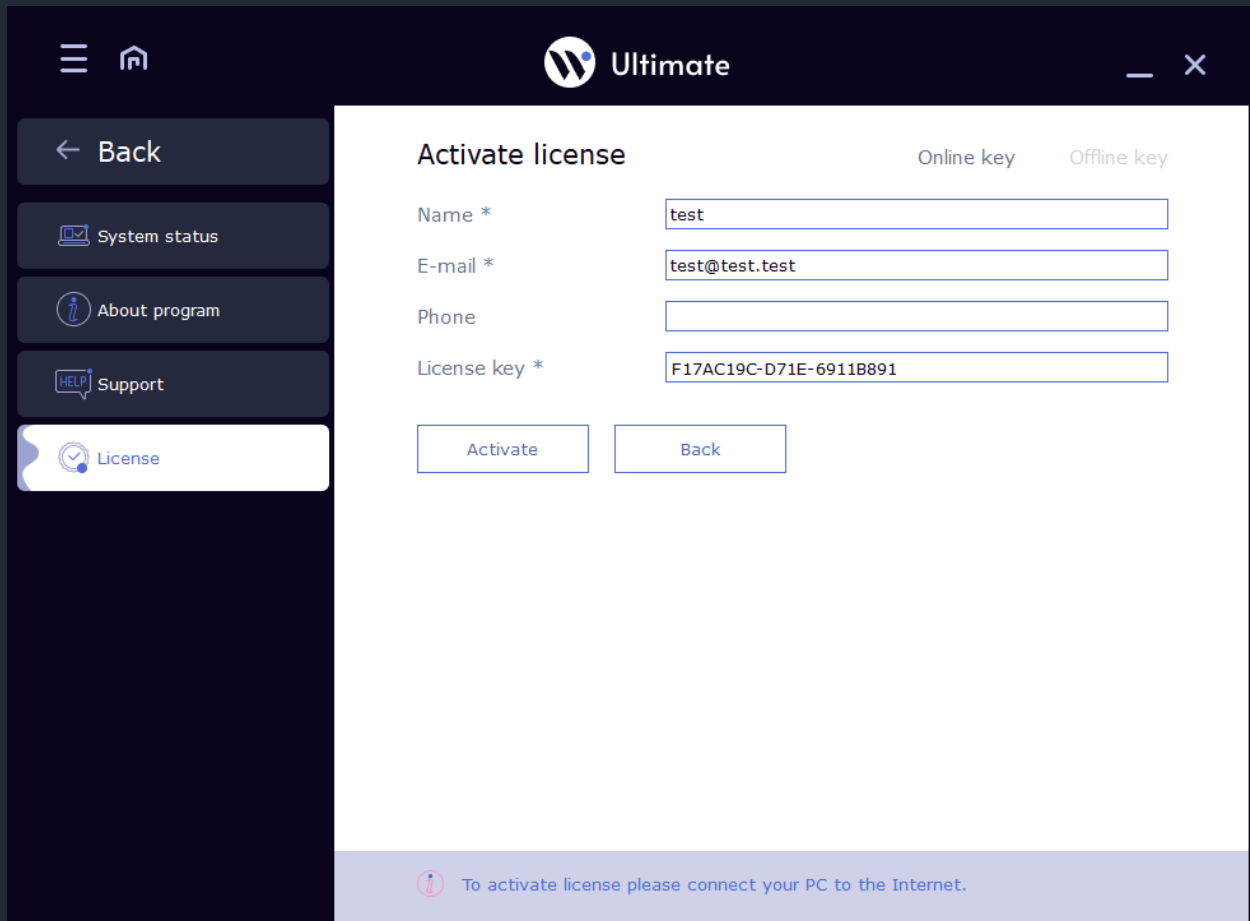
This is how unregistered program window looks like:



To register the program, open the main window of Waredot Ultimate, 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:



