Waredot Total Protection

USER GUIDE

CONTENTS

Introduction 3

Waredot Total Protection System Requirements 4

Installation of Waredot Total Protection 5

System Status 11

System Scanning 15

When Waredot Total Protection finds the threats 19

Modules of the antivirus protection 21

Modules of the Network protection

Tools 41

Reports 46

Settings of Waredot Total Protection 52

Databases and program modules updates 62

Waredot Total Protection registration 65

Customer support 71

Introduction

Dear user!

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

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

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

Waredot Total Protection System Requirements

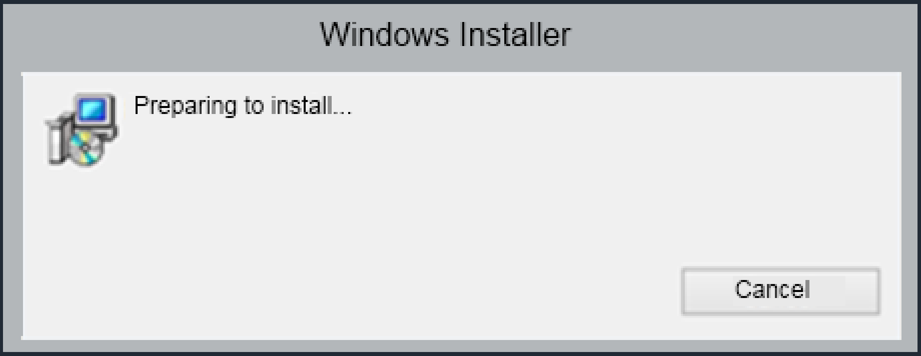
Minimal system requirements for Waredot Total Protection:

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 Total Protection

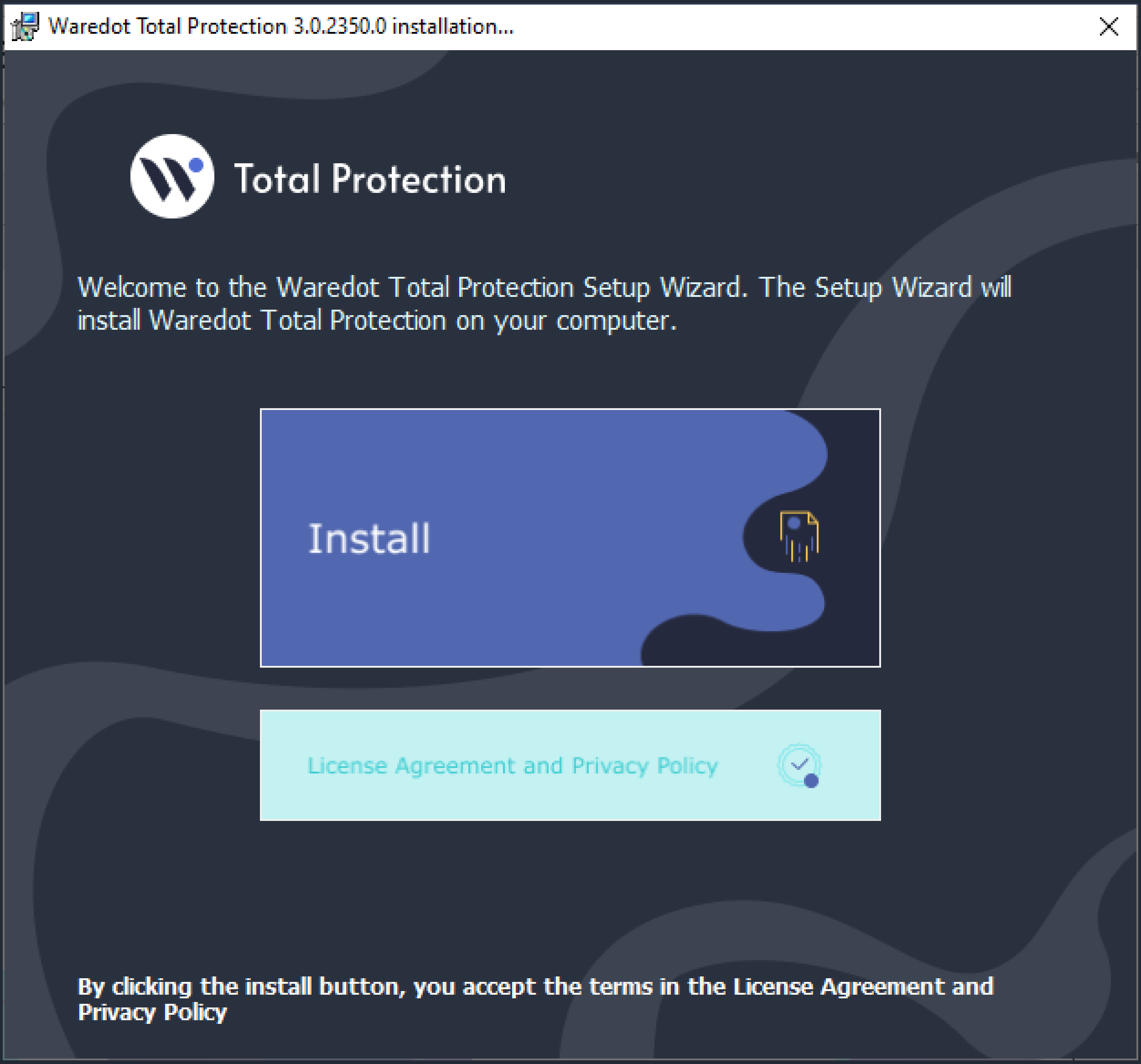
Proper installation of Waredot Total Protection is provided by Waredot Total Protection Installation Wizard. You just need to follow the wizard.

Preparing to install


Windows Installer

Preparing to install...

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

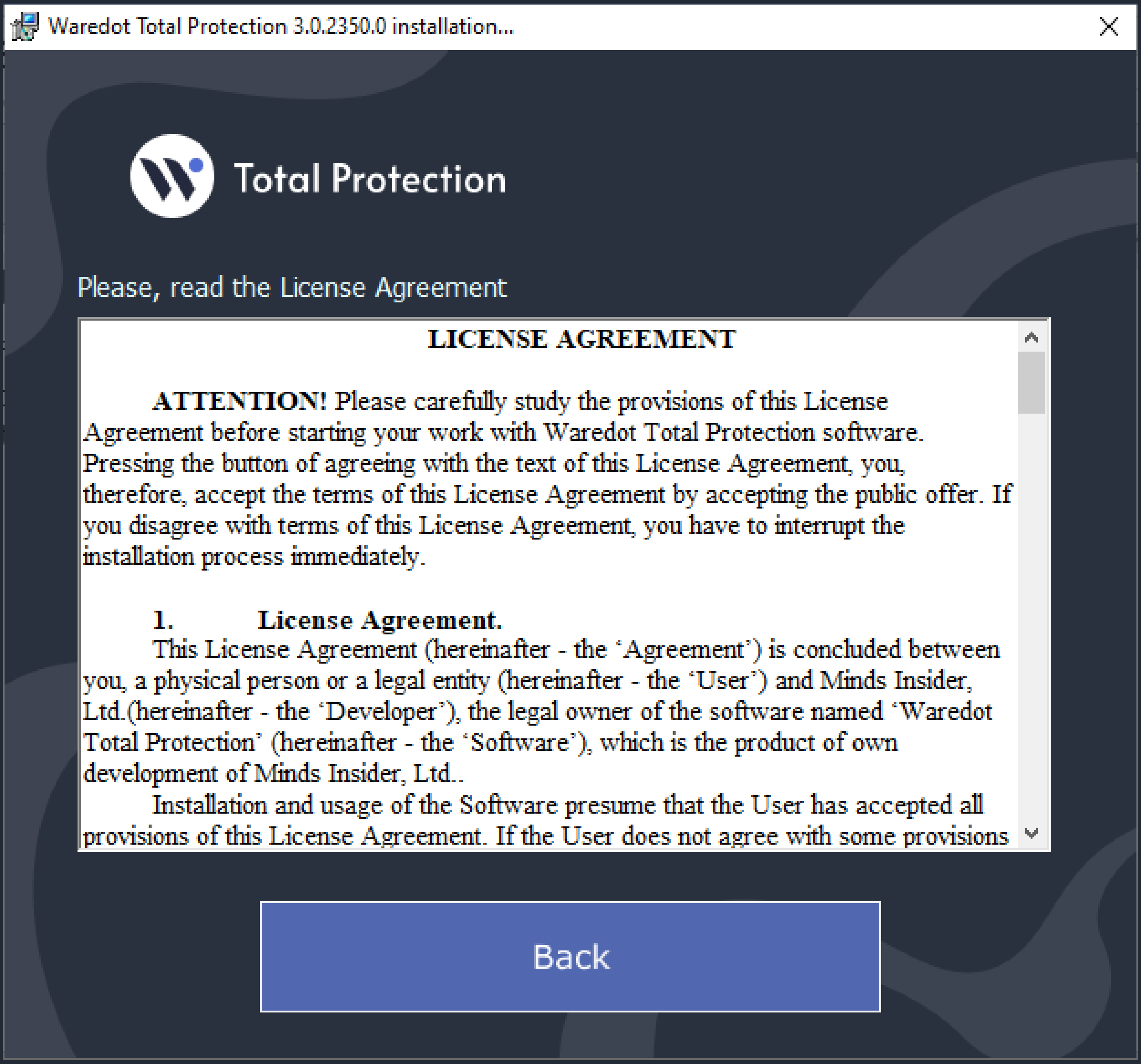


Waredot Total Protection 3.0.2350.0 installation...

Welcome to the Waredot Total Protection Setup Wizard. The Setup Wizard will install Waredot Total Protection on your computer.

By clicking the install button, you accept the terms in the License Agreement and Privacy Policy

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.


Waredot Total Protection 3.0.2350.0 installation...
Total Protection
Please, read the License Agreement
Back

LICENSE AGREEMENT

ATTENTION! Please carefully study the provisions of this License Agreement before starting your work with Waredot Total Protection software. Pressing the button of agreeing with the text of this License Agreement, you, therefore, accept the terms of this License Agreement by accepting the public offer. If you disagree with terms of this License Agreement, you have to interrupt the installation process immediately.

1. License Agreement.

This License Agreement (hereinafter - the 'Agreement') is concluded between you, a physical person or a legal entity (hereinafter - the 'User') and Minds Insider, Ltd.(hereinafter - the 'Developer'), the legal owner of the software named 'Waredot Total Protection' (hereinafter - the 'Software'), which is the product of own development of Minds Insider, Ltd..

Installation and usage of the Software presume that the User has accepted all provisions of this License Agreement. If the User does not agree with some provisions

ATTENTION

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

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.

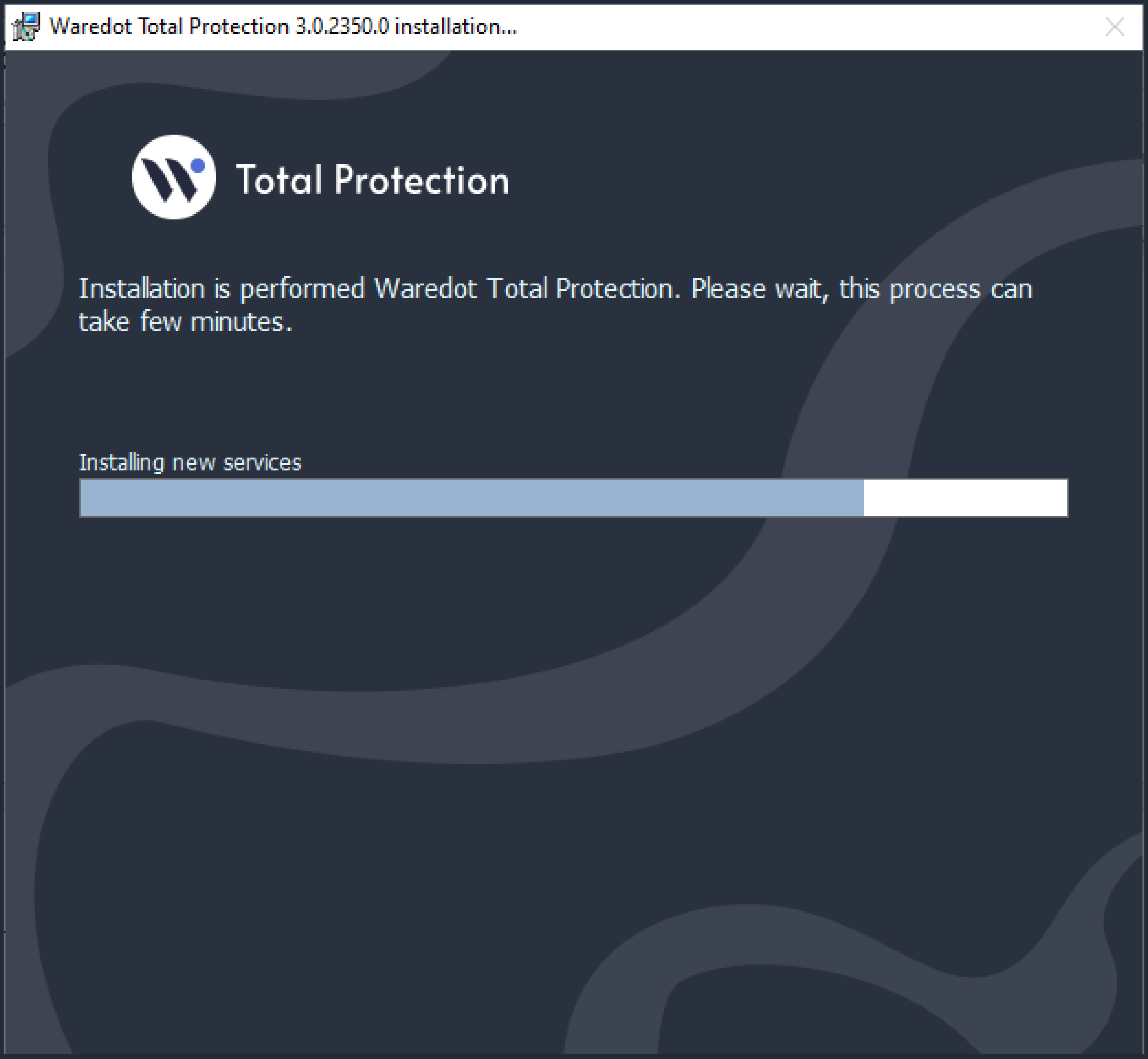
Also, before installing Waredot Total Protection you should remove its previous version.

To remove an old version of Waredot Total Protection (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.

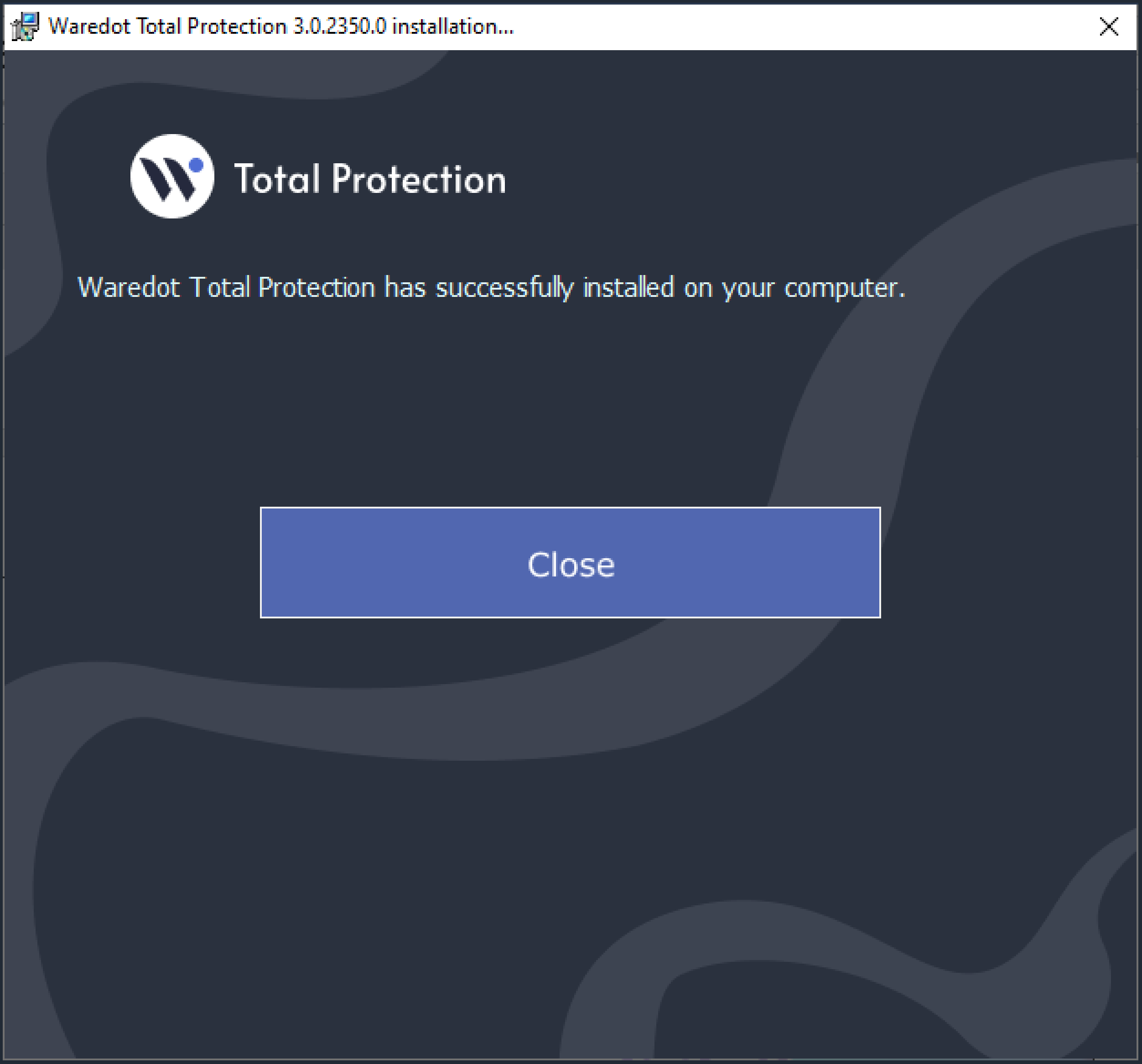


Waredot Total Protection 3.0.2350.0 installation...

Installation is performed Waredot Total Protection. Please wait, this process can take few minutes.

Installing new services

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



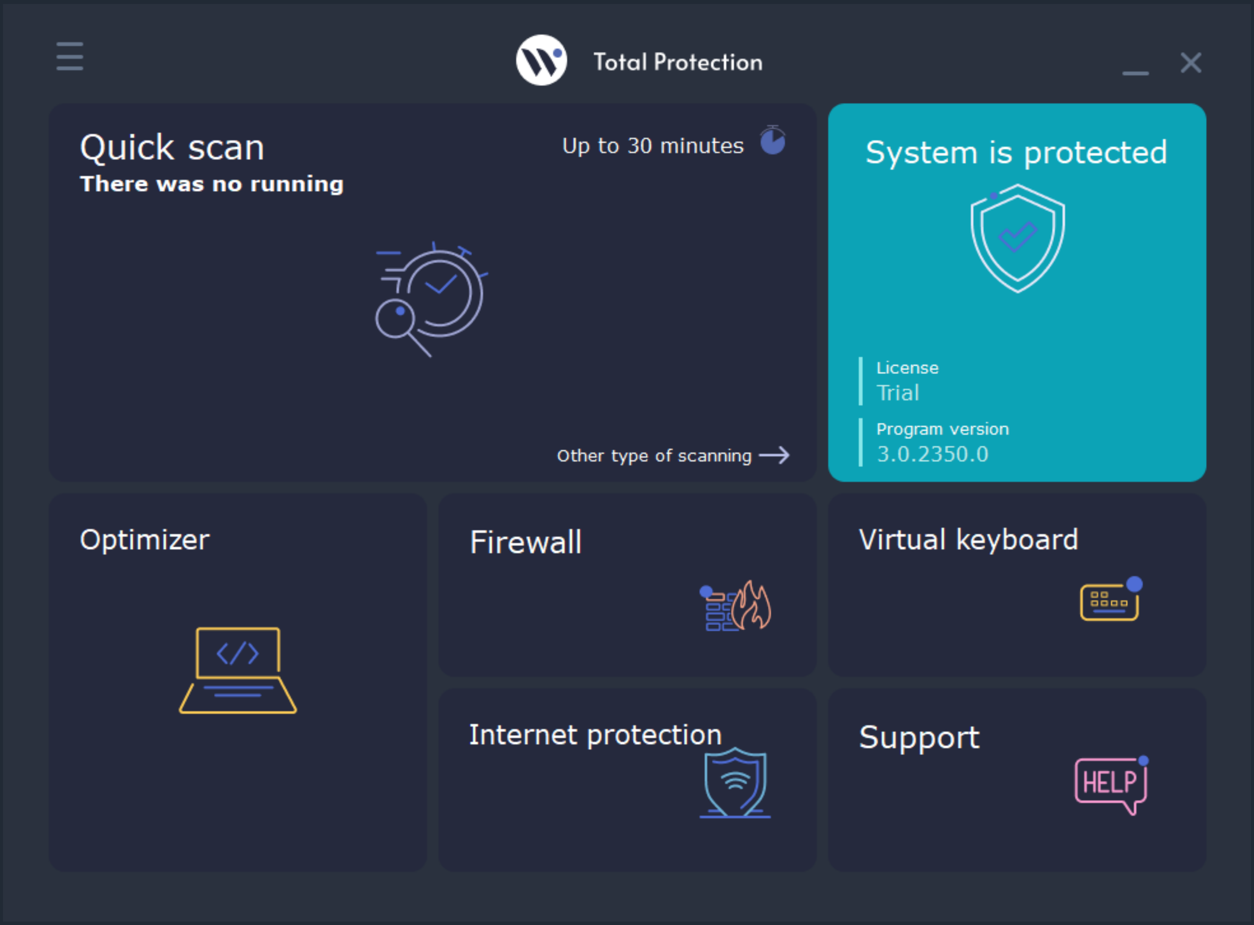
Waredot Total Protection 3.0.2350.0 installation...

Waredot Total Protection has successfully installed on your computer.

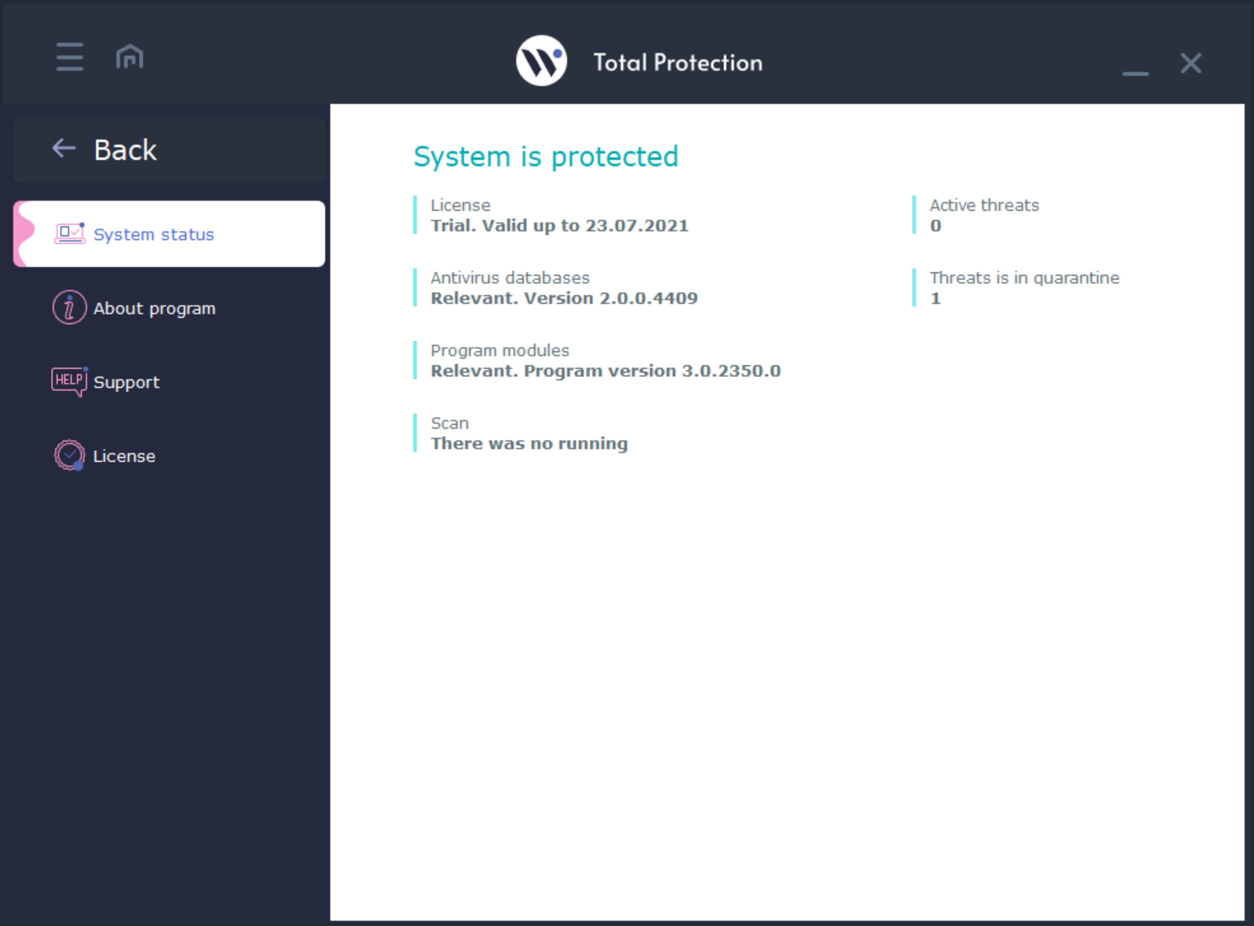
System Status

Waredot Total Protection 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:



System is protected

License
Trial. Valid up to 23.07.2021

Antivirus databases
Relevant. Version 2.0.0.4409

Program modules
Relevant. Program version 3.0.2350.0

Scan
There was no running

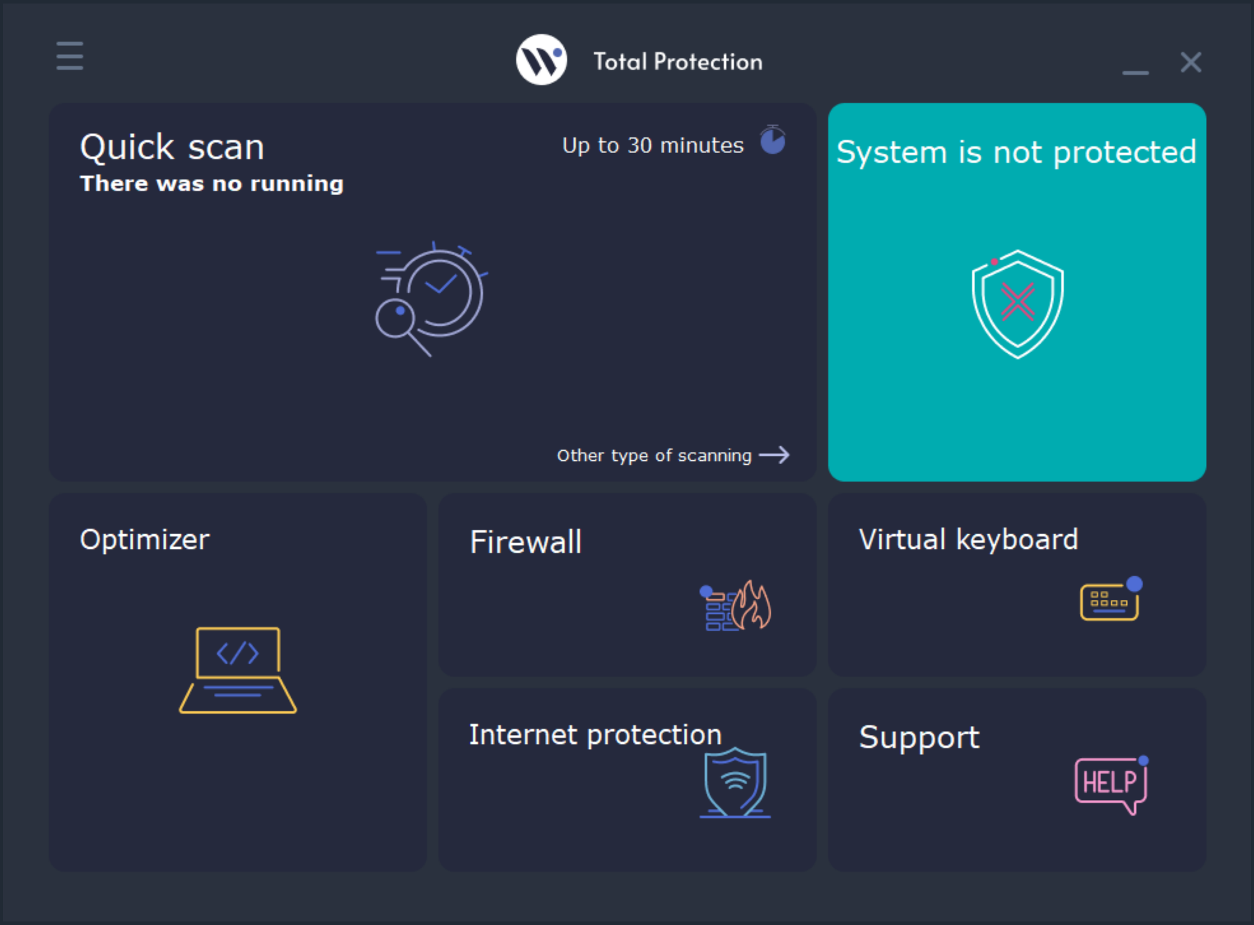
Active threats
0

Threats is in quarantine
1

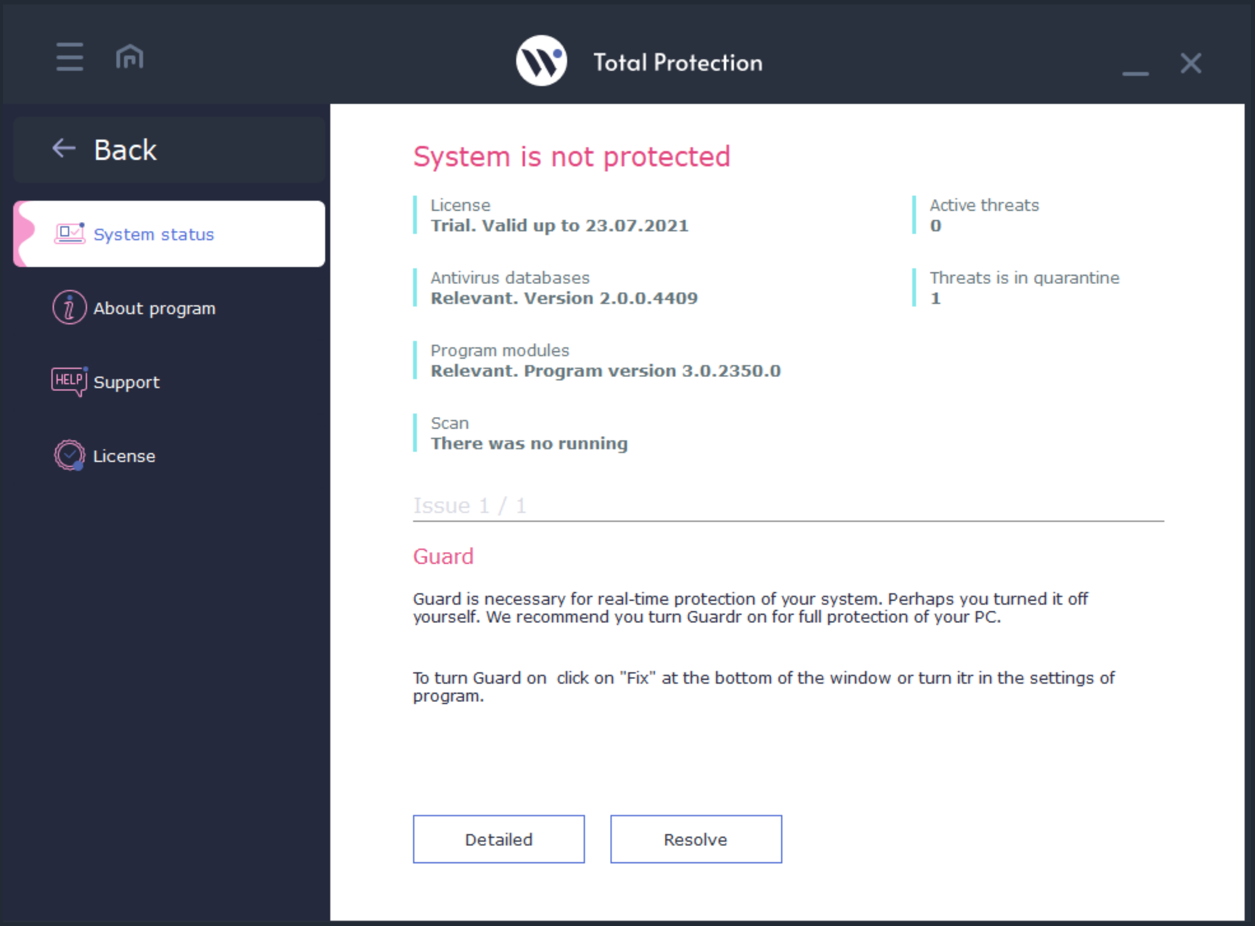
Graphical representation of the system status is presented by Waredot Total Protection **in 2 colors**.

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:



System is not protected

License
Trial. Valid up to 23.07.2021

Active threats
0

Antivirus databases
Relevant. Version 2.0.0.4409

Threats is in quarantine
1

Program modules
Relevant. Program version 3.0.2350.0

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 Guardr on for full protection of your PC.

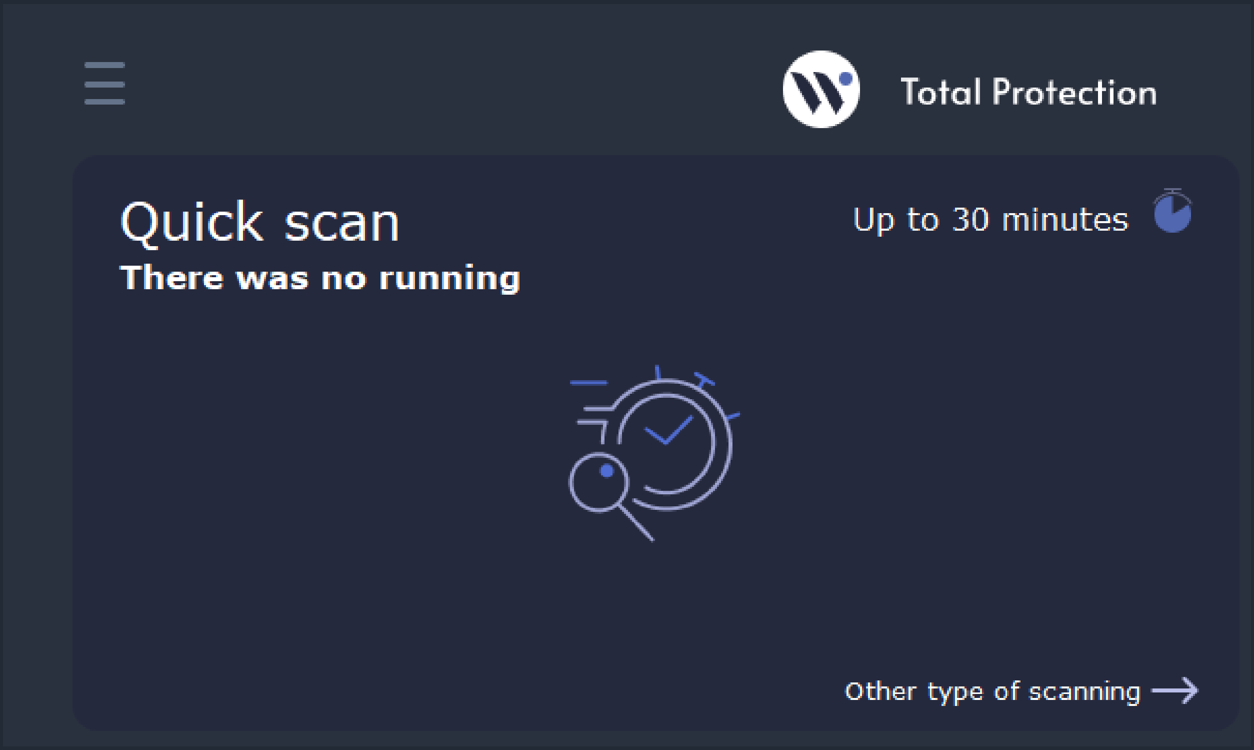
To turn Guard on click on "Fix" at the bottom of the window or turn itr in the settings of program.

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

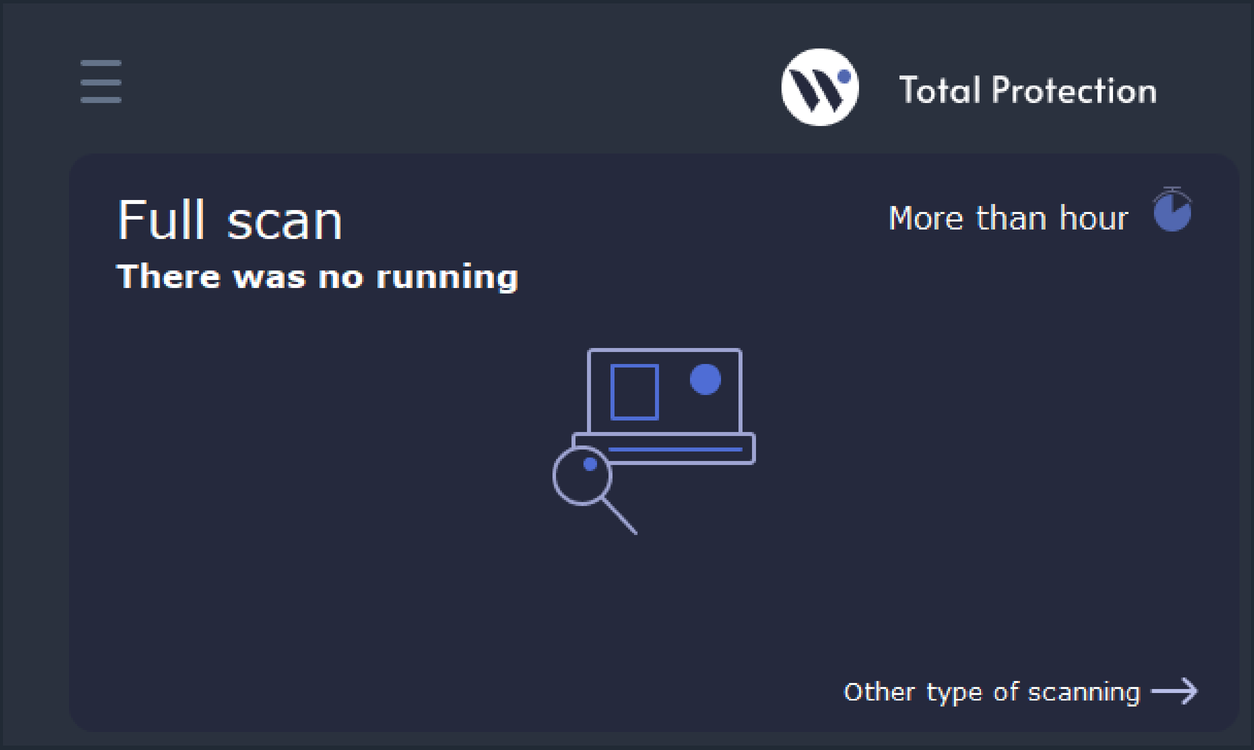
Waredot Total Protection has three scan modes which are available in the main window: **Quick**, **Full** and **Custom Scan**. Each set is provided with certain parameters of the mode. You can choose type of Scan using pointer in the right corner at the bottom of the Scan button.

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.

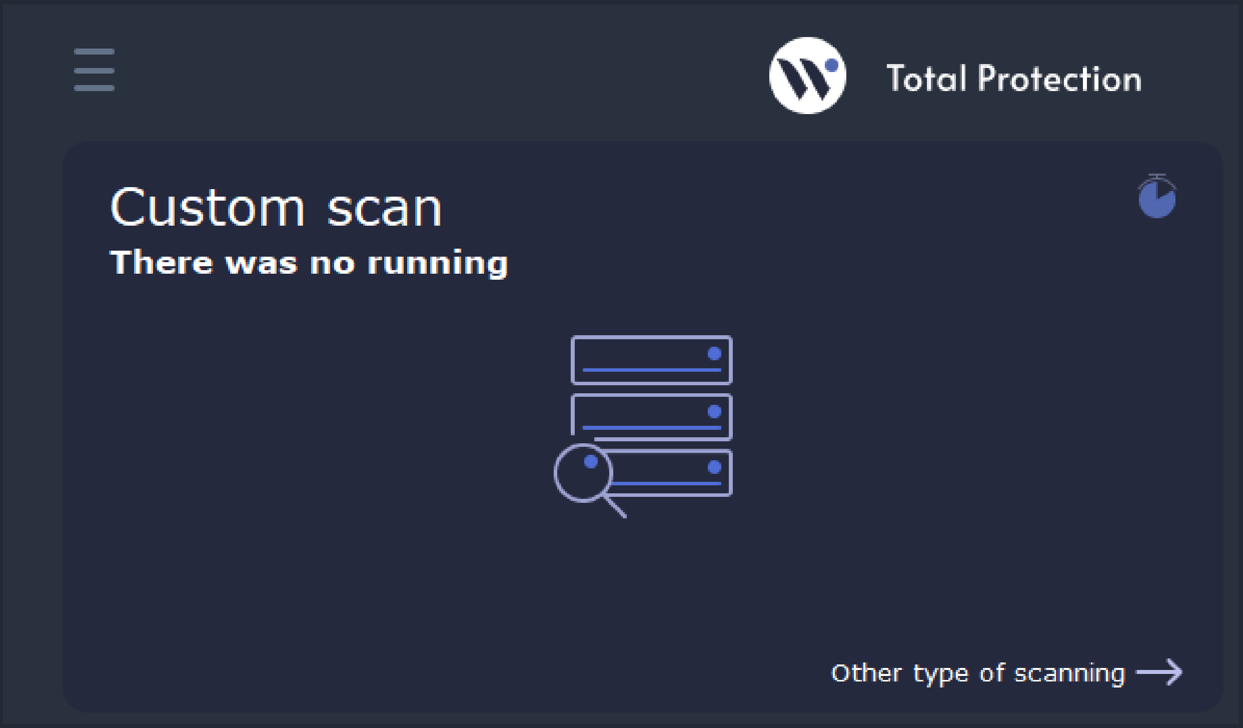


Full Scan – total system check. Thorough scanning of the system. The following items are scanned: system memory, objects that run on startup, backup storage systems, mail bases, hard and removable drives.

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.


Total Protection

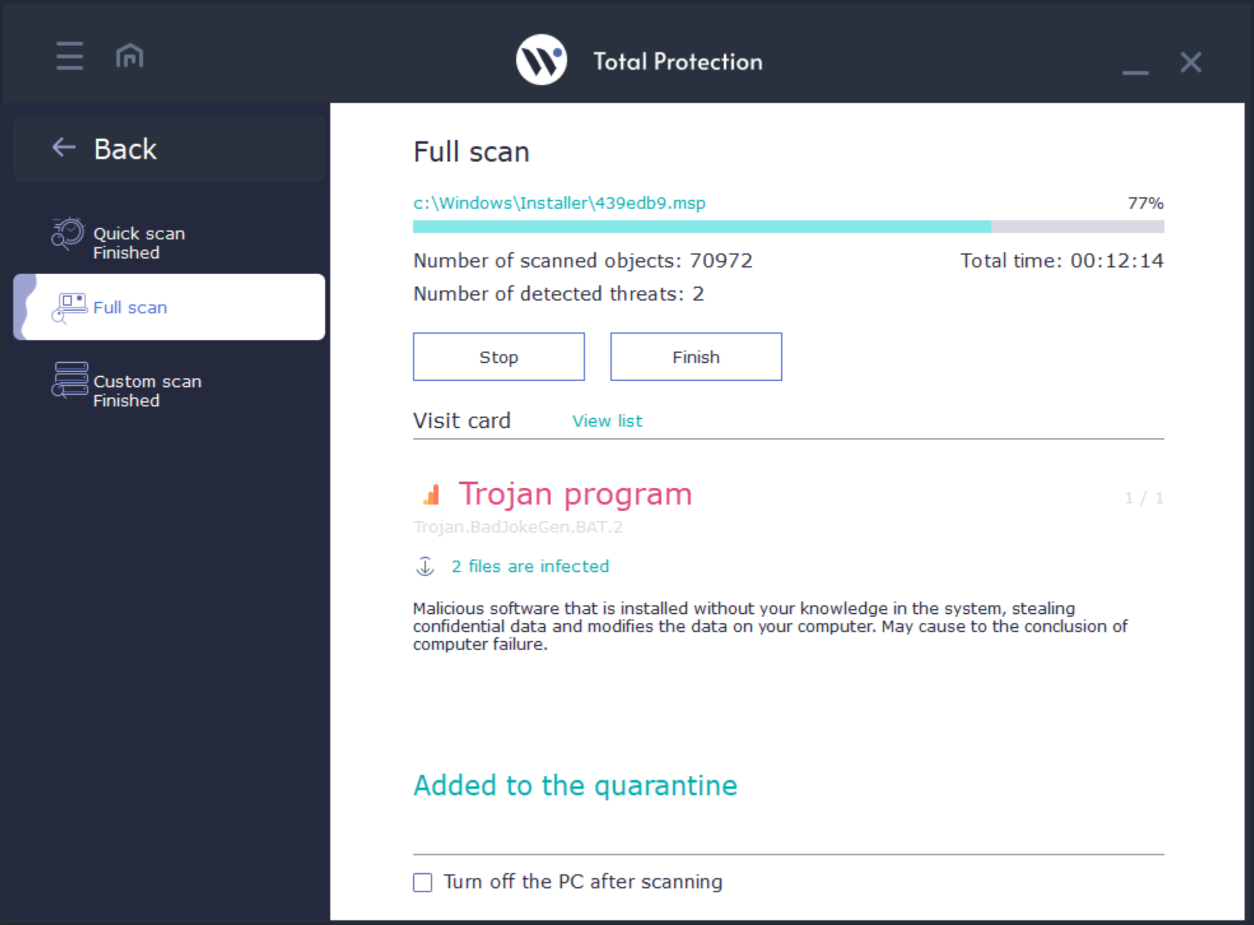
Custom scan

There was no running

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 Total Protection will apply an optimal action to neutralize infected files automatically or offer to user the action for the found threats. The behavior of Waredot Total Protection depends on the settings of antivirus which user can change.

When this process be completed, Waredot Total Protection 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.



Full scan

c:\Windows\Installer\439edb9.msp 77%

Number of scanned objects: 70972 Total time: 00:12:14

Number of detected threats: 2

Trojan program

Trojan.BadJokeGen.BAT.2

2 files are infected

Malicious software that is installed without your knowledge in the system, stealing confidential data and modifies the data on your computer. May cause to the conclusion of computer failure.

Added to the quarantine

□ Turn off the PC after scanning

There are **three levels** of danger of threats in Waredot Total Protection:

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.

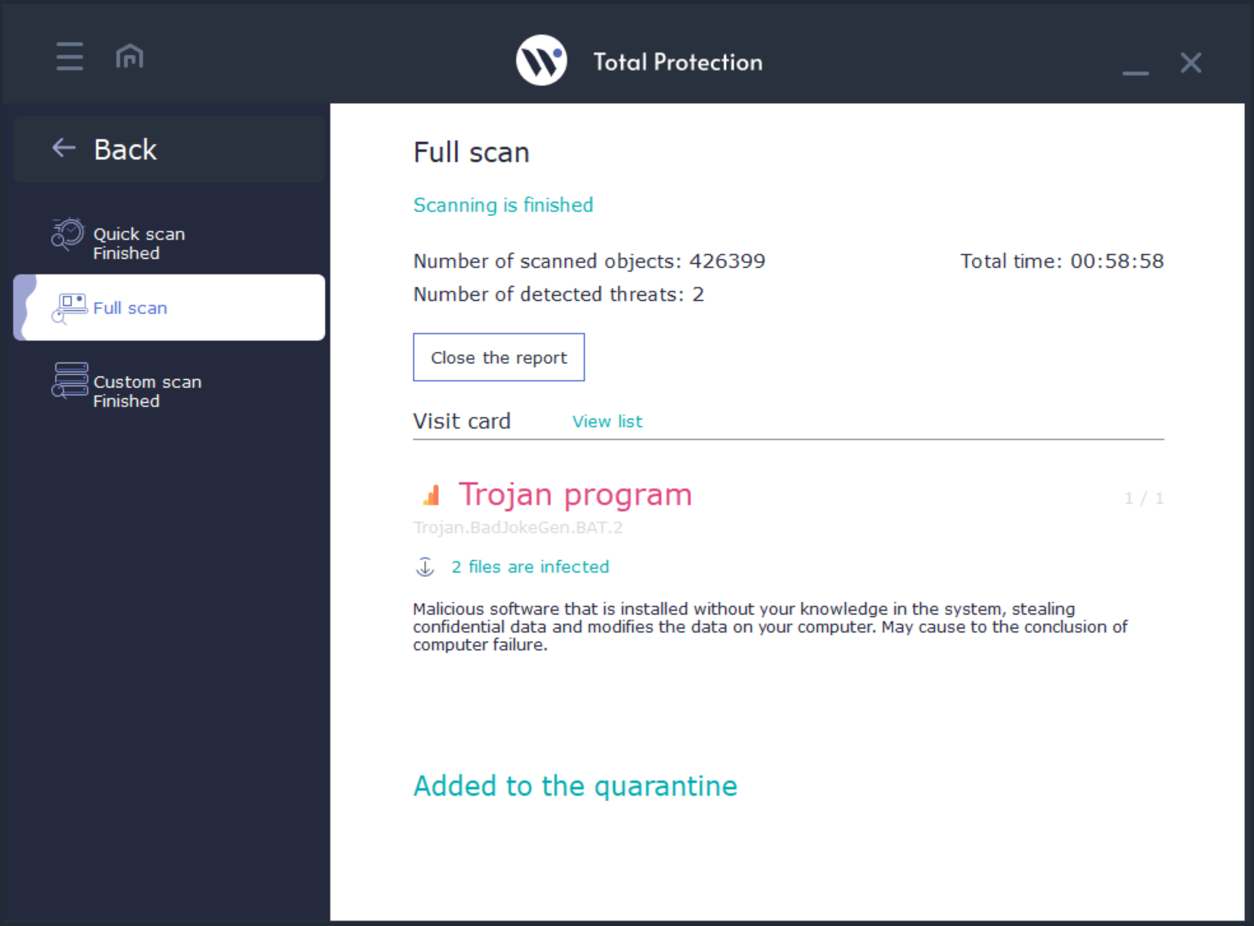
THIRD LEVEL – infected files, which were found on the computer. These are the most dangerous files, they can lead to infection of the Operating System and to lowering of its performance. These viruses may be dangerous for users' data too. We recommend users to apply one of the long-term actions for neutralizing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

Waredot Total Protection 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.



Full scan

Scanning is finished

Number of scanned objects: 426399 Total time: 00:58:58

Number of detected threats: 2

Trojan program

Trojan.BadJokeGen.BAT.2

2 files are infected

Malicious software that is installed without your knowledge in the system, stealing confidential data and modifies the data on your computer. May cause to the conclusion of computer failure.

Added to the quarantine

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 Total Protection 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 Total Protection 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.