Ultimate

← Back

System status

About program

Support

License

Activate license

Online key Offline key

Name * test

E-mail * test@test.test

Phone

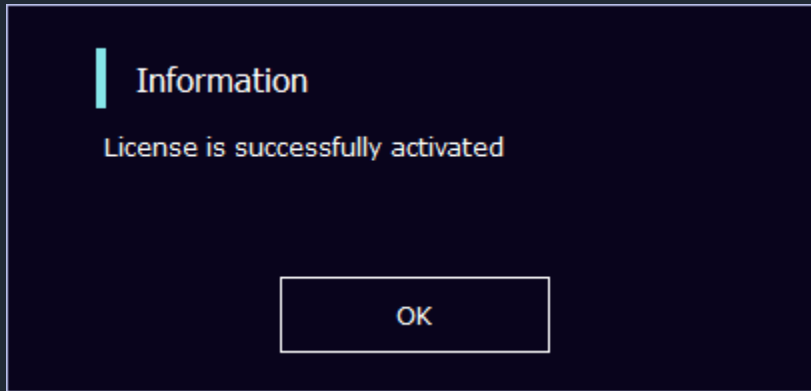
License key * F17AC19C-D71E-6911B891

Activate Back

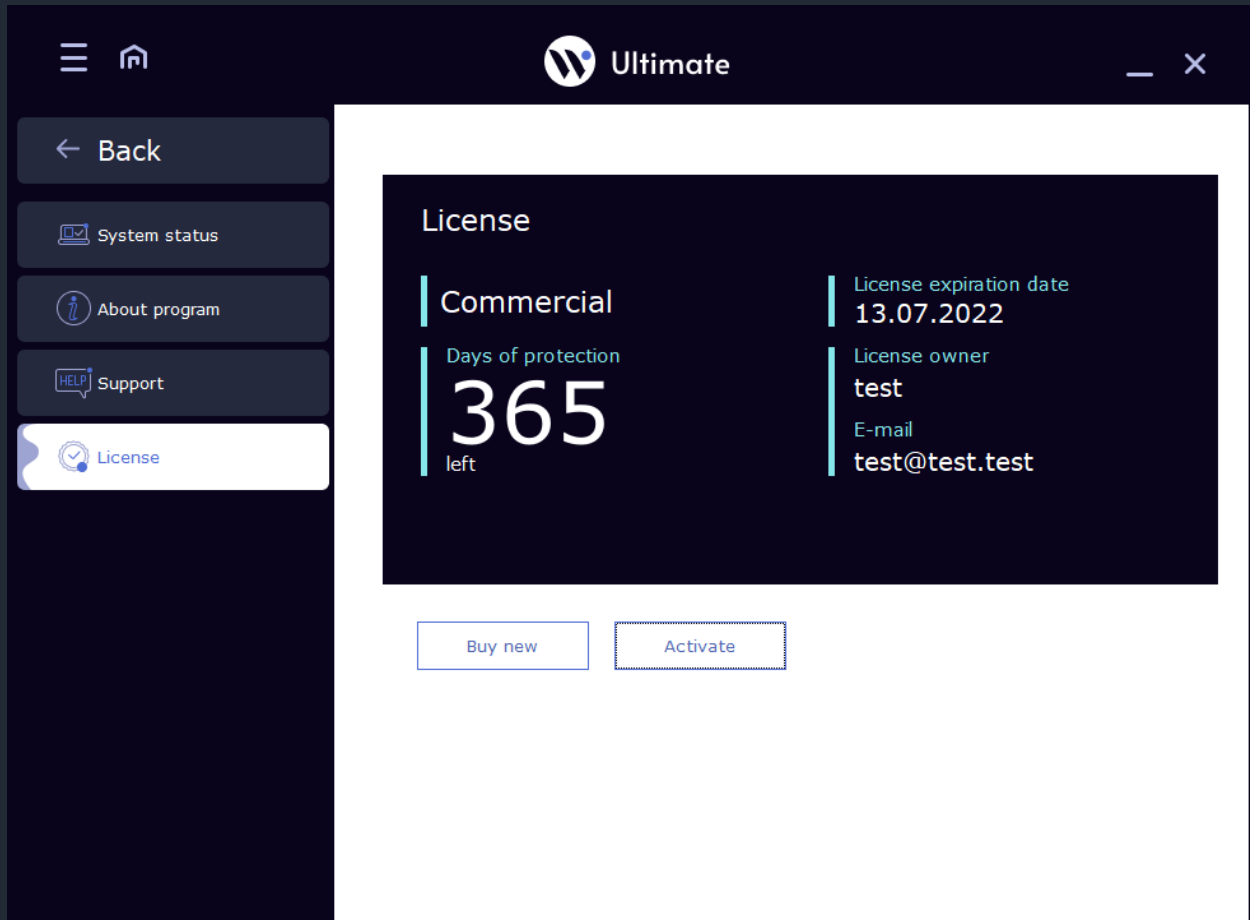
To activate license please connect your PC to the Internet.