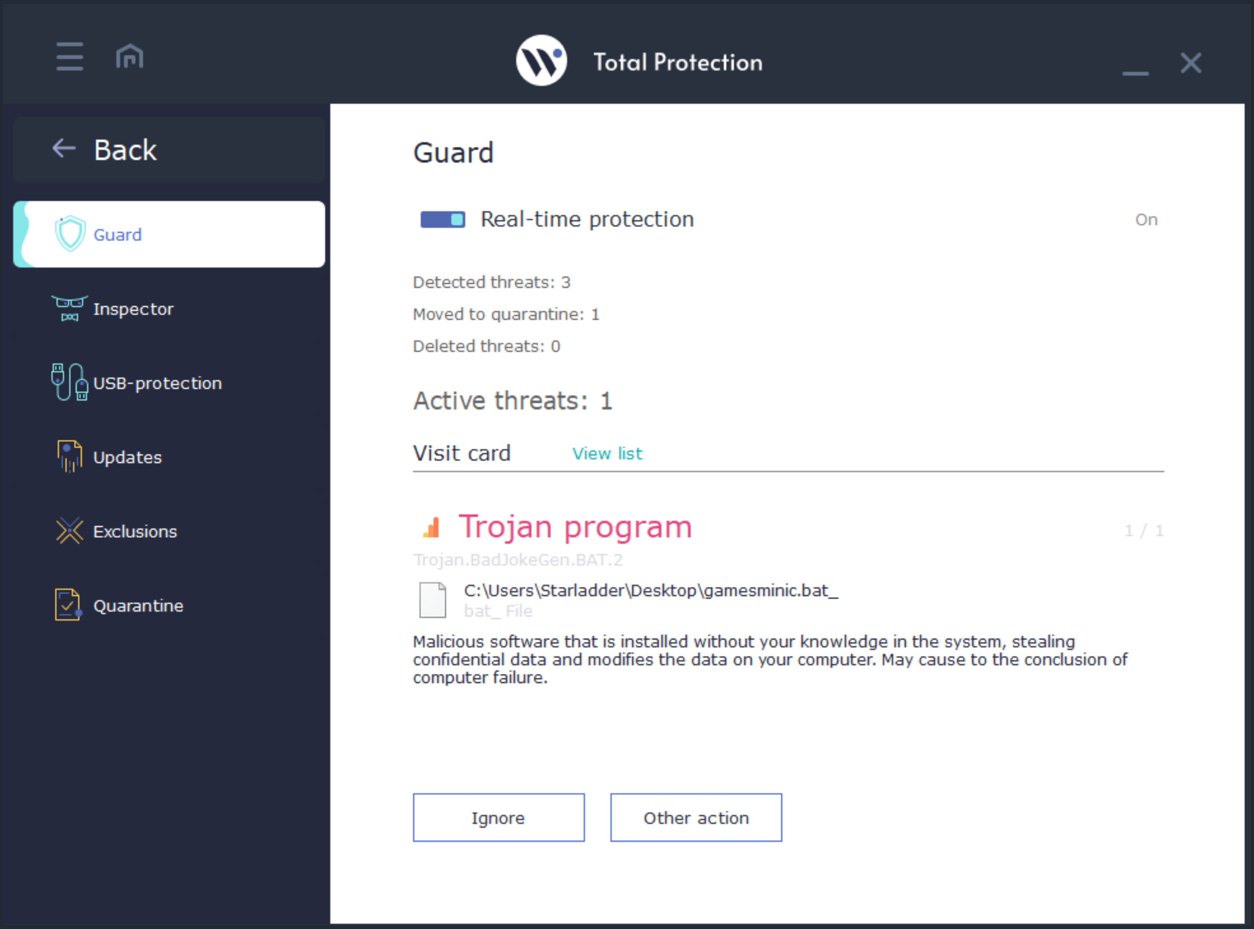
Block – via applying of this action user block the threats. After applying of the action "Block" the file is blocked by Waredot Total Protection and stays in Active threats until user will choose and apply the other action for this threat. If Waredot Total Protection blocks the virus or infected file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

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.



Guard

Real-time protection On

Detected threats: 3

Moved to quarantine: 1

Deleted threats: 0

Active threats: 1

Visit card View list

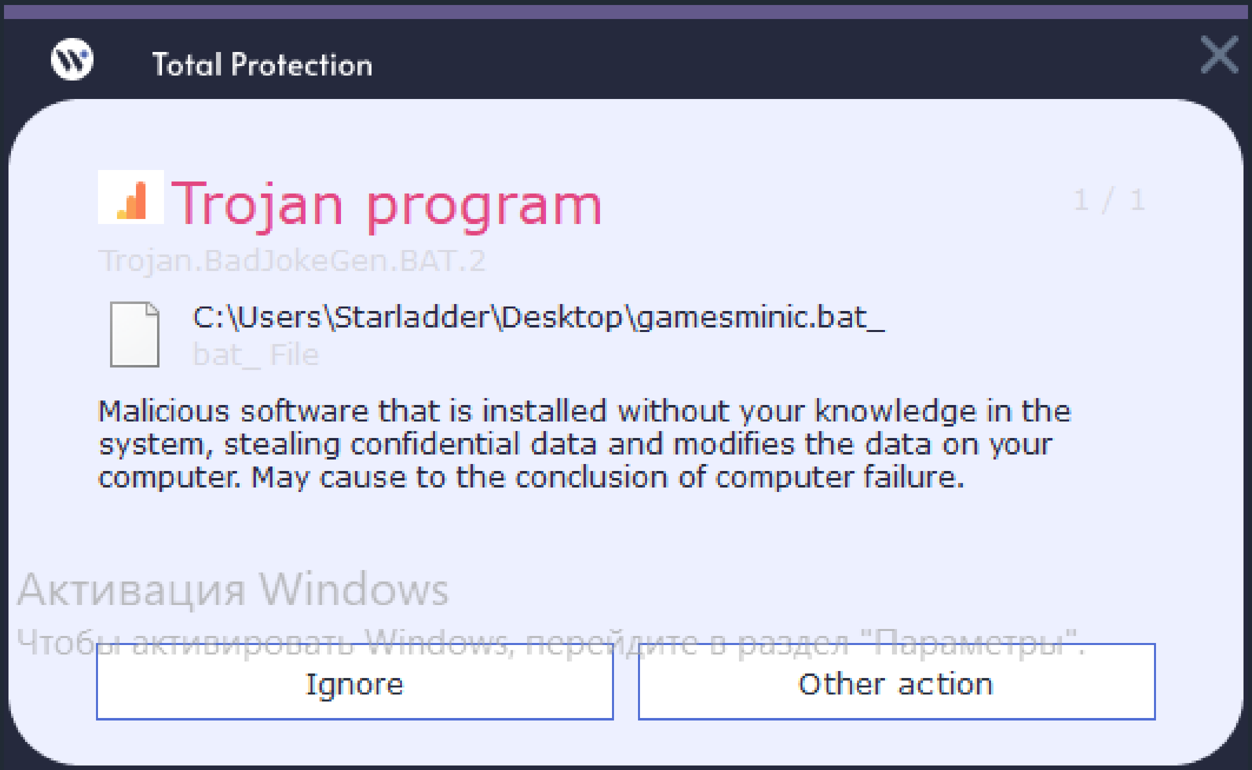
Trojan program 1 / 1

Trojan.BadJokeGen.BAT.2

C:\Users\Starladder\Desktop\gamesminic.bat_

bat_ File

Malicious software that is installed without your knowledge in the system, stealing confidential data and modifies the data on your computer. May cause to the conclusion of computer failure.



Trojan program

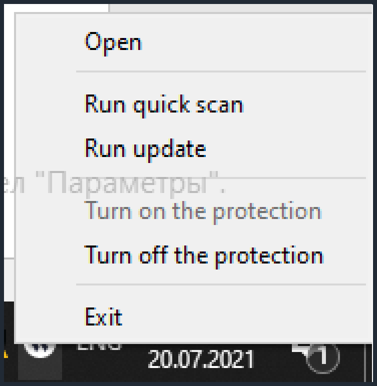
Trojan.BadJokeGen.BAT.2

C:\Users\Starladder\Desktop\gamesminic.bat_

bat_ File

Malicious software that is installed without your knowledge in the system, stealing confidential data and modifies the data on your computer. May cause to the conclusion of computer failure.

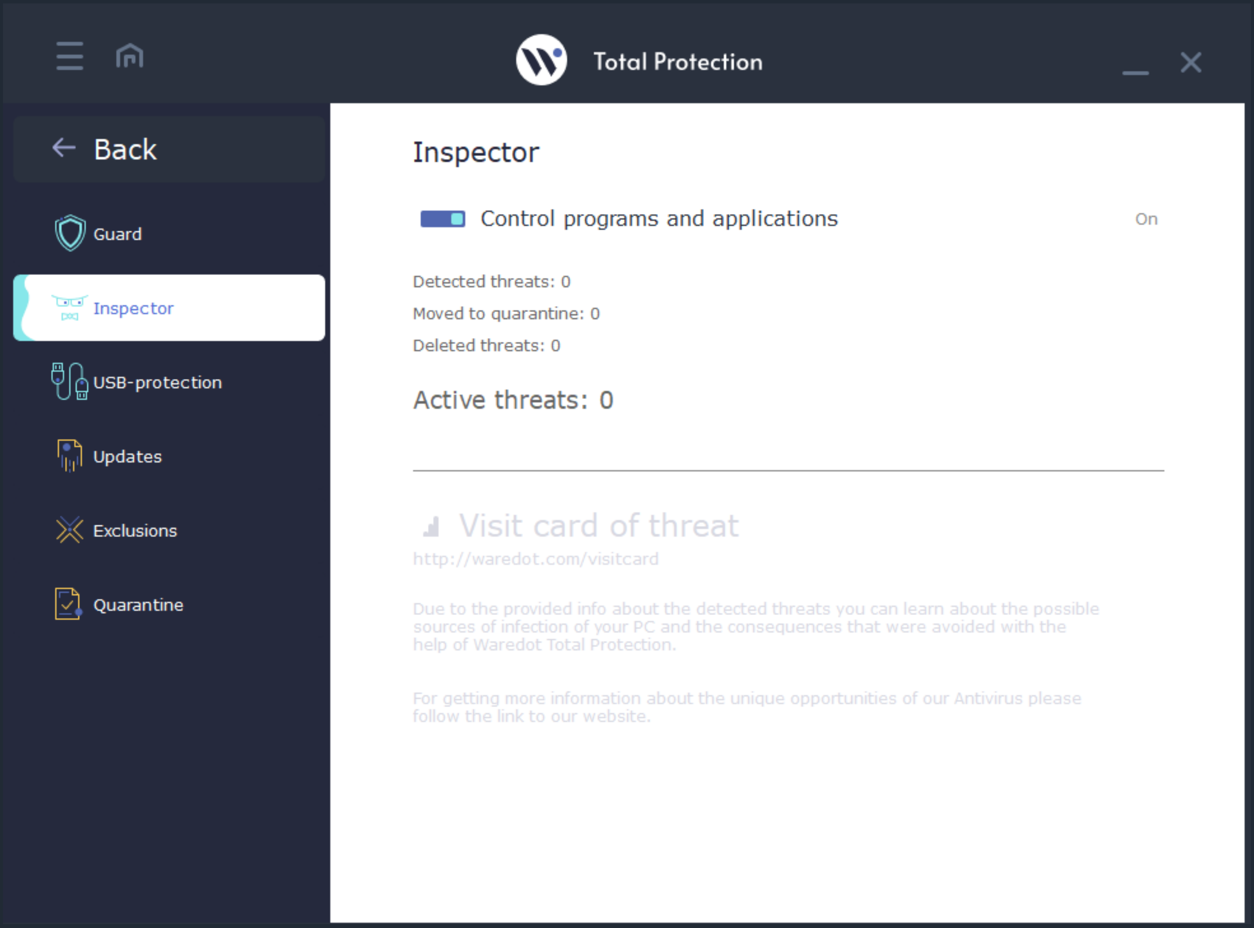
By default, the Guard is automatically activated every time you start the program. This is a very important component of protection. We do not recommend you disable this feature. To check whether the Guard is turned on, click the right mouse button on Waredot Total Protection icon in the taskbar notification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

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.



Inspector

Control programs and applications On

Detected threats: 0
Moved to quarantine: 0
Deleted threats: 0

Active threats: 0

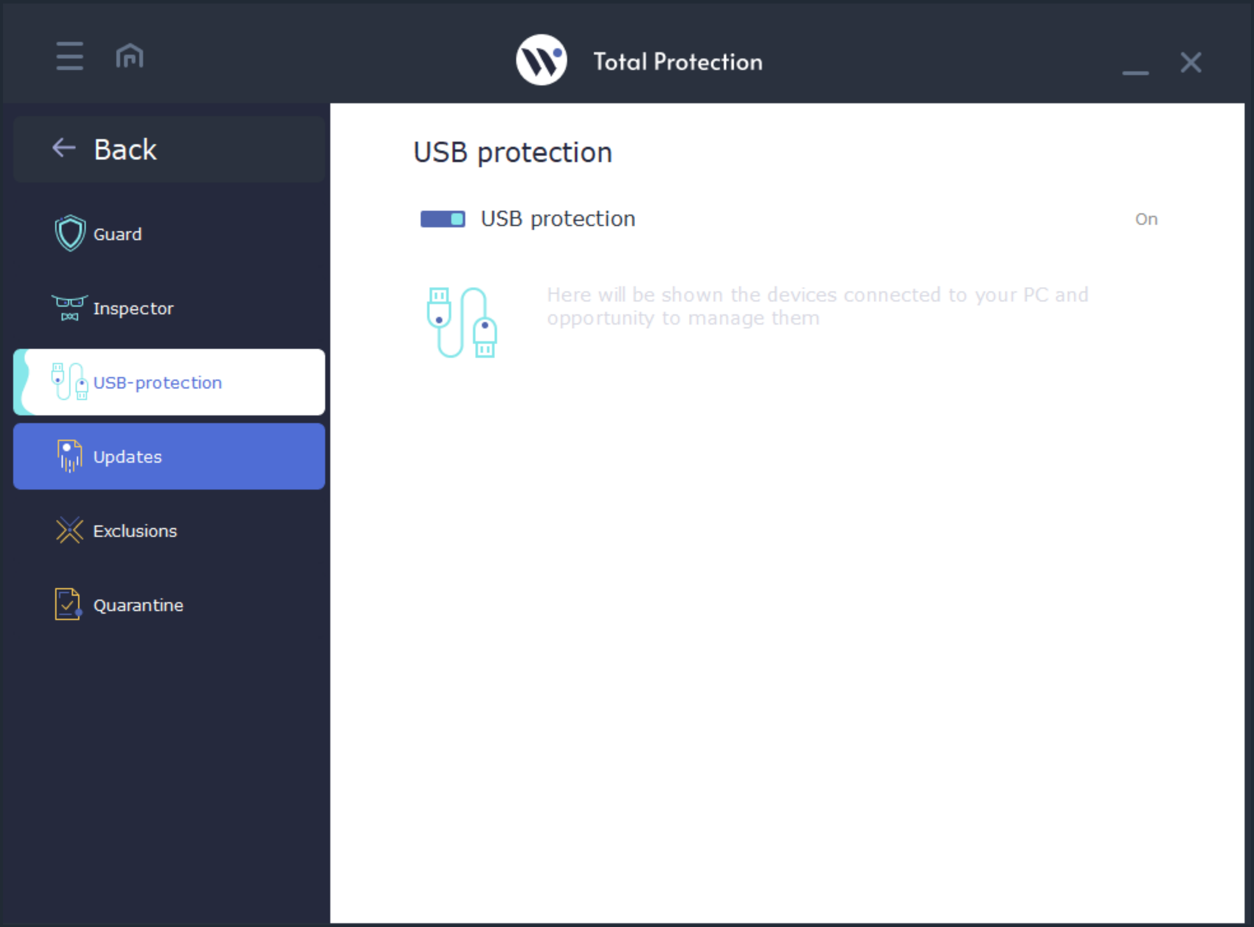
Visit card of threat
http://waredot.com/visitcard

Due to the provided info about the detected threats you can learn about the possible sources of infection of your PC and the consequences that were avoided with the help of Waredot Total Protection.

For getting more information about the unique opportunities of our Antivirus please follow the link to our website.

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.

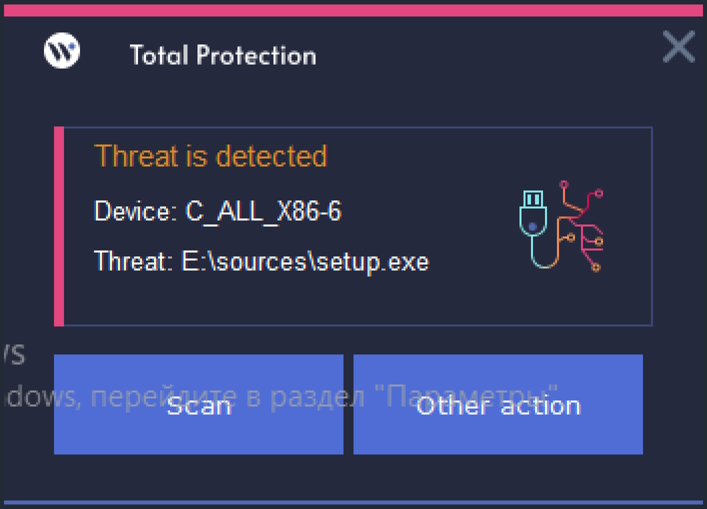
When a new USB-drive is connected, Waredot! detects it, performs a brief analysis and informs the user about the evaluated level of security of the disc. In the case of detection of the viruses or any suspicious objects on the flash drive, antivirus immediately prompts the user to remove them.



USB protection

USB protection On

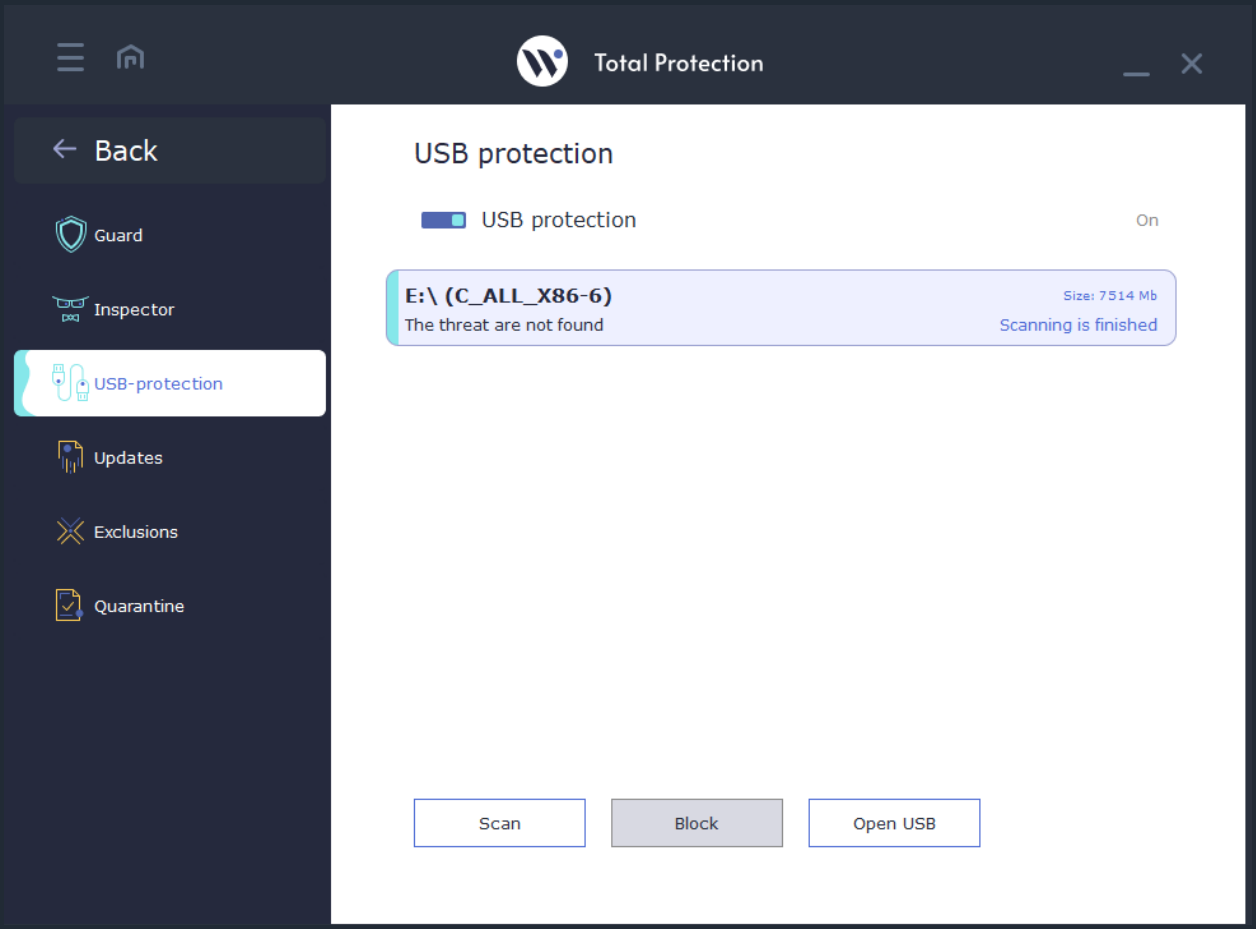
Here will be shown the devices connected to your PC and opportunity to manage them



Threat is detected

Device: C_ALL_X86-6

Threat: E:\sources\setup.exe



USB protection

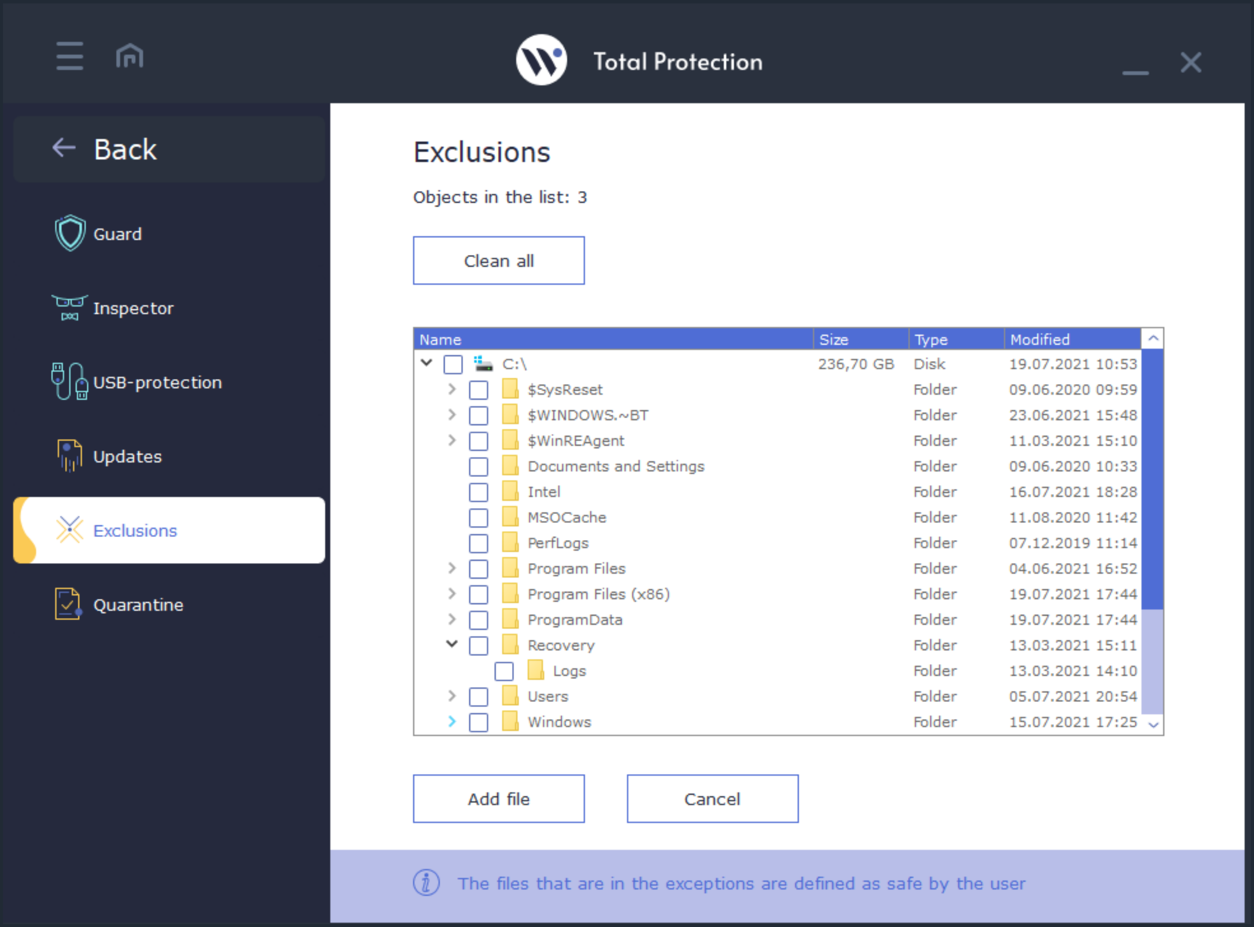
USB protection On

E:\ (C_ALL_X86-6) Size: 7514 Mb

The threat are not found Scanning is finished

Exclusions tab contains files which were marked as exclusions by Waredot Total Protection. It means that Waredot Total Protection 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 Total Protection, click the "burger" button in the left upper side of the window and go to "Antivirus protection" section, press the item Exclusions.



Exclusions

Objects in the list: 3

Name	Size	Type	Modified
C:\	236,70 GB	Disk	19.07.2021 10:53
$SysReset		Folder	09.06.2020 09:59
$WINDOWS.~BT		Folder	23.06.2021 15:48
$WinREAgent		Folder	11.03.2021 15:10
Documents and Settings		Folder	09.06.2020 10:33
Intel		Folder	16.07.2021 18:28
MSOCache		Folder	11.08.2020 11:42
PerfLogs		Folder	07.12.2019 11:14
Program Files		Folder	04.06.2021 16:52
Program Files (x86)		Folder	19.07.2021 17:44
ProgramData		Folder	19.07.2021 17:44
Recovery		Folder	13.03.2021 15:11
Logs		Folder	13.03.2021 14:10
Users		Folder	05.07.2021 20:54
Windows		Folder	15.07.2021 17:25

The files that are in the exceptions are defined as safe by the user

Button "Add file" - you can use it for adding files, folders and drives to Exclusions of Waredot Total Protection. 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 Total Protection because all files in Exclusions are not scanned by Waredot Total Protection till they stay in Exclusions.

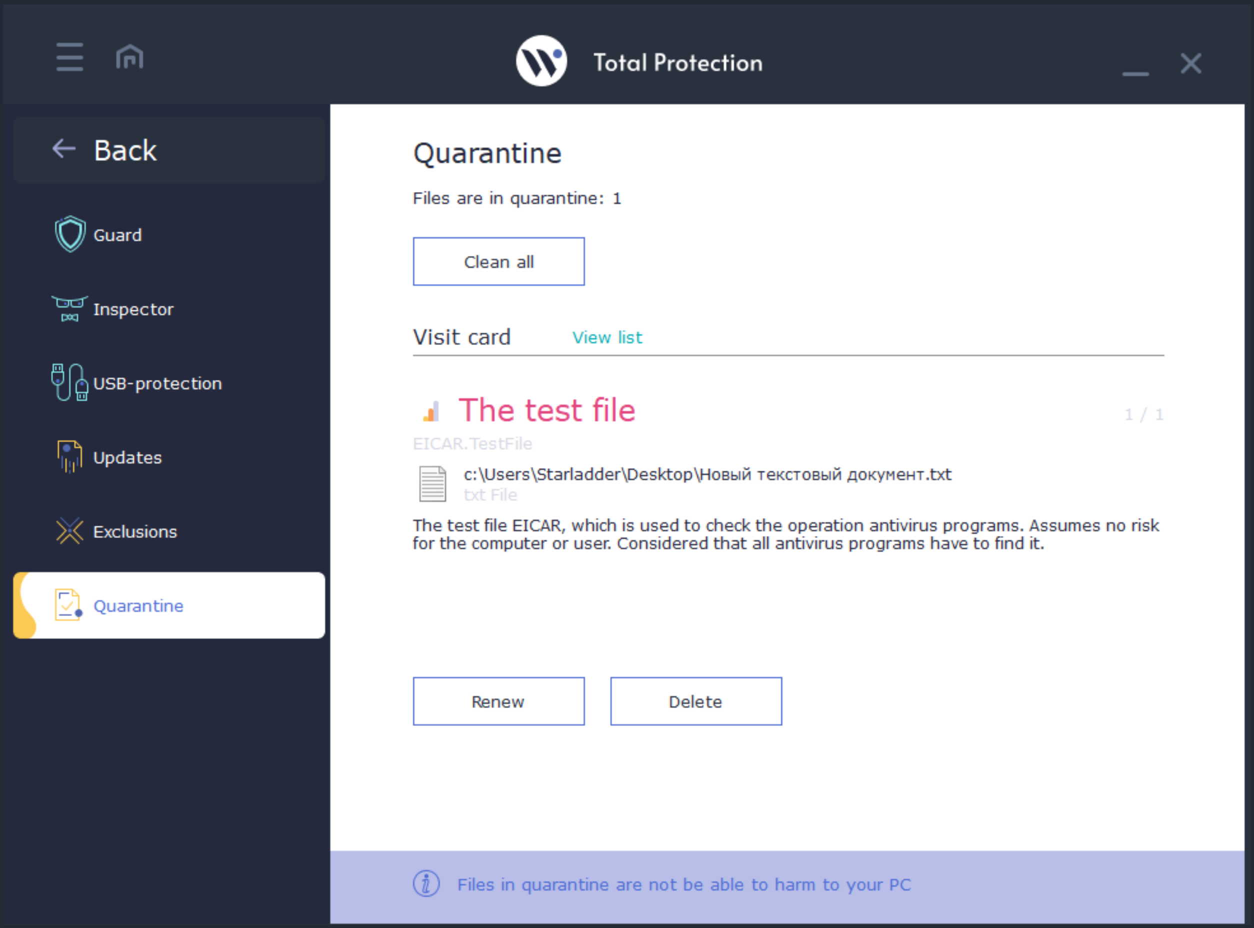
Button "Delete" - you can use it for deleting files, folders and drives from the Exclusions of Waredot Total Protection. For deleting the item from the Exclusions we recommend you to choose the object (the file, folder or drive) and click the button "Delete".

Button "Clear all" – allows user to clear whole list of the Exclusions of Waredot Total Protection with a single click of this button.

Quarantine tab contains the files which were marked by **Waredot Total Protection 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 Total Protection do not threaten for the data or software on the user's PC.**



Quarantine

Files are in quarantine: 1

The test file 1 / 1

EICAR.TestFile

c:\Users\Starladder\Desktop\Новый текстовый документ.txt

txt File

The test file EICAR, which is used to check the operation antivirus programs. Assumes no risk for the computer or user. Considered that all antivirus programs have to find it.

Files in quarantine are not be able to harm to your PC

ware.

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

- 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 Total Protection.

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

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

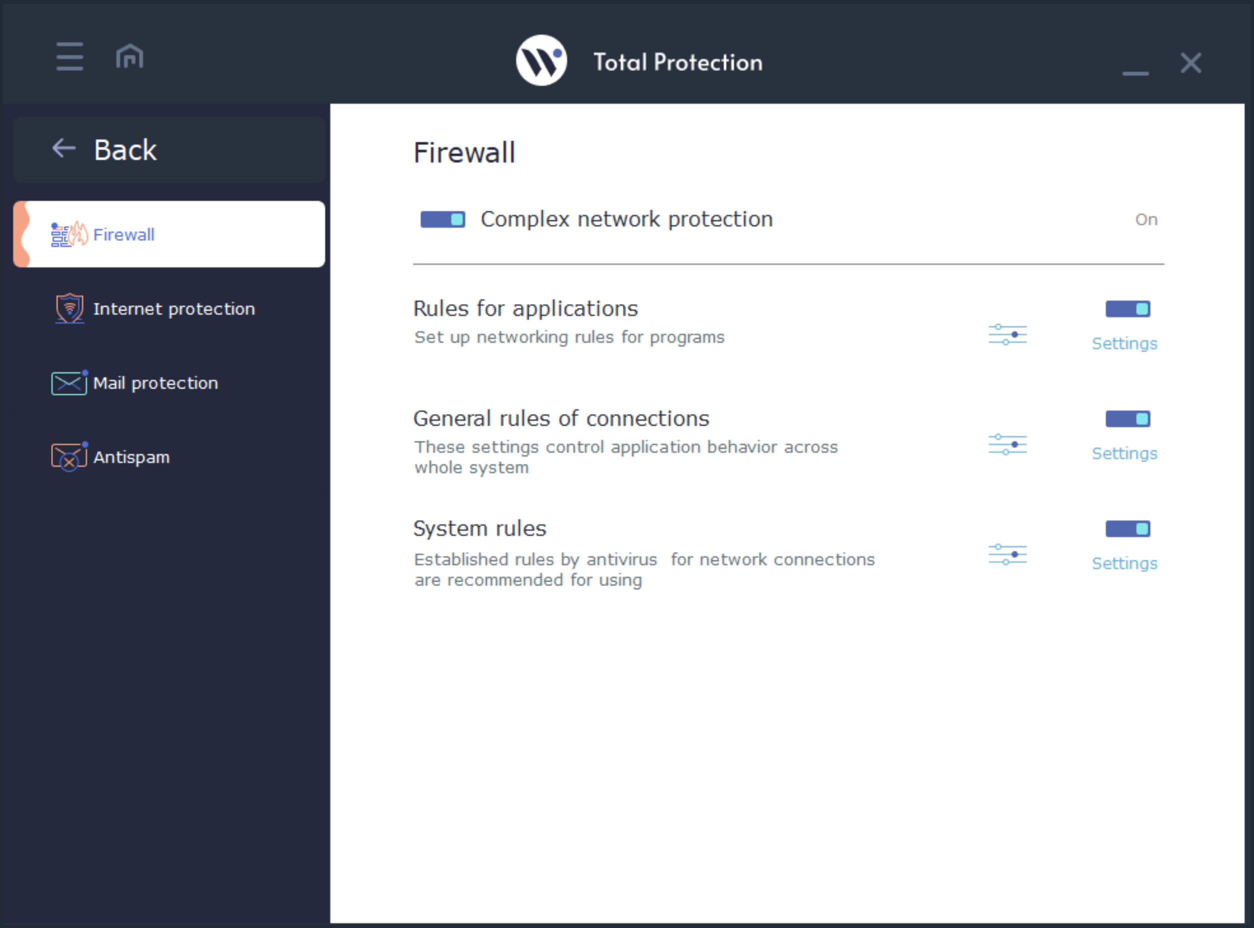
Button “**Delete**” – user can use it for deleting the files from the Quarantine of Waredot Total Protection. For deleting the item from the Quarantine we recommend you to select the file and click the button “Delete”. After deleting the file it could not be restored.

Button “**Clear all**” – allows user to clear whole list of the Quarantine of Waredot Total Protection 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.



Firewall

Complex network protection On

Rules for applications
Set up networking rules for programs
Settings

General rules of connections
These settings control application behavior across whole system
Settings

System rules
Established rules by antivirus for network connections are recommended for using
Settings

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.

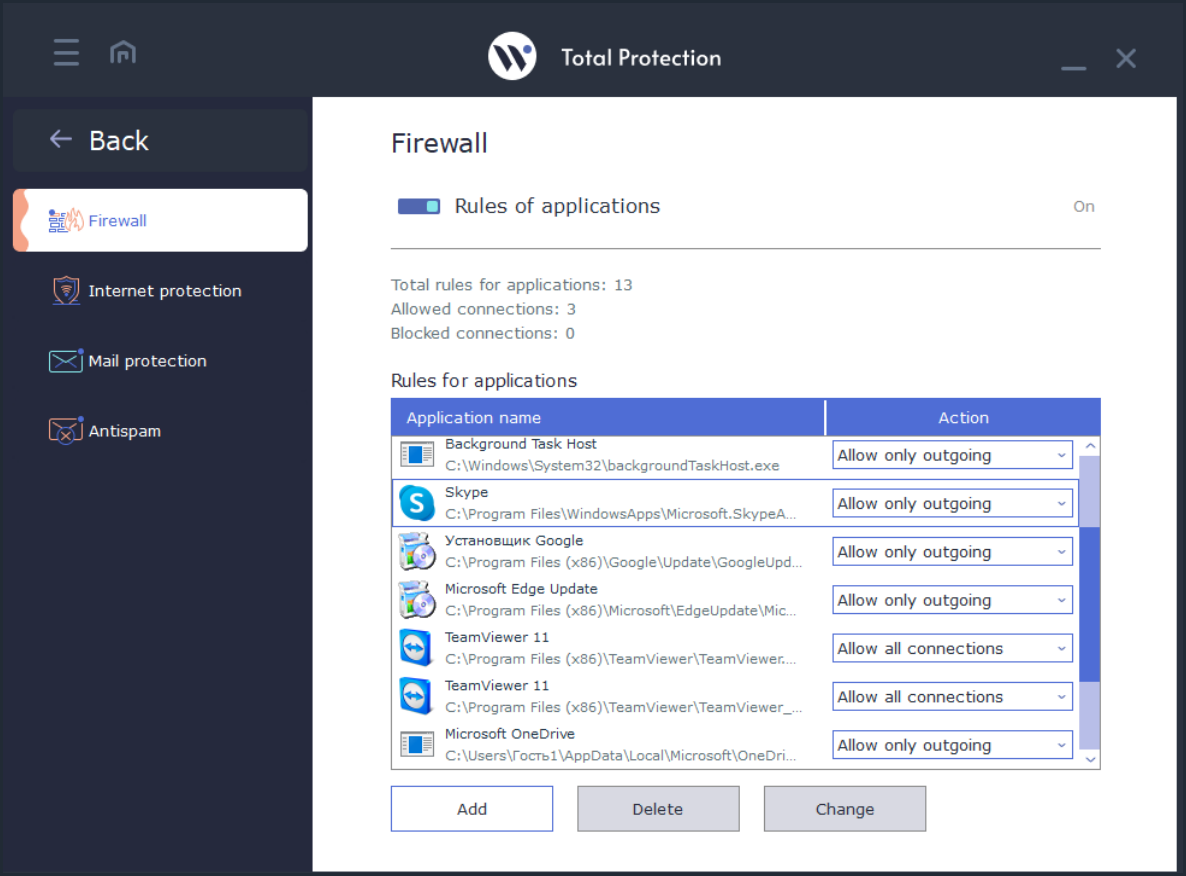
Interactive mode is for experienced users.

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).



Firewall

Rules of applications On

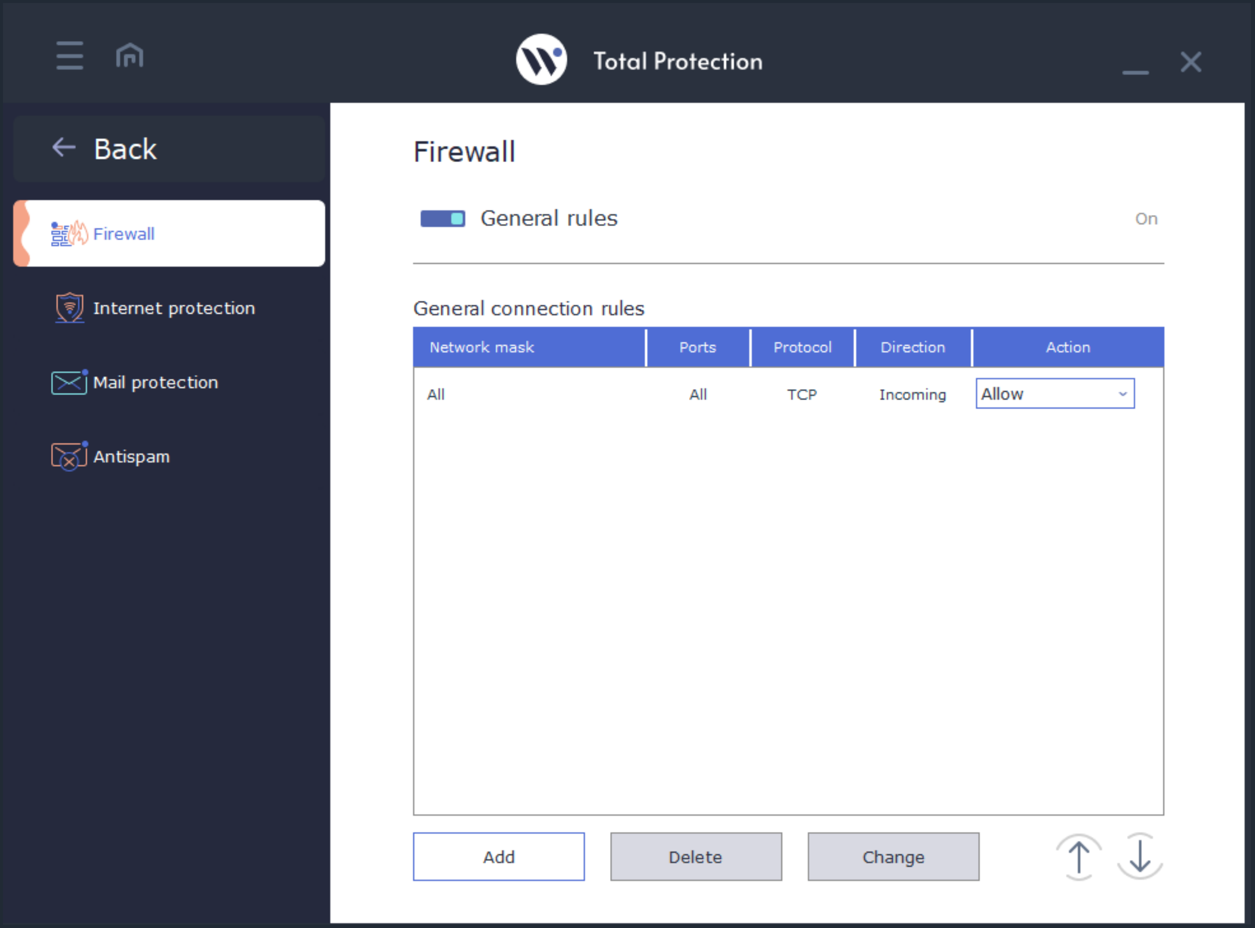
Total rules for applications: 13
Allowed connections: 3
Blocked connections: 0

Rules for applications

Application name	Action
Background Task Host C:\Windows\System32\backgroundTaskHost.exe	Allow only outgoing
Skype C:\Program Files\WindowsApps\Microsoft.SkypeA...	Allow only outgoing
Установщик Google C:\Program Files (x86)\Google\Update\GoogleUpd...	Allow only outgoing
Microsoft Edge Update C:\Program Files (x86)\Microsoft\EdgeUpdate\Mic...	Allow only outgoing
TeamViewer 11 C:\Program Files (x86)\TeamViewer\TeamViewer....	Allow all connections
TeamViewer 11 C:\Program Files (x86)\TeamViewer\TeamViewer_...	Allow all connections
Microsoft OneDrive C:\Users\Гость1\AppData\Local\Microsoft\OneDri...	Allow only outgoing

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

Waredot Total Protection 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.*



Firewall

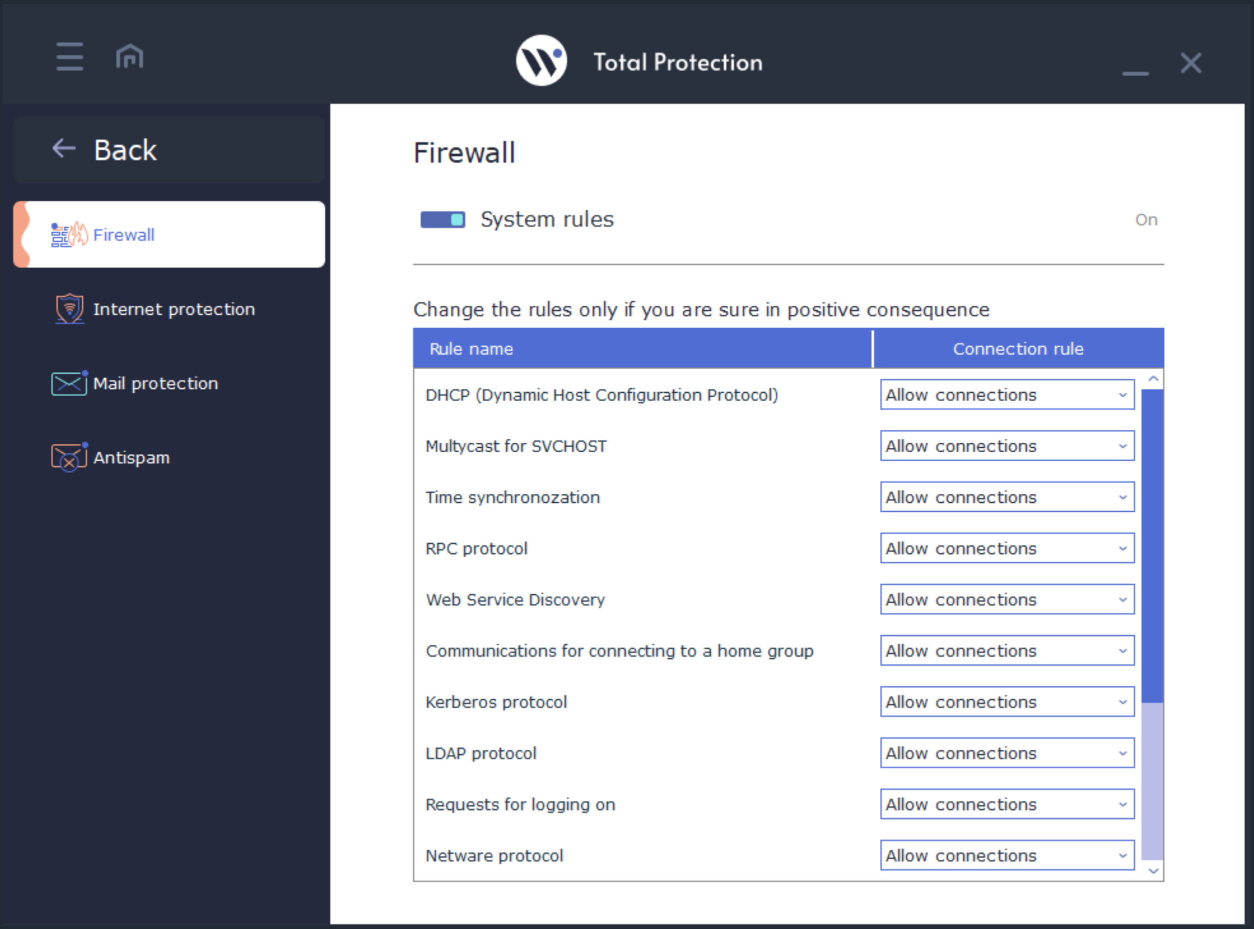
General rules On

General connection rules

Network mask	Ports	Protocol	Direction	Action
All	All	TCP	Incoming	Allow

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.



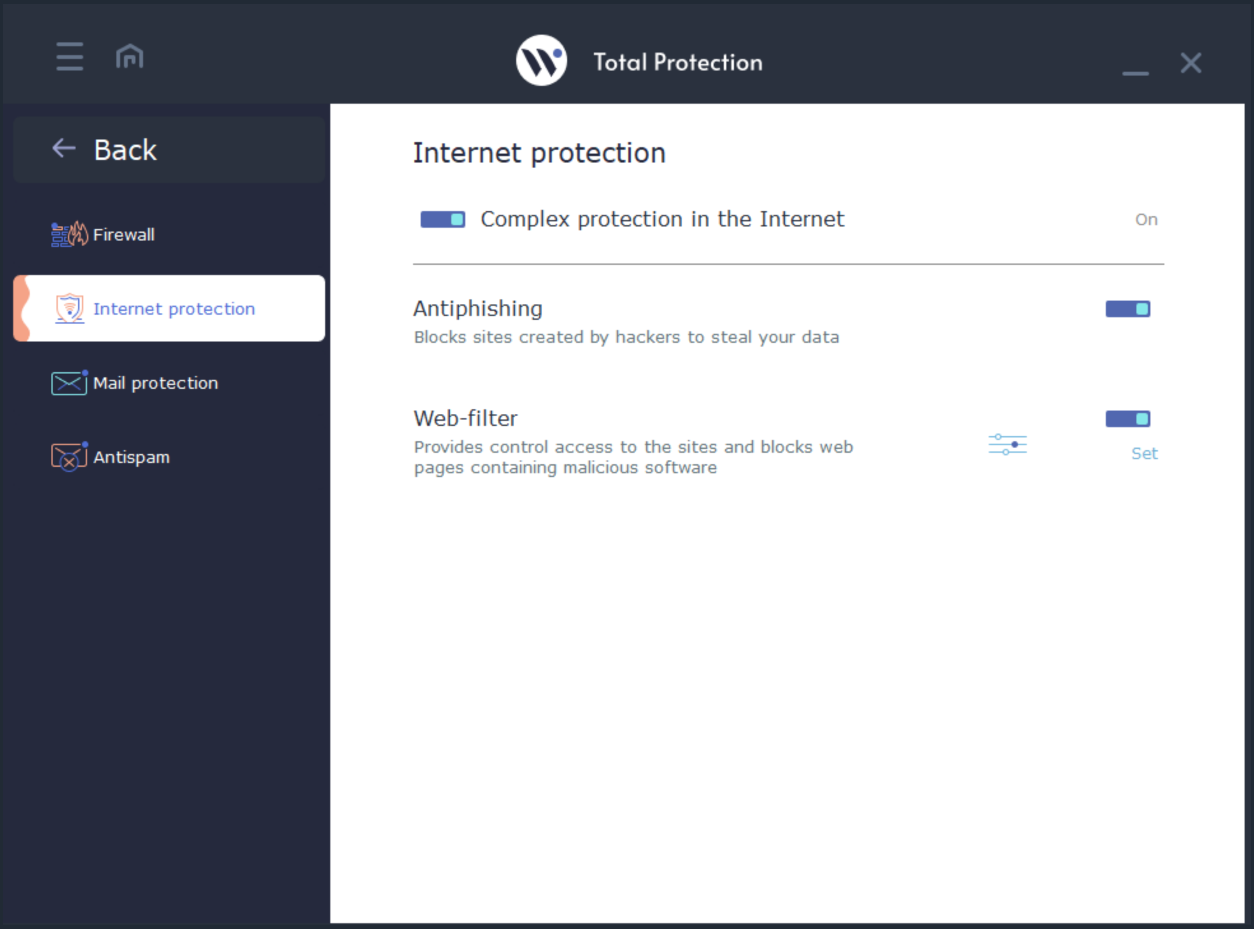
Firewall

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
Multycast 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.



Internet protection

Complex protection in the Internet On

Antiphishing

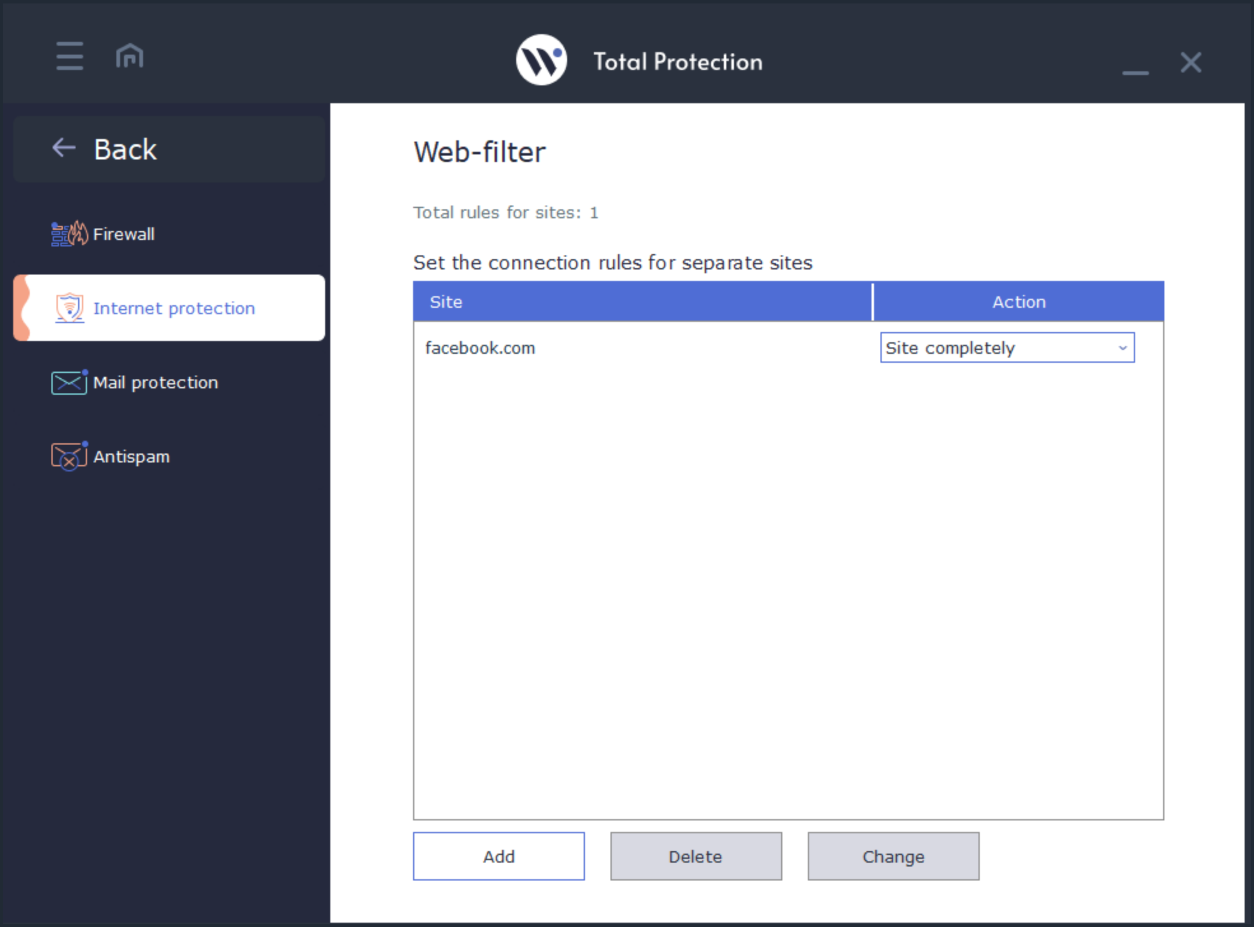
Blocks sites created by hackers to steal your data

Web-filter

Provides control access to the sites and blocks web pages containing malicious software

WEB-filter can block dangerous sites and potentially dangerous content from suspicious sites. Waredot Total Protection 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 Total Protection 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.