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



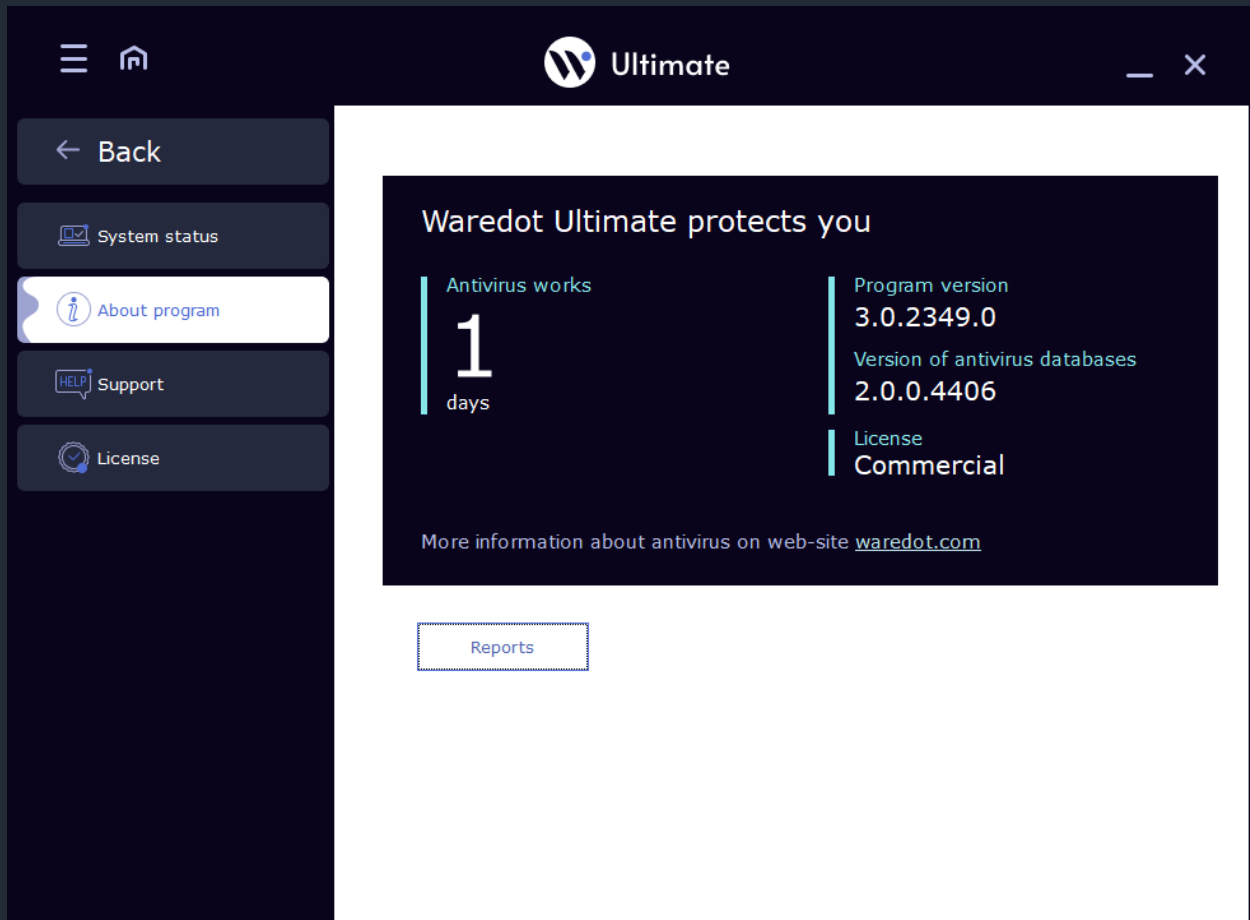
This is how the window of successful registered program looks like:



It is also possible to activate Waredot Ultimate 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 Ultimate, the version of its software modules and antivirus bases, and also specified license type (commercial or trial).