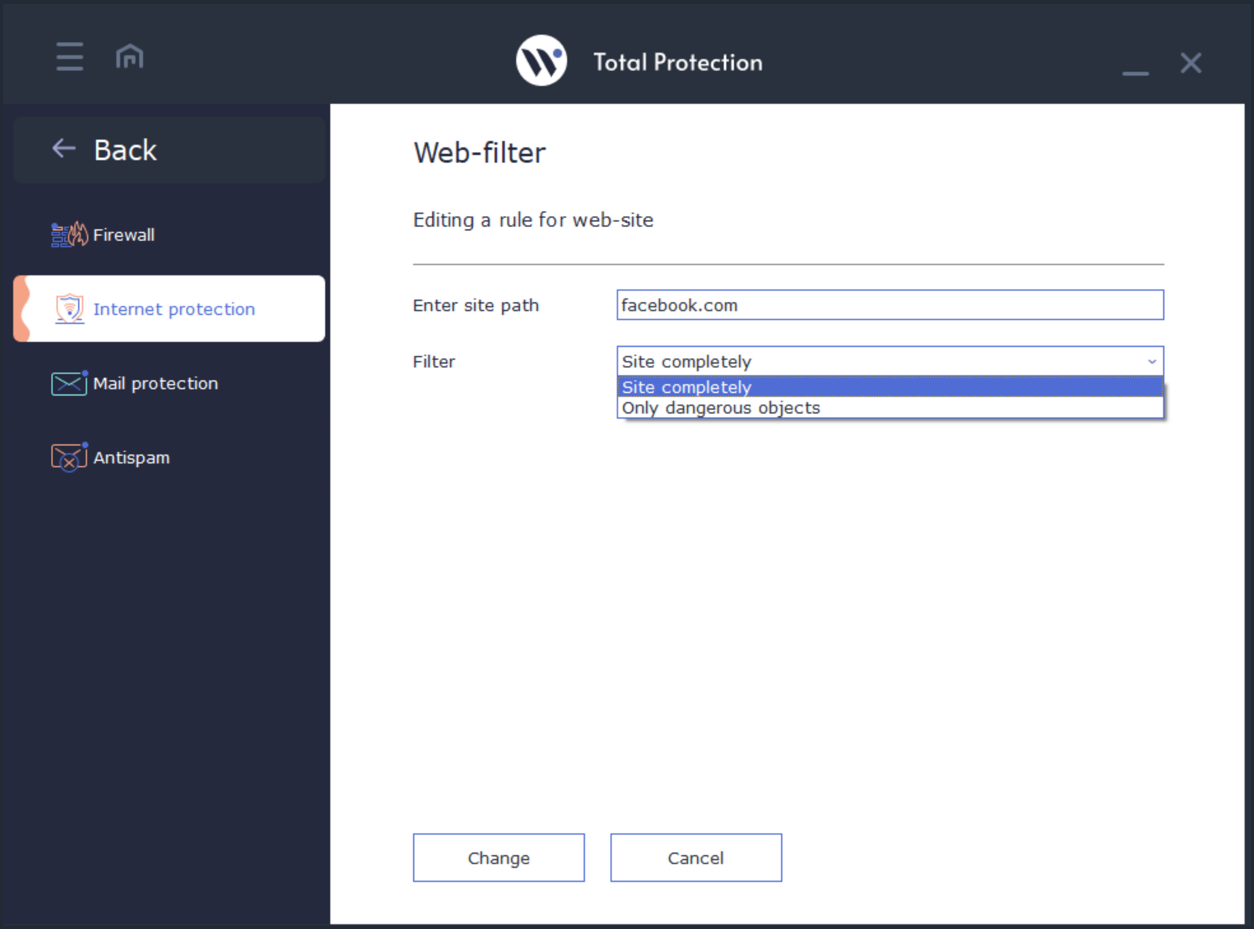
Web-filter

Total rules for sites: 1

Set the connection rules for separate sites

Site	Action
facebook.com	Site completely

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”.



Web-filter

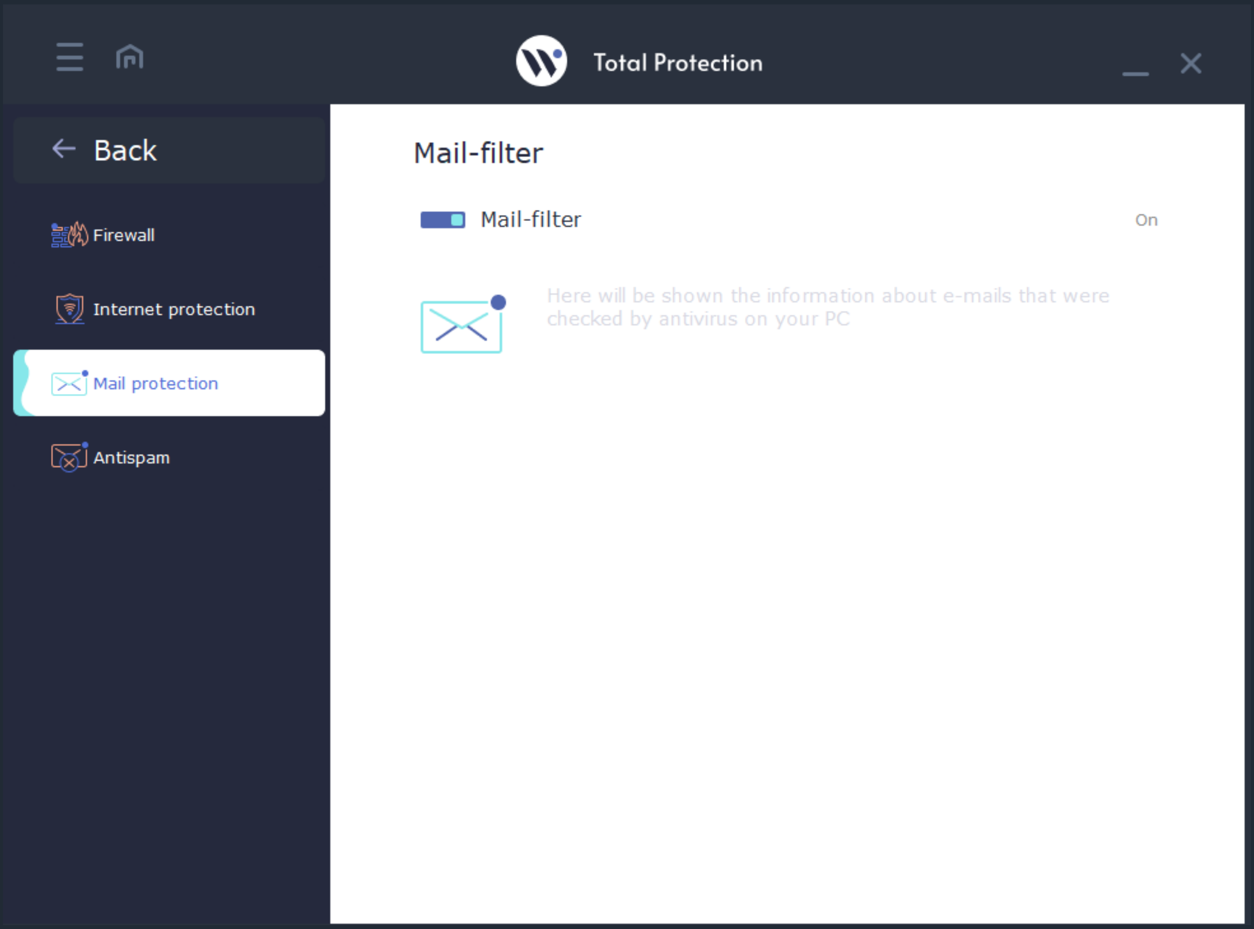
Editing a rule for web-site

Enter site path: facebook.com

Filter: Site completely

Site completely
Only dangerous objects

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.

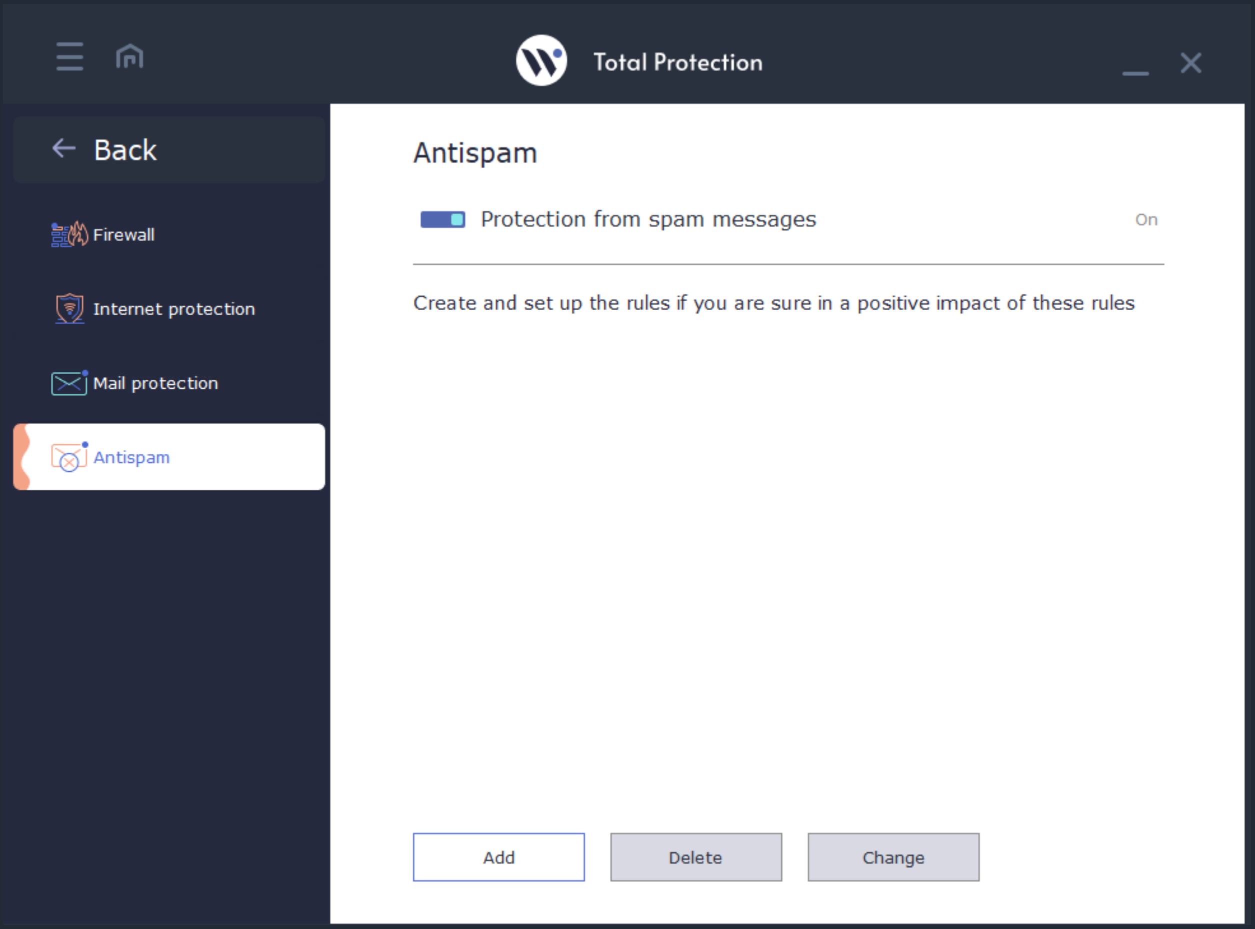


Mail-filter

Mail-filter On

Here will be shown the information about e-mails that were checked by antivirus on your PC

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.

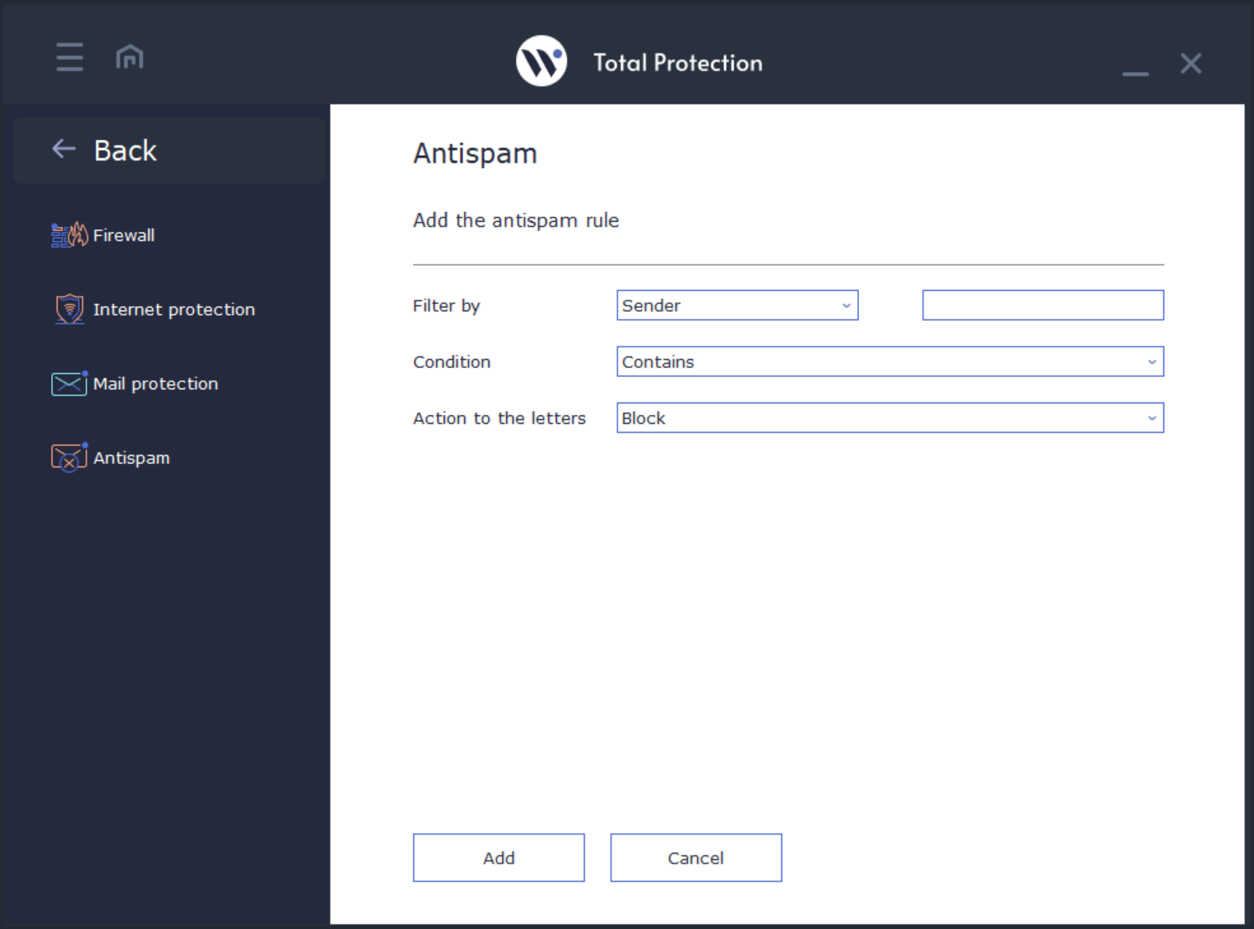


Antispam

Protection from spam messages On

Create and set up the rules if you are sure in a positive impact of these rules

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.



Antispam

Add the antispam rule

Filter by: Sender

Condition: Contains

Action to the letters: Block

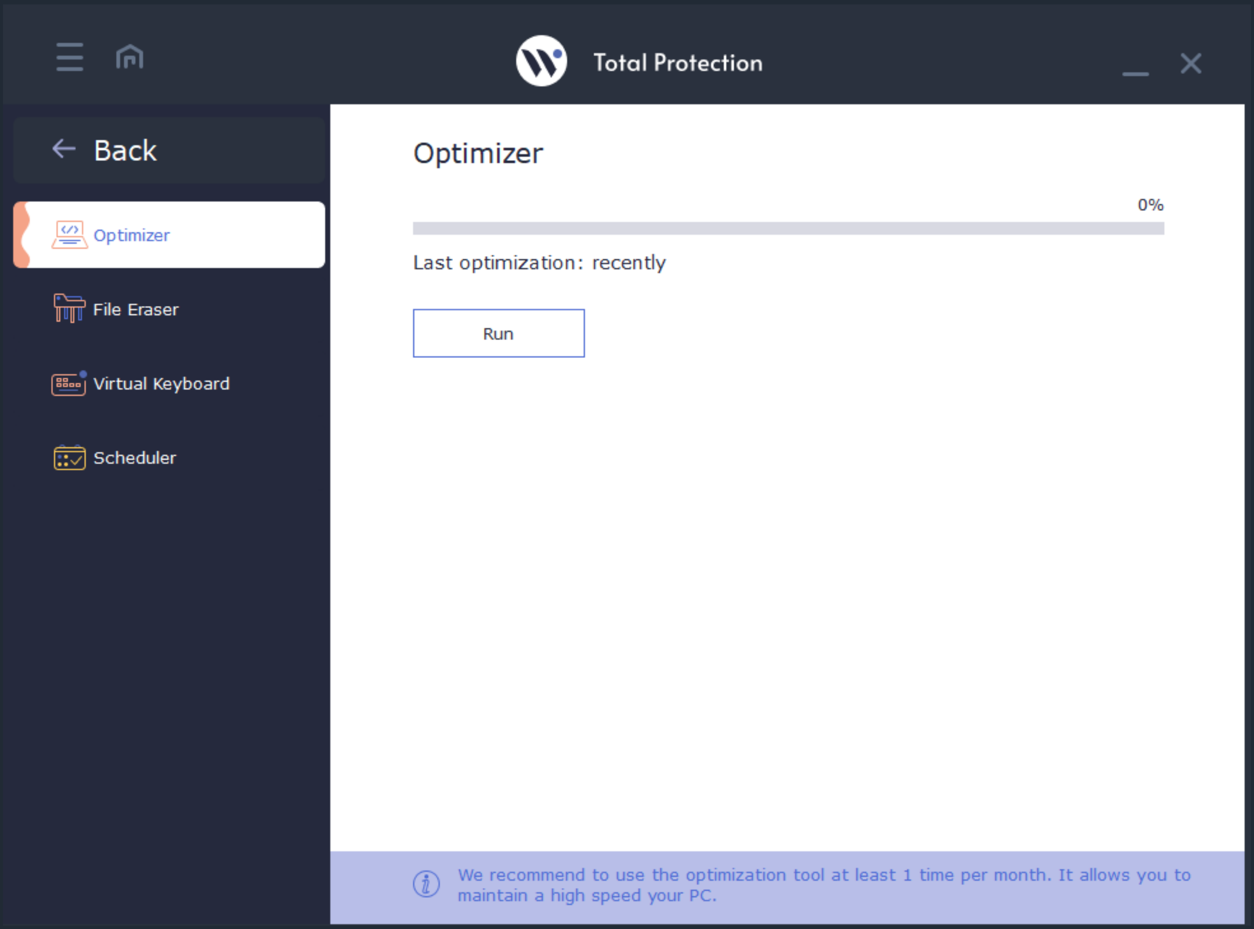
Tools

Waredot Total Protection 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.



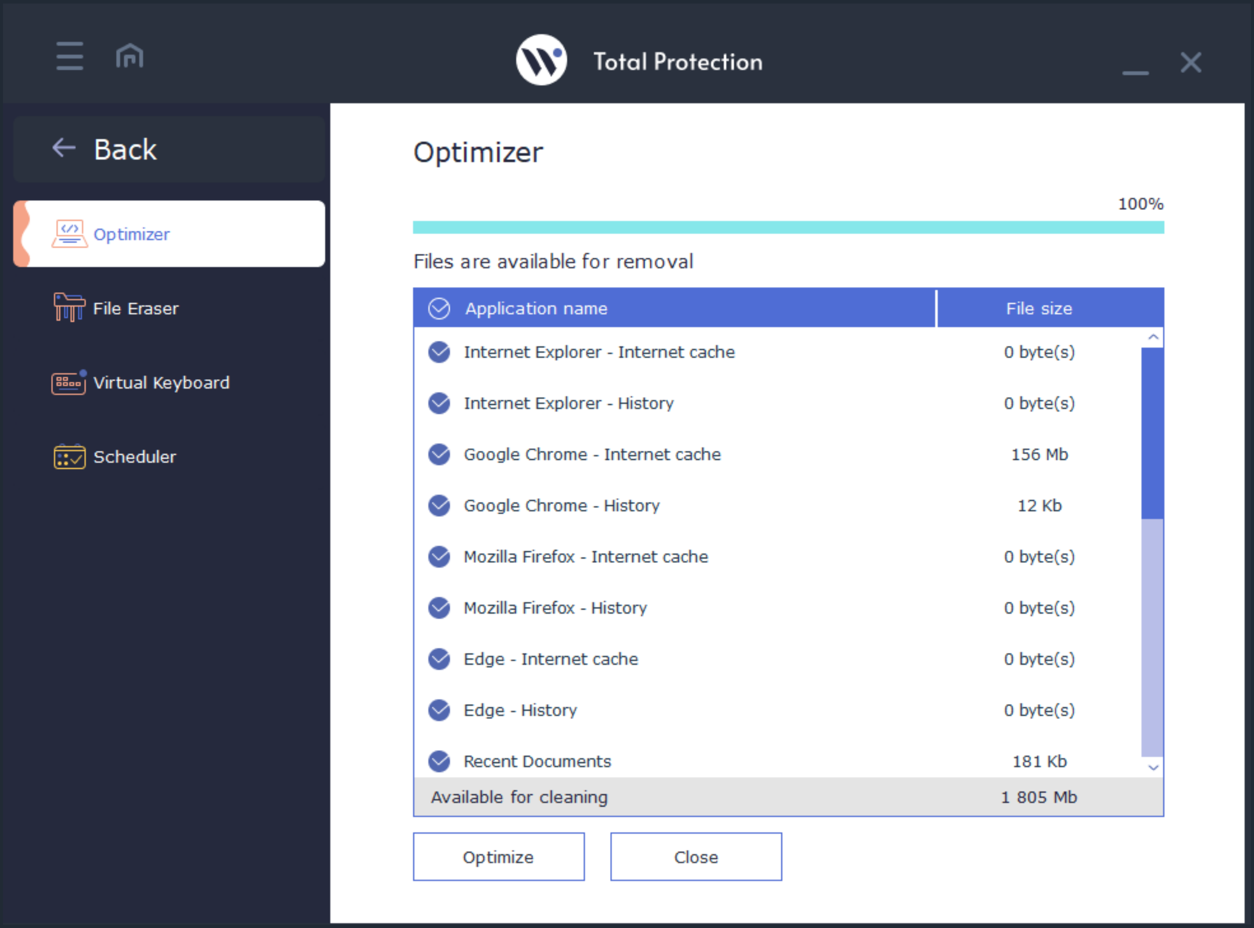
Optimizer

0%

Last optimization: recently

We recommend to use the optimization tool at least 1 time per month. It allows you to maintain a high speed your PC.

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.



Optimizer

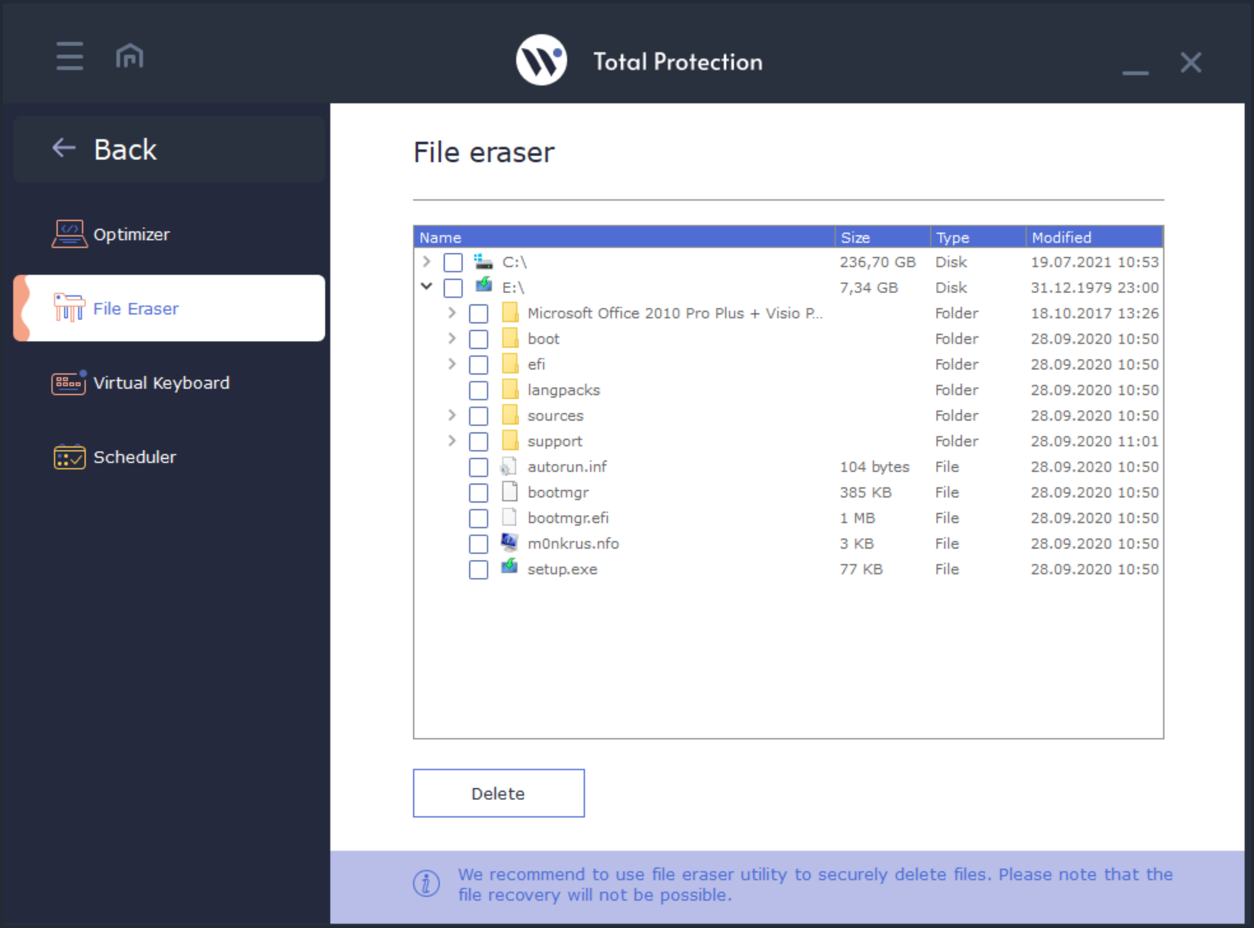
100%

Files are available for removal

Application name	File size
Internet Explorer - Internet cache	0 byte(s)
Internet Explorer - History	0 byte(s)
Google Chrome - Internet cache	156 Mb
Google Chrome - History	12 Kb
Mozilla Firefox - Internet cache	0 byte(s)
Mozilla Firefox - History	0 byte(s)
Edge - Internet cache	0 byte(s)
Edge - History	0 byte(s)
Recent Documents	181 Kb
Available for cleaning	1 805 Mb

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.

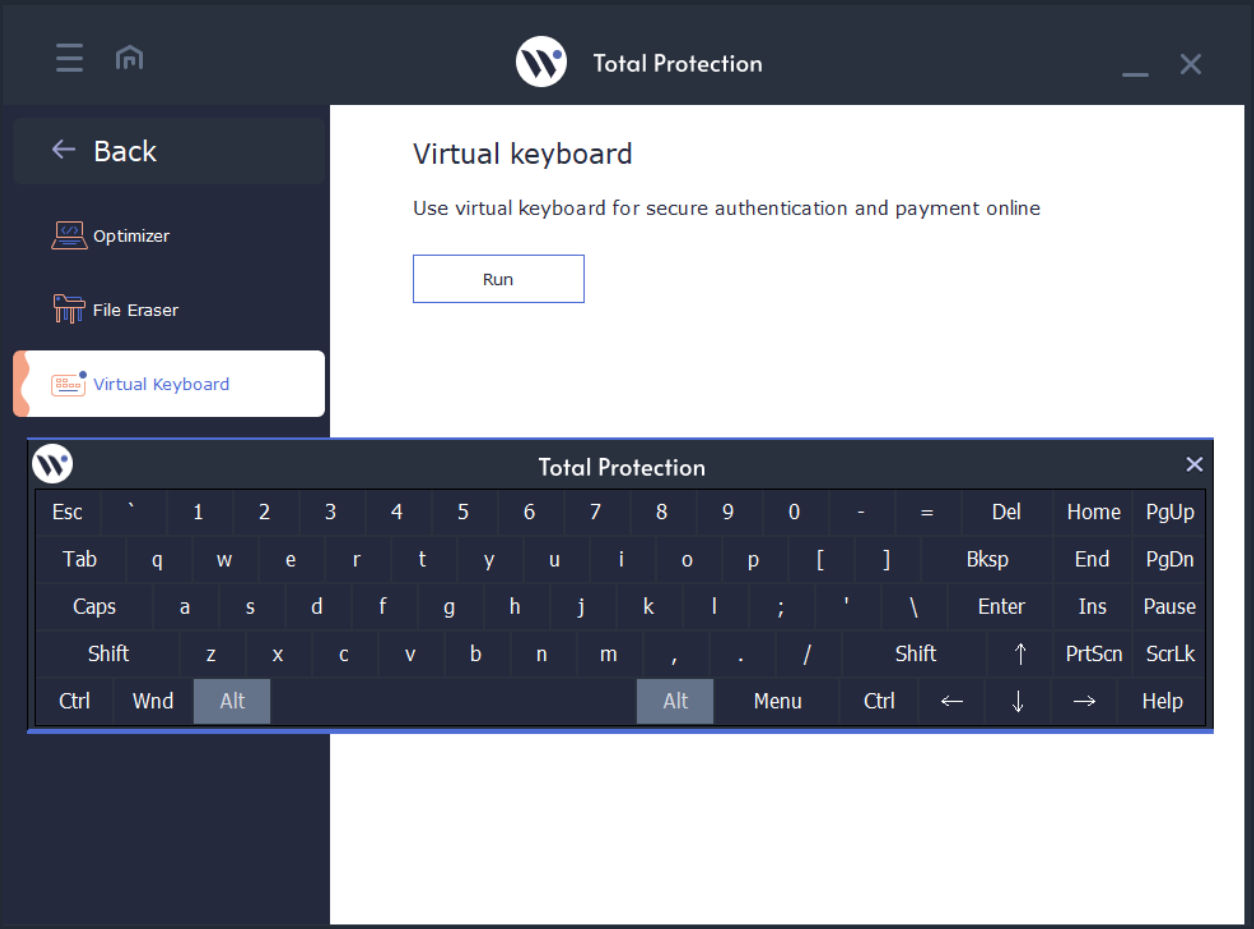


File eraser

Name	Size	Type	Modified
□ C:\	236,70 GB	Disk	19.07.2021 10:53
□ E:\	7,34 GB	Disk	31.12.1979 23:00
□ Microsoft Office 2010 Pro Plus + Visio P...		Folder	18.10.2017 13:26
□ boot		Folder	28.09.2020 10:50
□ efi		Folder	28.09.2020 10:50
□ langpacks		Folder	28.09.2020 10:50
□ sources		Folder	28.09.2020 10:50
□ support		Folder	28.09.2020 11:01
□ autorun.inf	104 bytes	File	28.09.2020 10:50
□ bootmgr	385 KB	File	28.09.2020 10:50
□ bootmgr.efi	1 MB	File	28.09.2020 10:50
□ m0nkrus.nfo	3 KB	File	28.09.2020 10:50
□ setup.exe	77 KB	File	28.09.2020 10:50

We recommend to use file eraser utility to securely delete files. Please note that the file recovery will not be possible.

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.).


Total Protection
Back
Optimizer
File Eraser
Virtual Keyboard

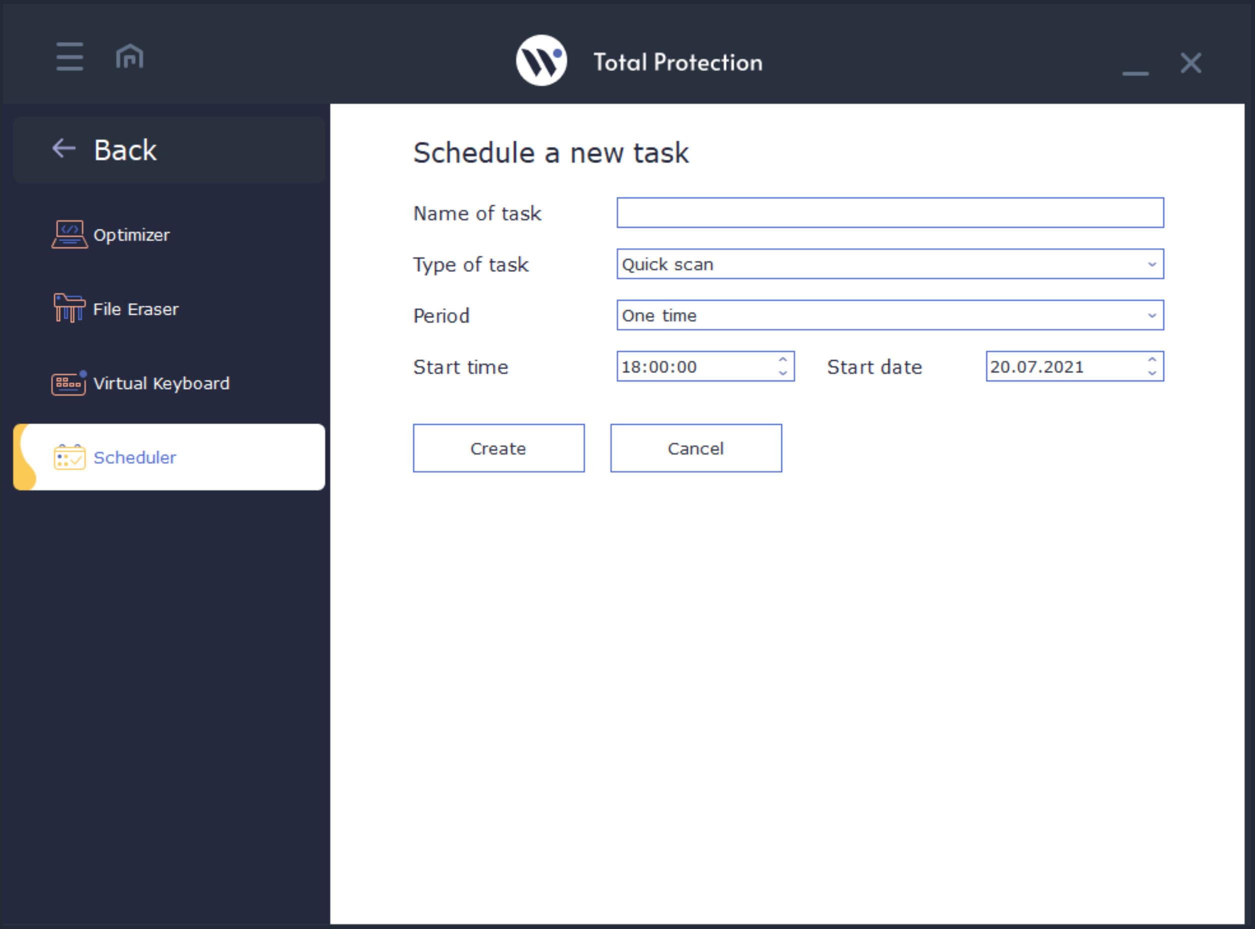
Virtual keyboard

Use virtual keyboard for secure authentication and payment online

Run
Total Protection
Esc ` 1 2 3 4 5 6 7 8 9 0 - = Del Home PgUp
Tab q w e r t y u i o p [ ] Bksp End PgDn
Caps a s d f g h j k l ; ' \ Enter Ins Pause
Shift z x c v b n m , . / Shift ↑ PrtScn ScrLk
Ctrl Wnd Alt Alt Menu Ctrl ← ↓ → Help

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.



Schedule a new task

Name of task

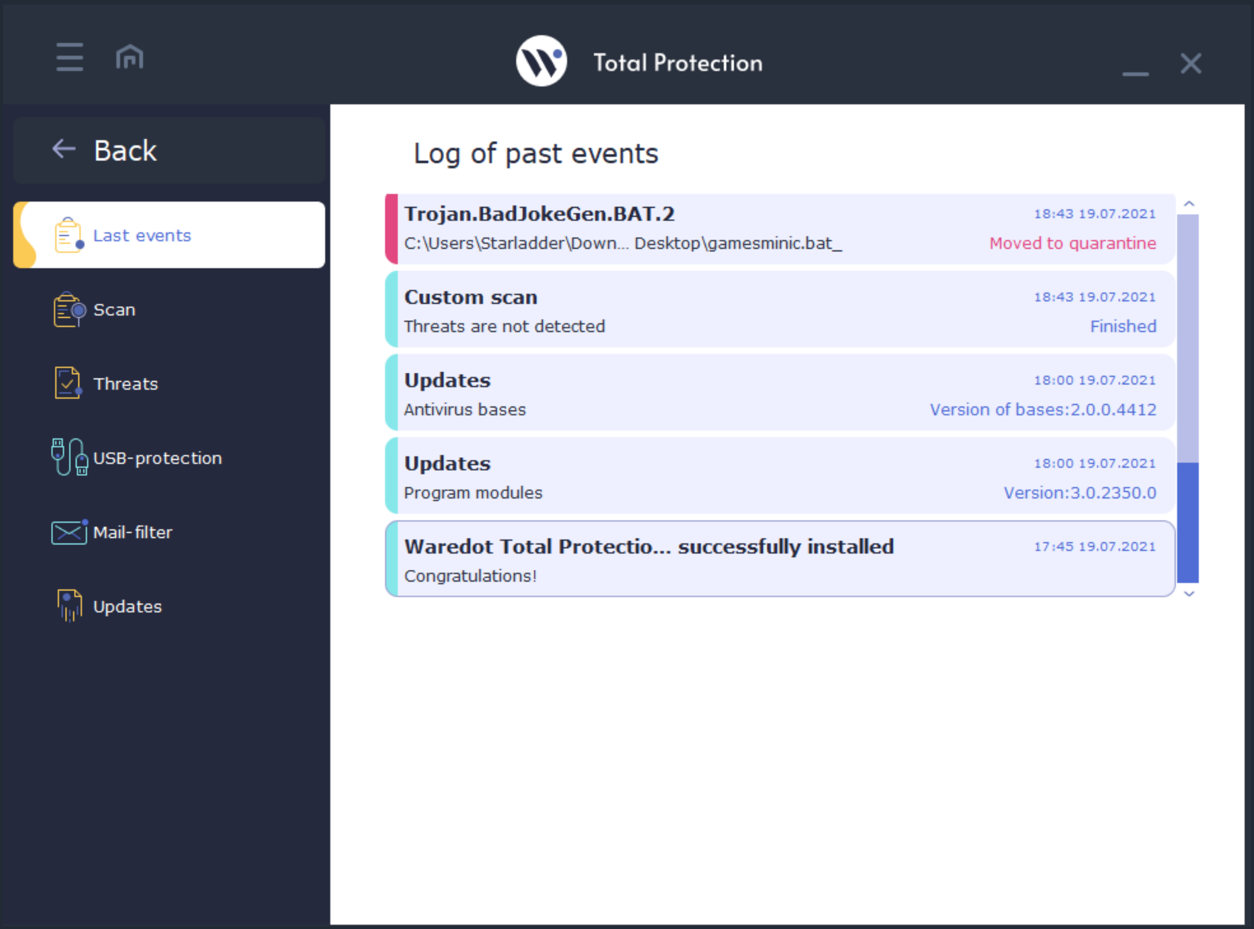
Type of task: Quick scan

Period: One time

Start time: 18:00:00 Start date: 20.07.2021

Reports

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



Log of past events

Trojan.BadJokeGen.BAT.2 18:43 19.07.2021
C:\Users\Starladder\Down... Desktop\gamesminic.bat_ Moved to quarantine

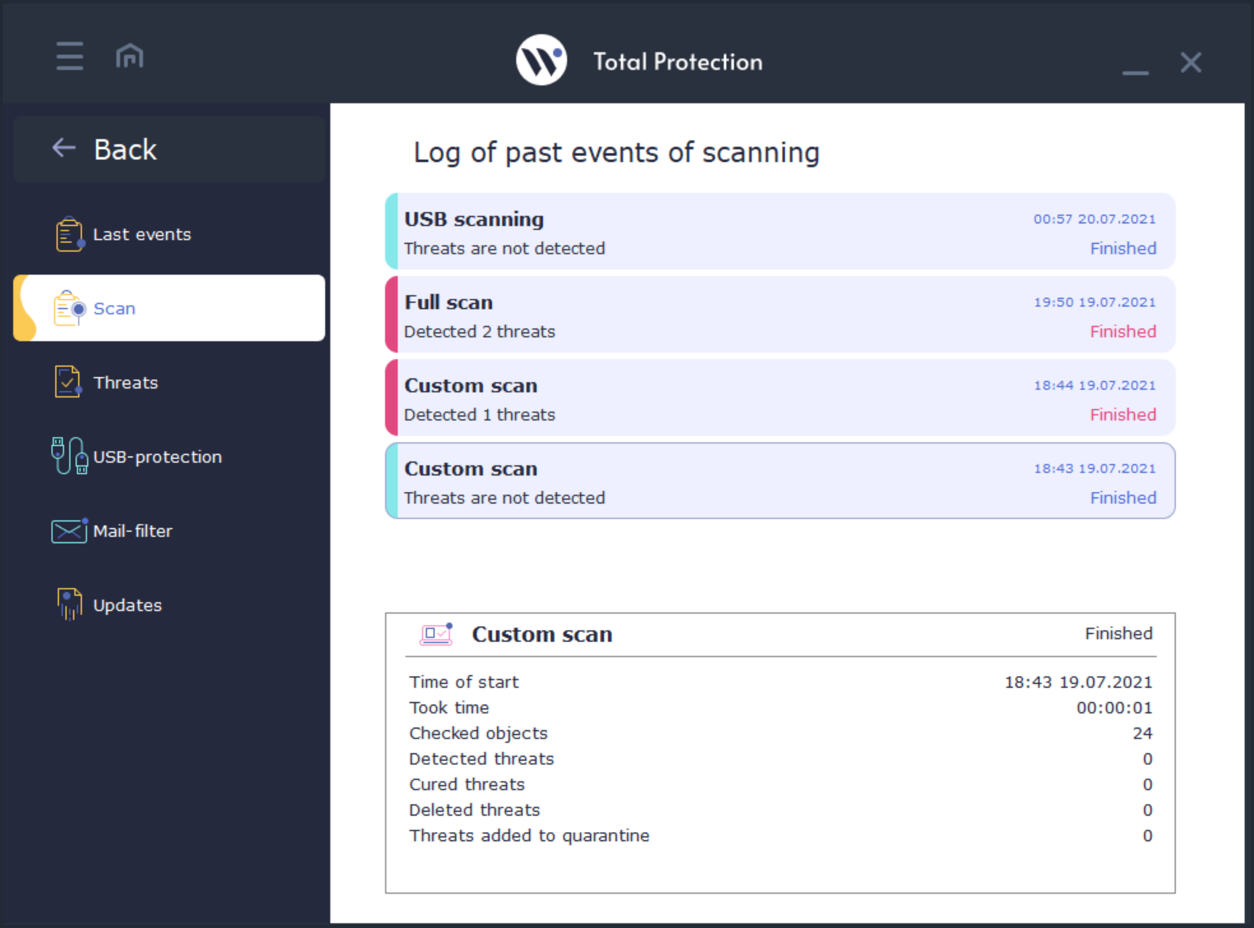
Custom scan 18:43 19.07.2021
Threats are not detected Finished

Updates 18:00 19.07.2021
Antivirus bases Version of bases:2.0.0.4412

Updates 18:00 19.07.2021
Program modules Version:3.0.2350.0

Waredot Total Protectio... successfully installed 17:45 19.07.2021
Congratulations!

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.



Log of past events of scanning

USB scanning 00:57 20.07.2021
Threats are not detected — Finished

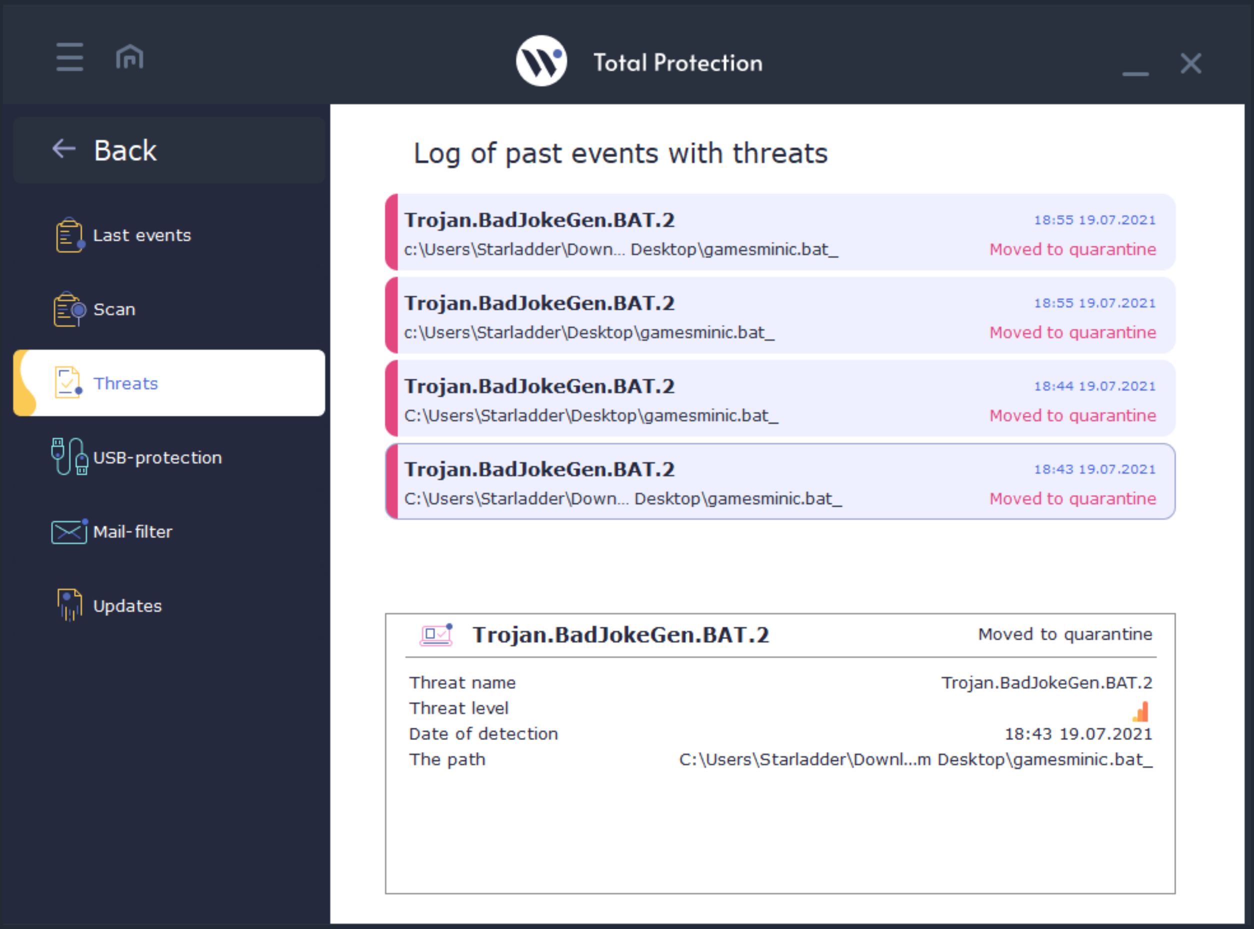
Full scan 19:50 19.07.2021
Detected 2 threats — Finished

Custom scan 18:44 19.07.2021
Detected 1 threats — Finished

Custom scan 18:43 19.07.2021
Threats are not detected — Finished

Custom scan	Finished
Time of start	18:43 19.07.2021
Took time	00:00:01
Checked objects	24
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.



Log of past events with threats

Trojan.BadJokeGen.BAT.2 18:55 19.07.2021
c:\Users\Starladder\Down... Desktop\gamesminic.bat_ Moved to quarantine

Trojan.BadJokeGen.BAT.2 18:55 19.07.2021
c:\Users\Starladder\Desktop\gamesminic.bat_ Moved to quarantine

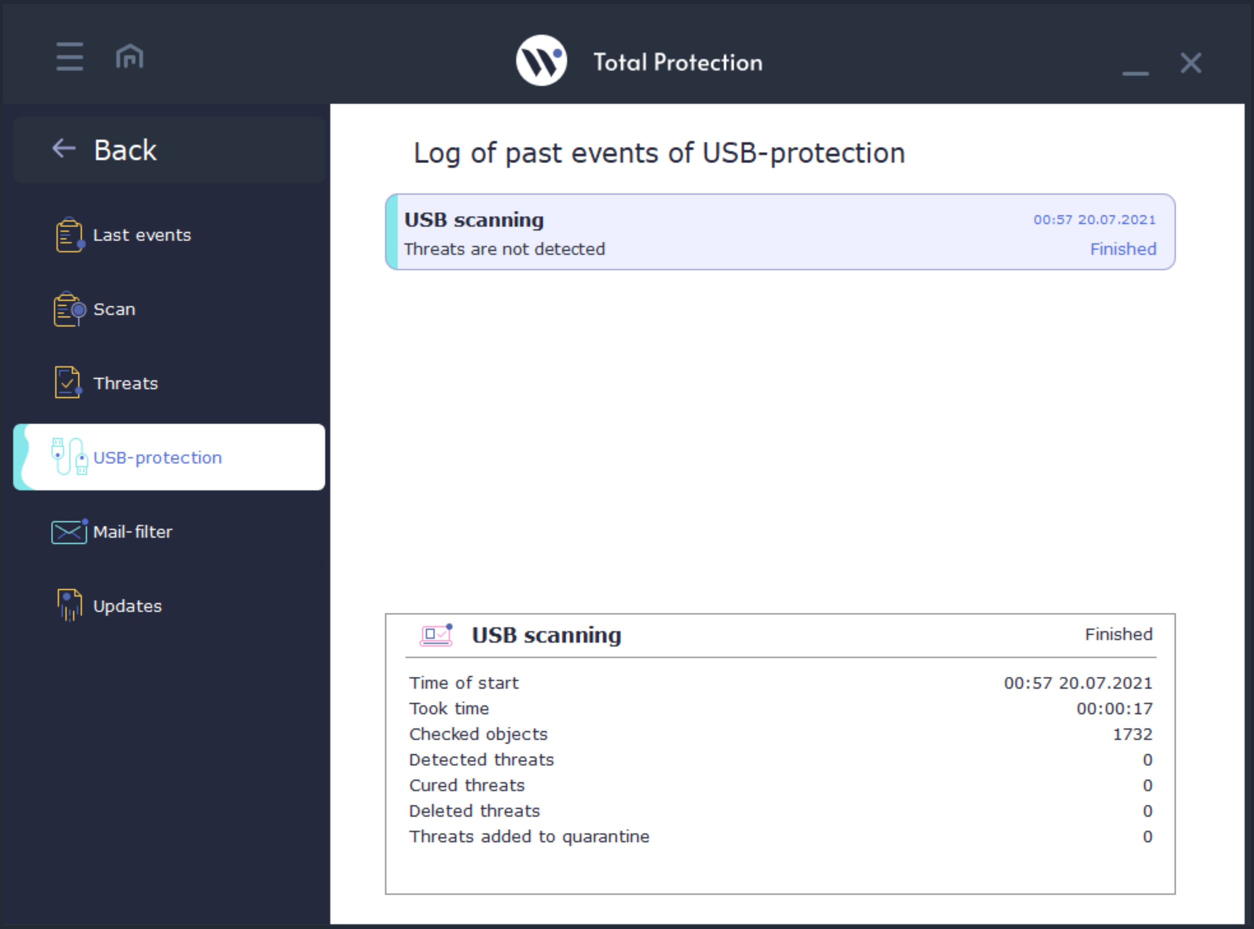
Trojan.BadJokeGen.BAT.2 18:44 19.07.2021
C:\Users\Starladder\Desktop\gamesminic.bat_ Moved to quarantine

Trojan.BadJokeGen.BAT.2 18:43 19.07.2021
C:\Users\Starladder\Down... Desktop\gamesminic.bat_ Moved to quarantine

Trojan.BadJokeGen.BAT.2 Moved to quarantine

Threat name	Trojan.BadJokeGen.BAT.2
Threat level	
Date of detection	18:43 19.07.2021
The path	C:\Users\Starladder\Downl...m Desktop\gamesminic.bat_

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.