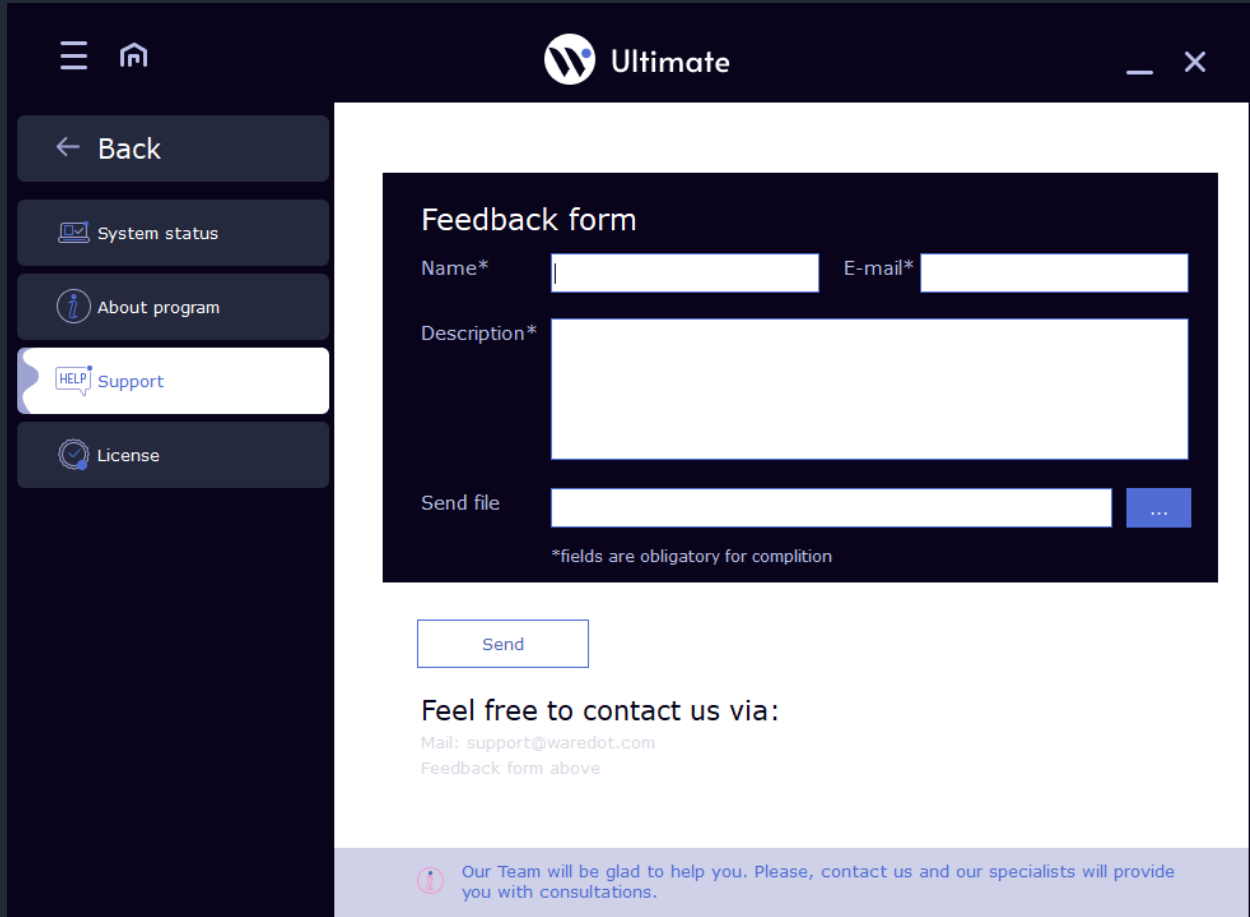
From the License tab user can go to Reports of Waredot Ultimate by clicking the button Reports.

Customer Support

If you have any questions about Waredot Ultimate 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 displays the Waredot Ultimate user interface. On the left is a dark sidebar with navigation options: 'Back', 'System status', 'About program', 'Support' (highlighted with a 'HELP' icon), and 'License'. The main content area features a 'Feedback form' with the following fields: 'Name*' (text input), 'E-mail*' (text input), 'Description*' (text area), and 'Send file' (file input with a blue '...' button). A note below the form states '*fields are obligatory for completion'. Below the form is a 'Send' button. Further down, the text 'Feel free to contact us via:' is followed by 'Mail: support@waredot.com' and 'Feedback form above'. At the bottom, a light blue banner contains an information icon and the text: 'Our Team will be glad to help you. Please, contact us and our specialists will provide you with consultations.'