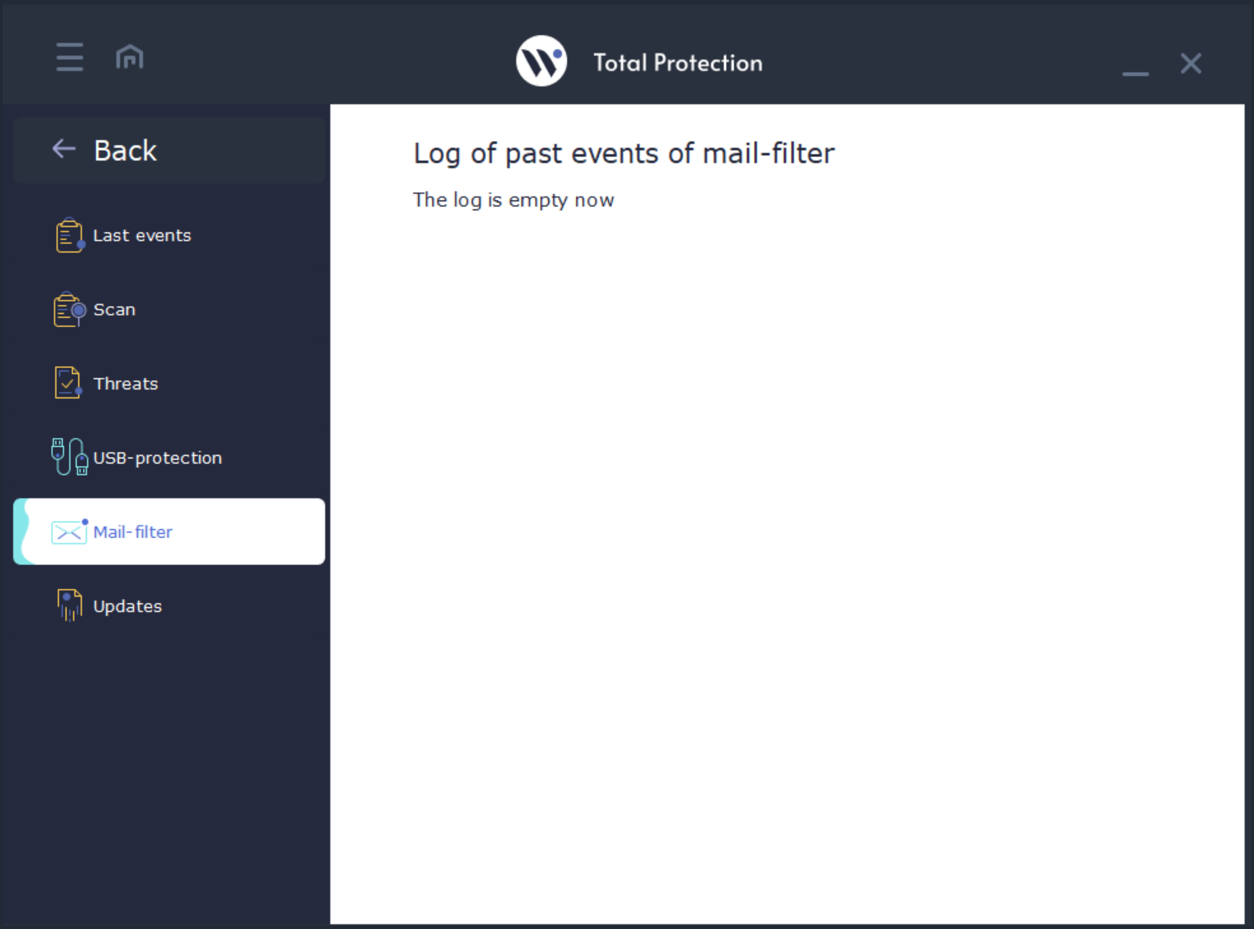


Log of past events of USB-protection

USB scanning 00:57 20.07.2021
Threats are not detected Finished

USB scanning	Finished
Time of start	00:57 20.07.2021
Took time	00:00:17
Checked objects	1732
Detected threats	0
Cured threats	0
Deleted threats	0
Threats added to quarantine	0

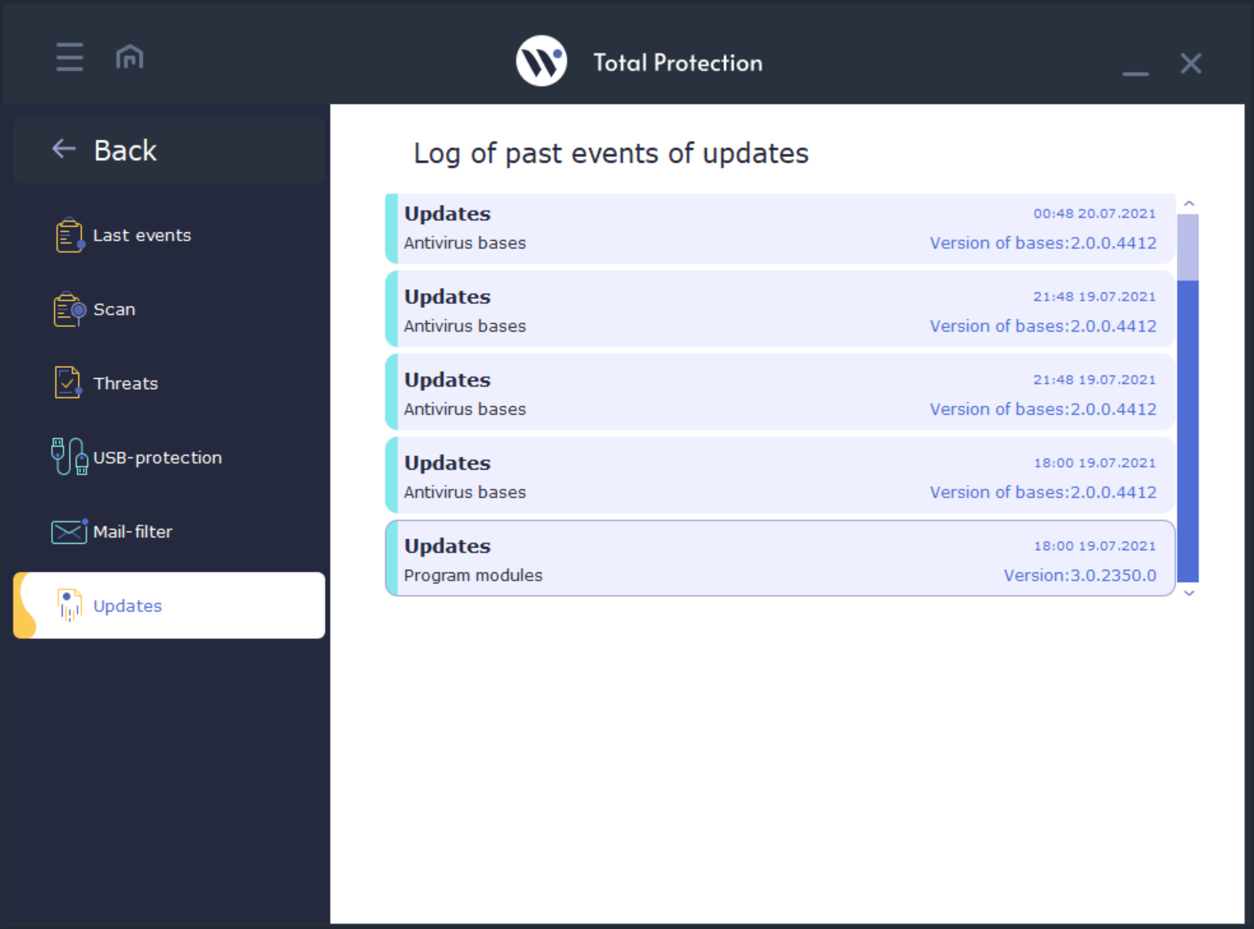
Mail-filter - this tab displays the information about the letters in which attachments were detected threats. Antivirus scans only letters in the mail clients (like The Bat, Outlook Express, Mozilla Thunderbird, etc.) rather than in a web browser. Information is displayed in list format.



Log of past events of mail-filter

The log is empty now

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.



Log of past events of updates

Updates 00:48 20.07.2021
Antivirus bases Version of bases:2.0.0.4412

Updates 21:48 19.07.2021
Antivirus bases Version of bases:2.0.0.4412

Updates 21:48 19.07.2021
Antivirus bases Version of bases:2.0.0.4412

Updates 18:00 19.07.2021
Antivirus bases Version of bases:2.0.0.4412

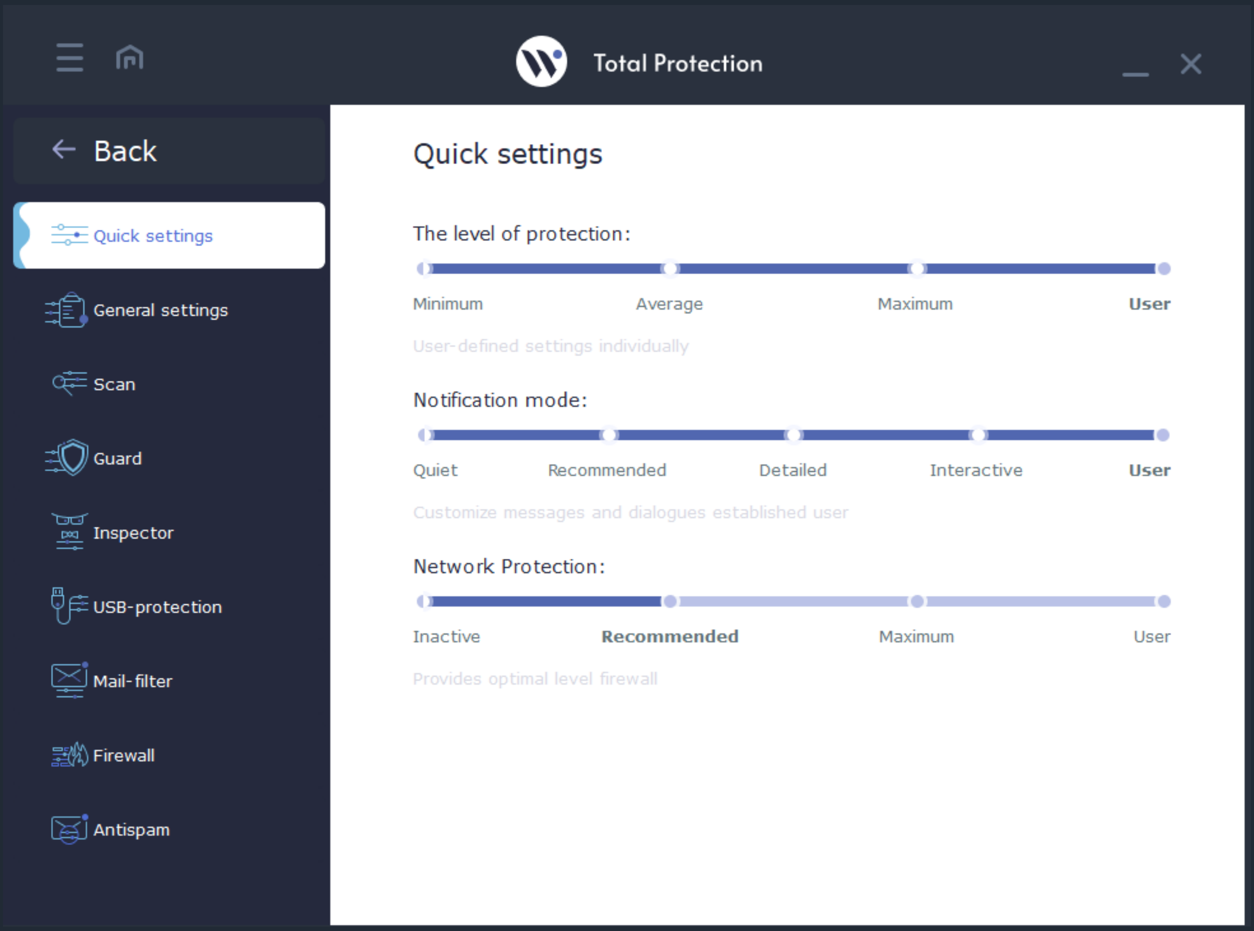
Updates 18:00 19.07.2021
Program modules Version:3.0.2350.0

Settings of Waredot Total Protection

User can set up Waredot Total Protection 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.



Quick settings

The level of protection:

Minimum — Average — Maximum — **User**

User-defined settings individually

Notification mode:

Quiet — Recommended — Detailed — Interactive — **User**

Customize messages and dialogues established user

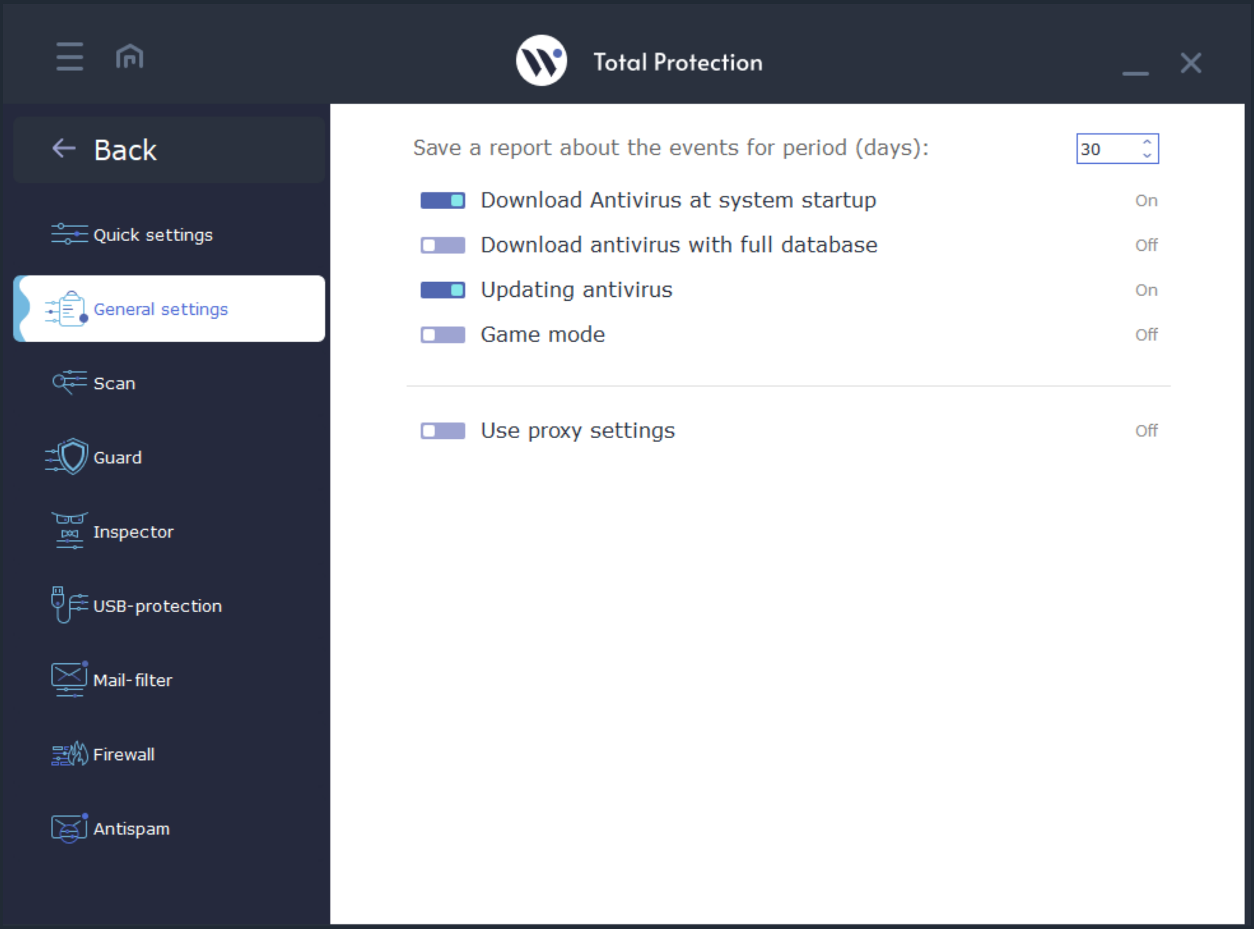
Network Protection:

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.



Save a report about the events for period (days): 30

Download Antivirus at system startup On

Download antivirus with full database Off

Updating antivirus On

Game mode Off

Use proxy settings Off

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.

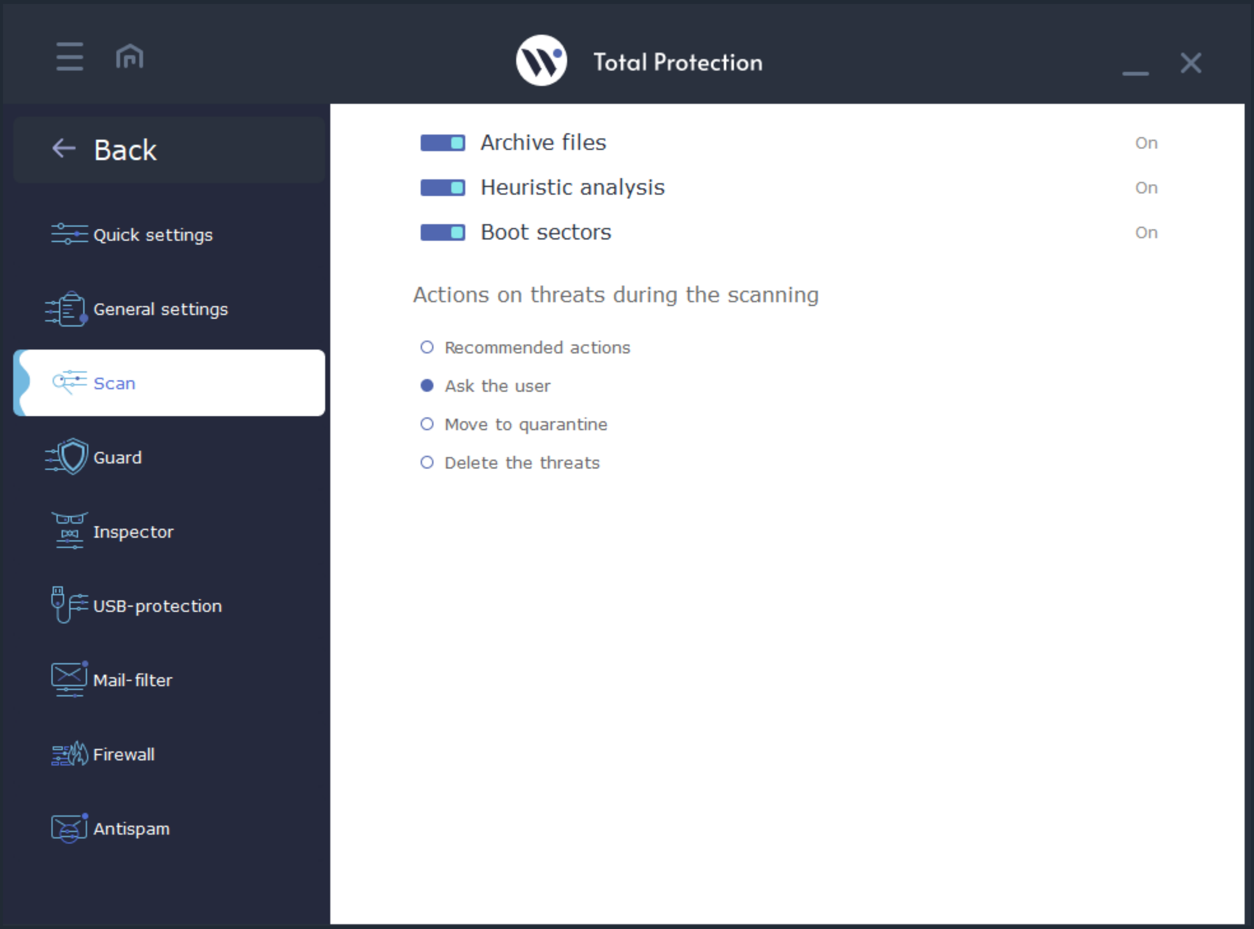
Actions on threats during the scanning:

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 Total Protection;

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



Archive files On

Heuristic analysis On

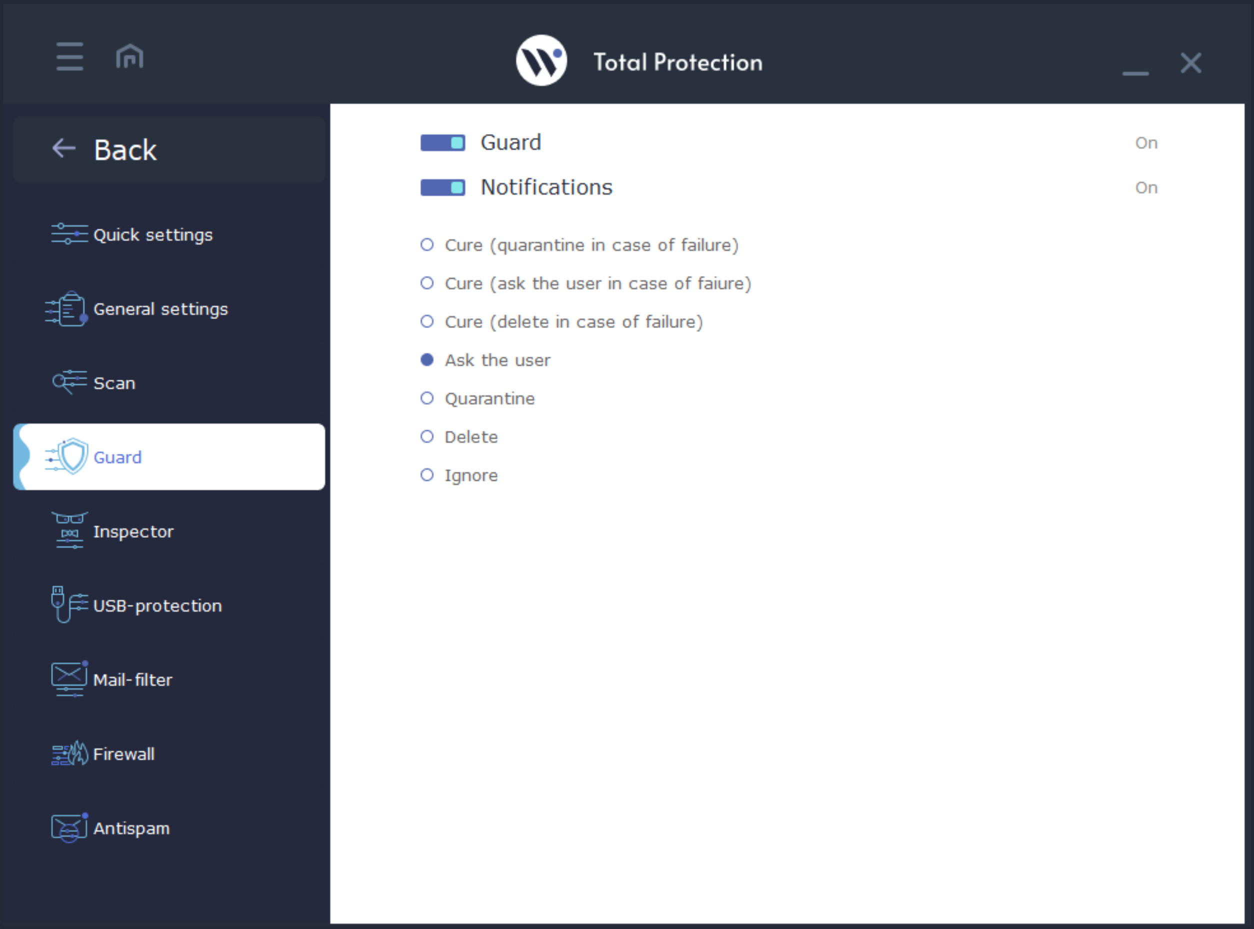
Boot sectors On

Actions on threats during the scanning

○ Recommended actions
● Ask the user
○ Move to quarantine
○ Delete the threats

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.



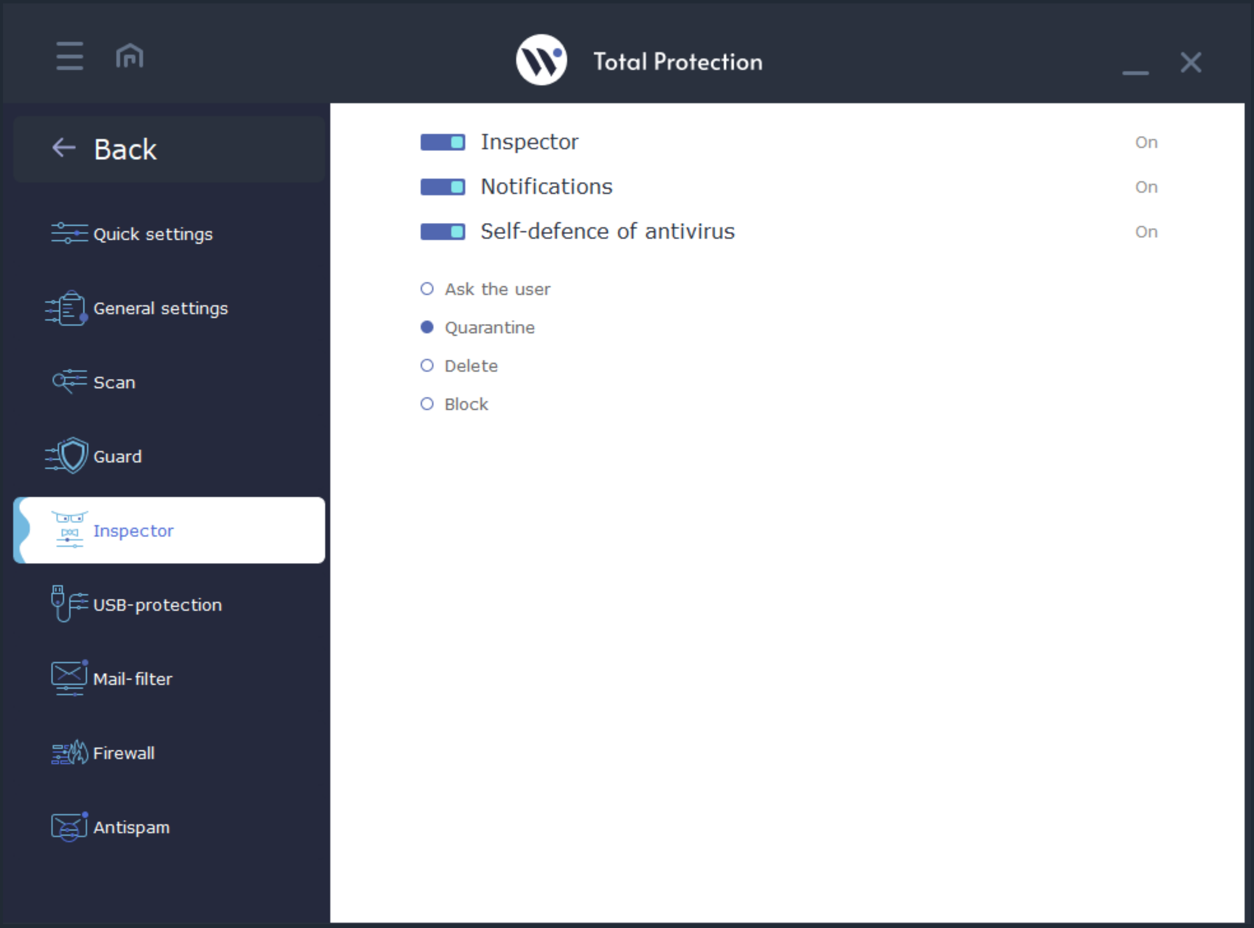
Guard On

Notifications On

○ Cure (quarantine in case of failure)
○ Cure (ask the user in case of faiure)
○ Cure (delete in case of failure)
● Ask the user
○ Quarantine
○ Delete
○ Ignore

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.



Inspector On

Notifications On

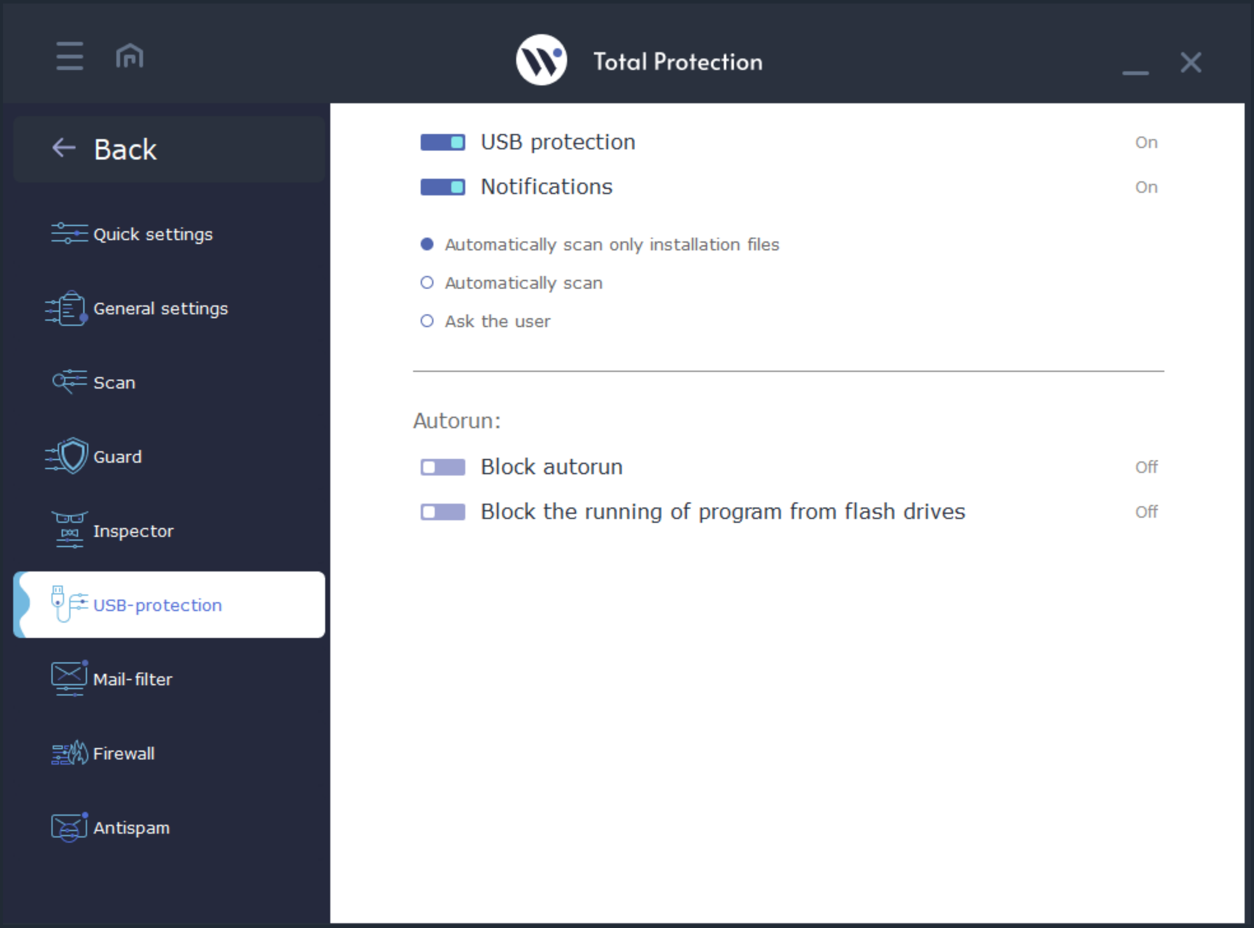
Self-defence of antivirus On

○ Ask the user
● Quarantine
○ Delete
○ Block

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.



USB protection On

Notifications On

● Automatically scan only installation files

○ Automatically scan

○ Ask the user

Autorun:

Block autorun Off

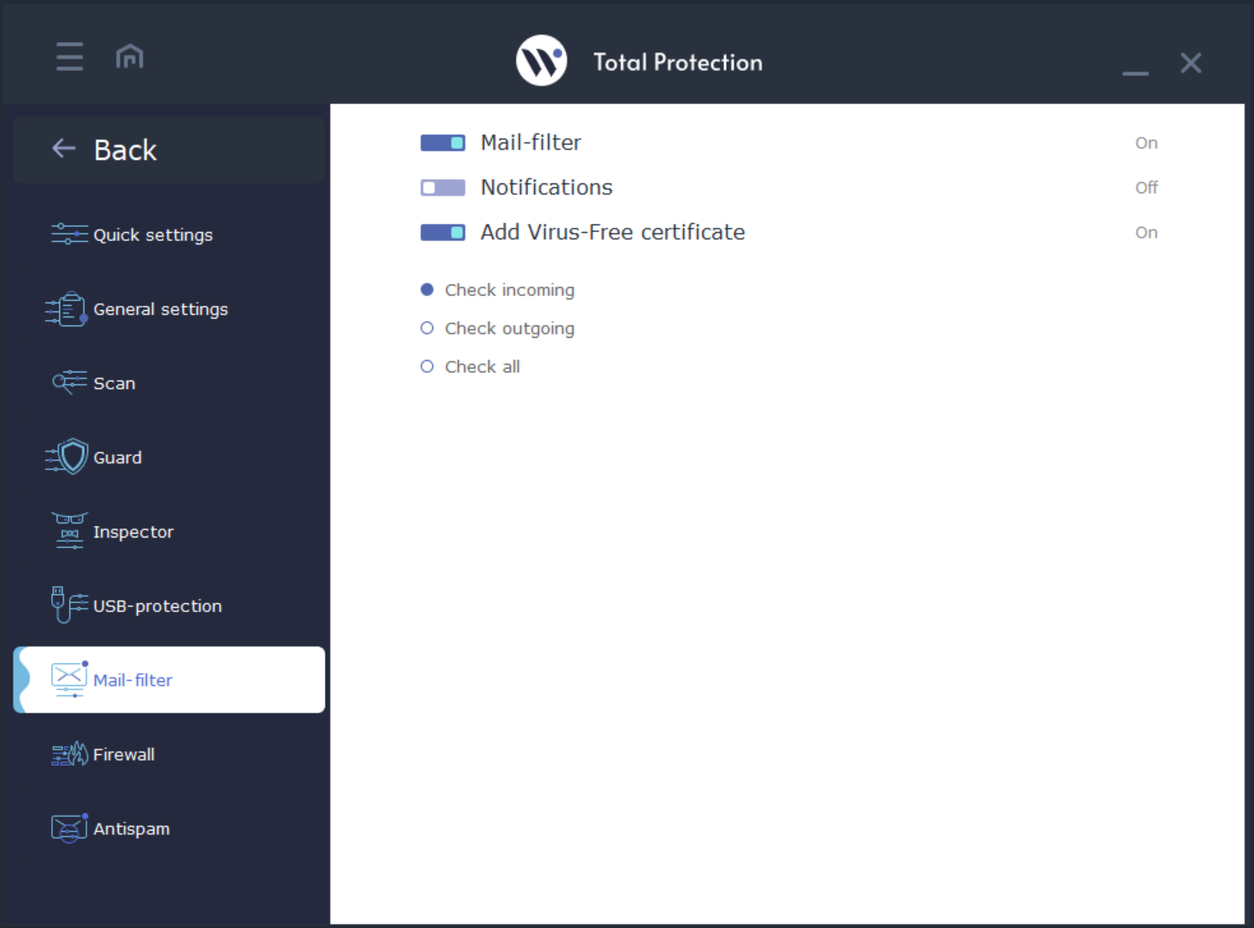
Block the running of program from flash drives Off

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 Total Protection.

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.



Mail-filter	On
Notifications	Off
Add Virus-Free certificate	On

● Check incoming
○ Check outgoing
○ Check all

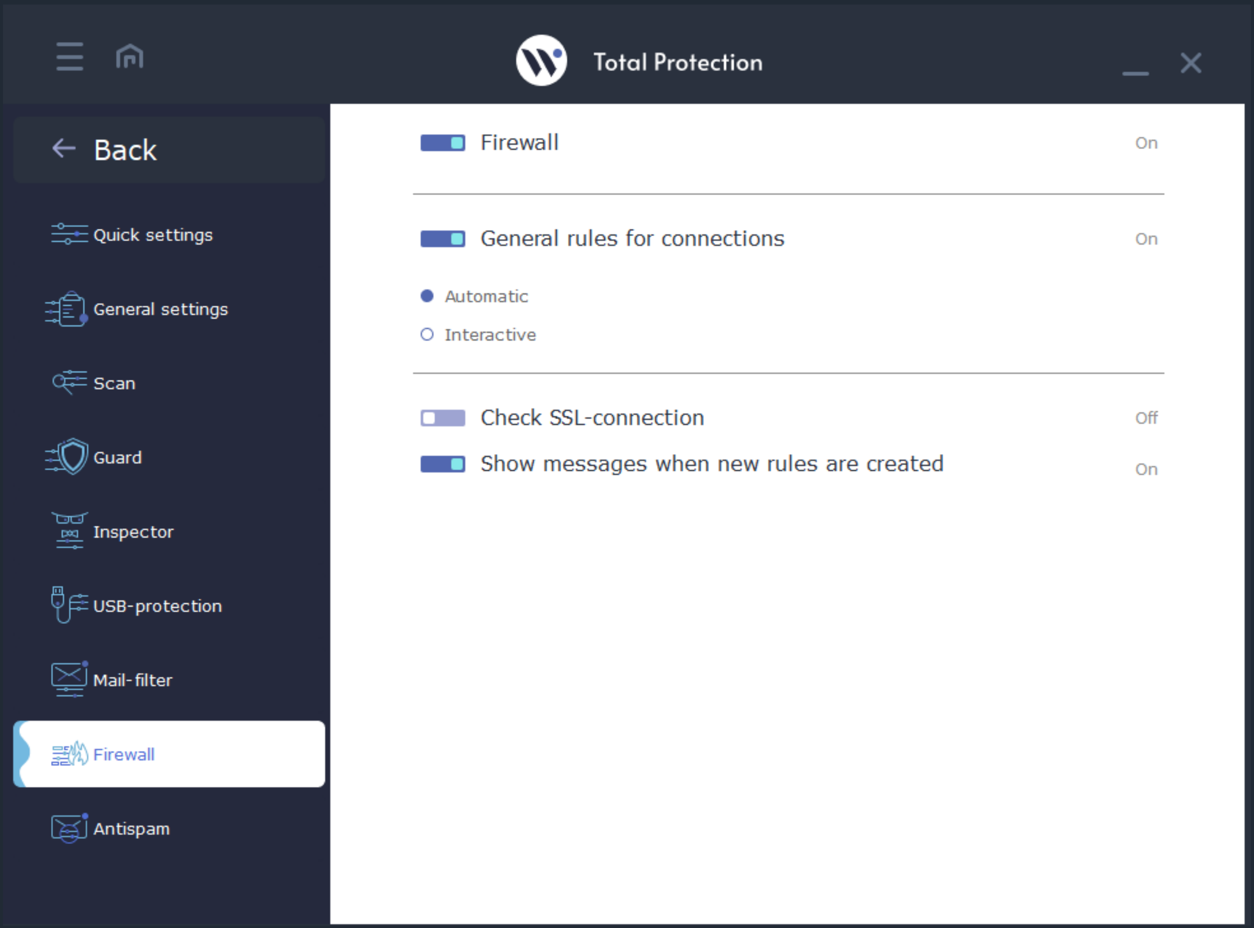
Firewall - sets the rules of incoming and outgoing connections for programs installed on your PC.

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

- Automatic - Waredot Total Protection set the rule for every program according to our base of the optimal rules.
- Interactive – in this mode Waredot Total Protection 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.



Firewall On

General rules for connections On

● Automatic

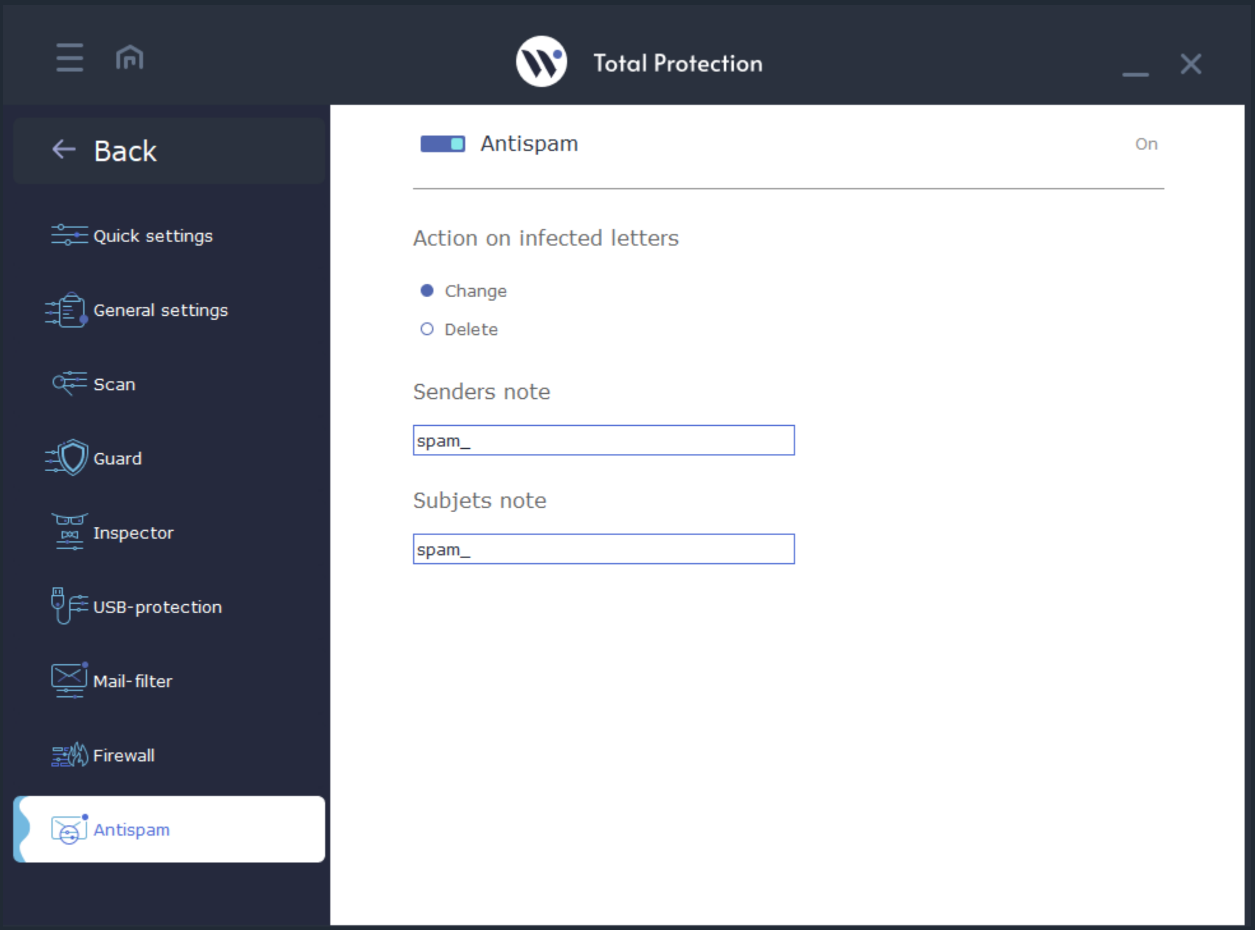
○ Interactive

Check SSL-connection Off

Show messages when new rules are created On

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.



Antispam On

Action on infected letters

● Change

○ Delete

Senders note

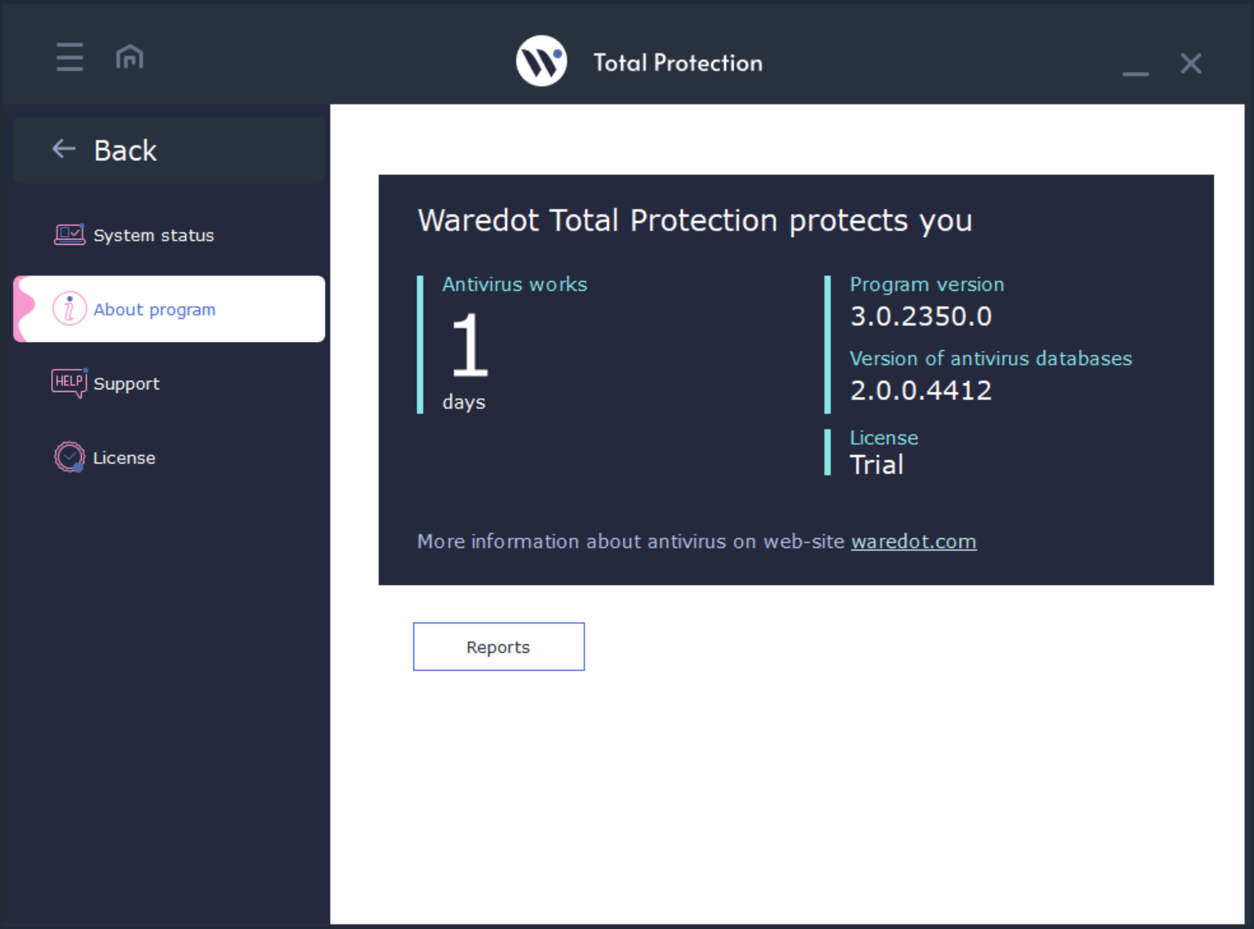
spam_

Subjets note

spam_

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.



Waredot Total Protection protects you

Antivirus works
1
days

Program version
3.0.2350.0

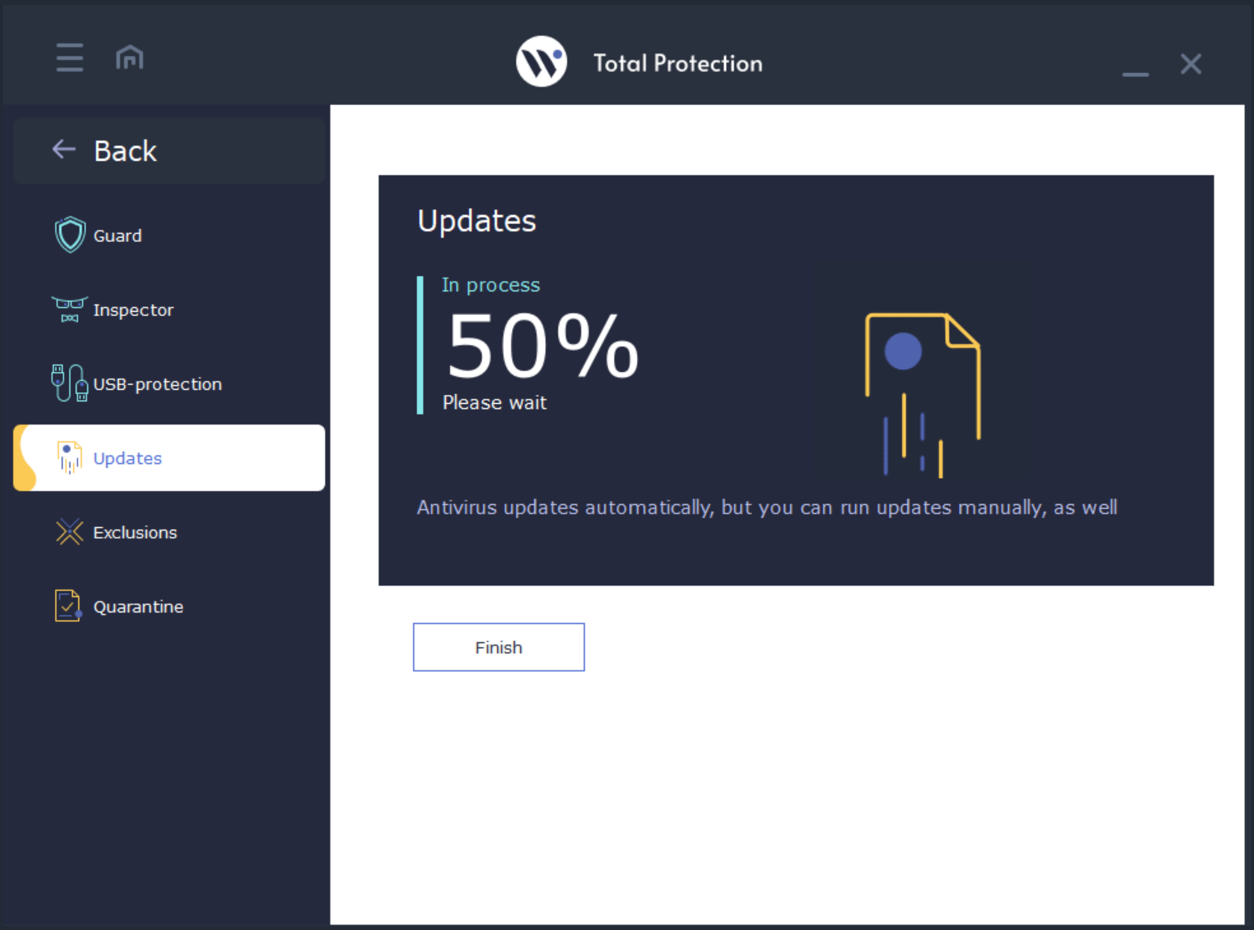
Version of antivirus databases
2.0.0.4412

License
Trial

More information about antivirus on web-site waredot.com

Updating takes place in two stages:

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



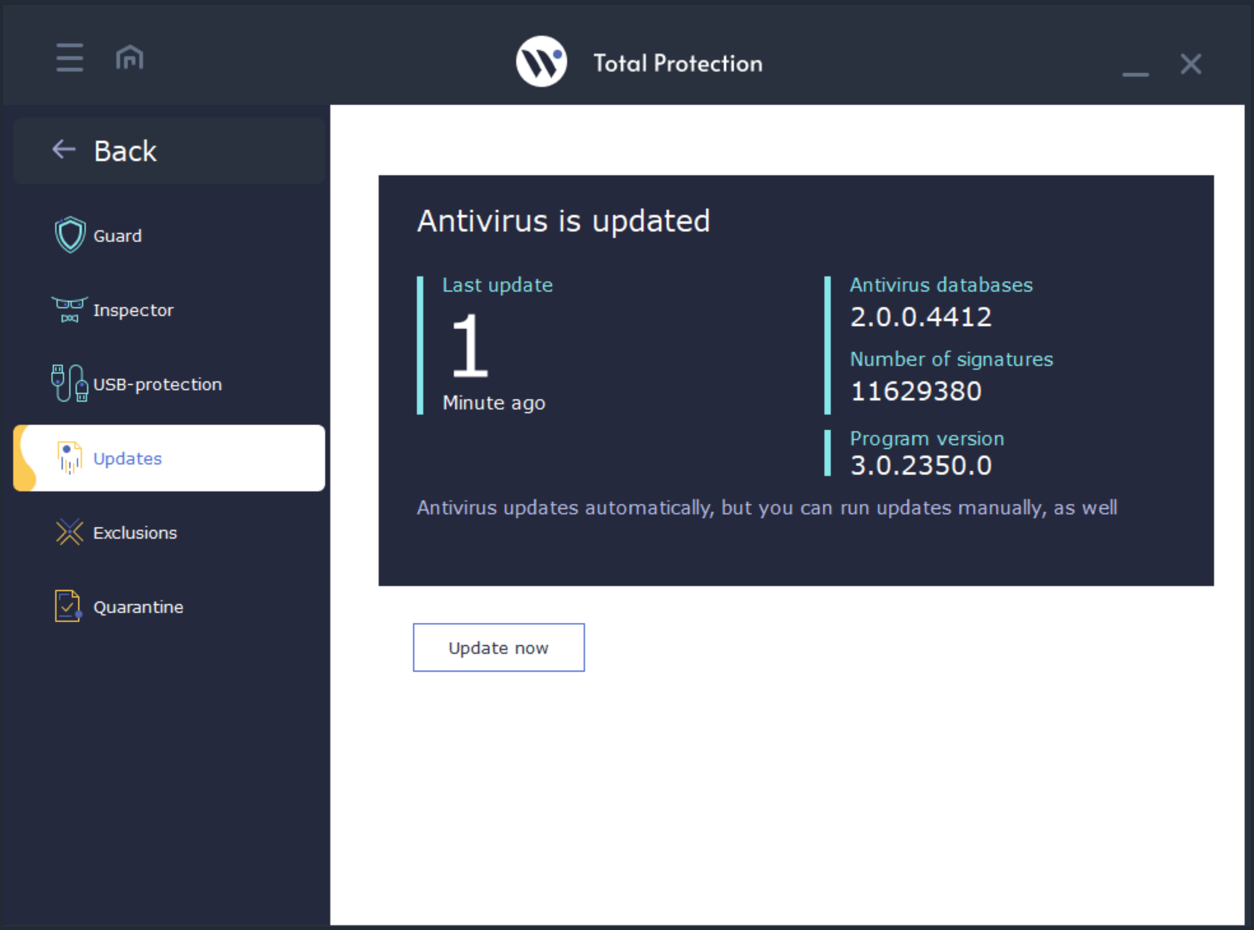
Updates

In process

50%

Please wait

Antivirus updates automatically, but you can run updates manually, as well



Antivirus is updated

Last update
1
Minute ago

Antivirus databases
2.0.0.4412

Number of signatures
11629380

Program version
3.0.2350.0

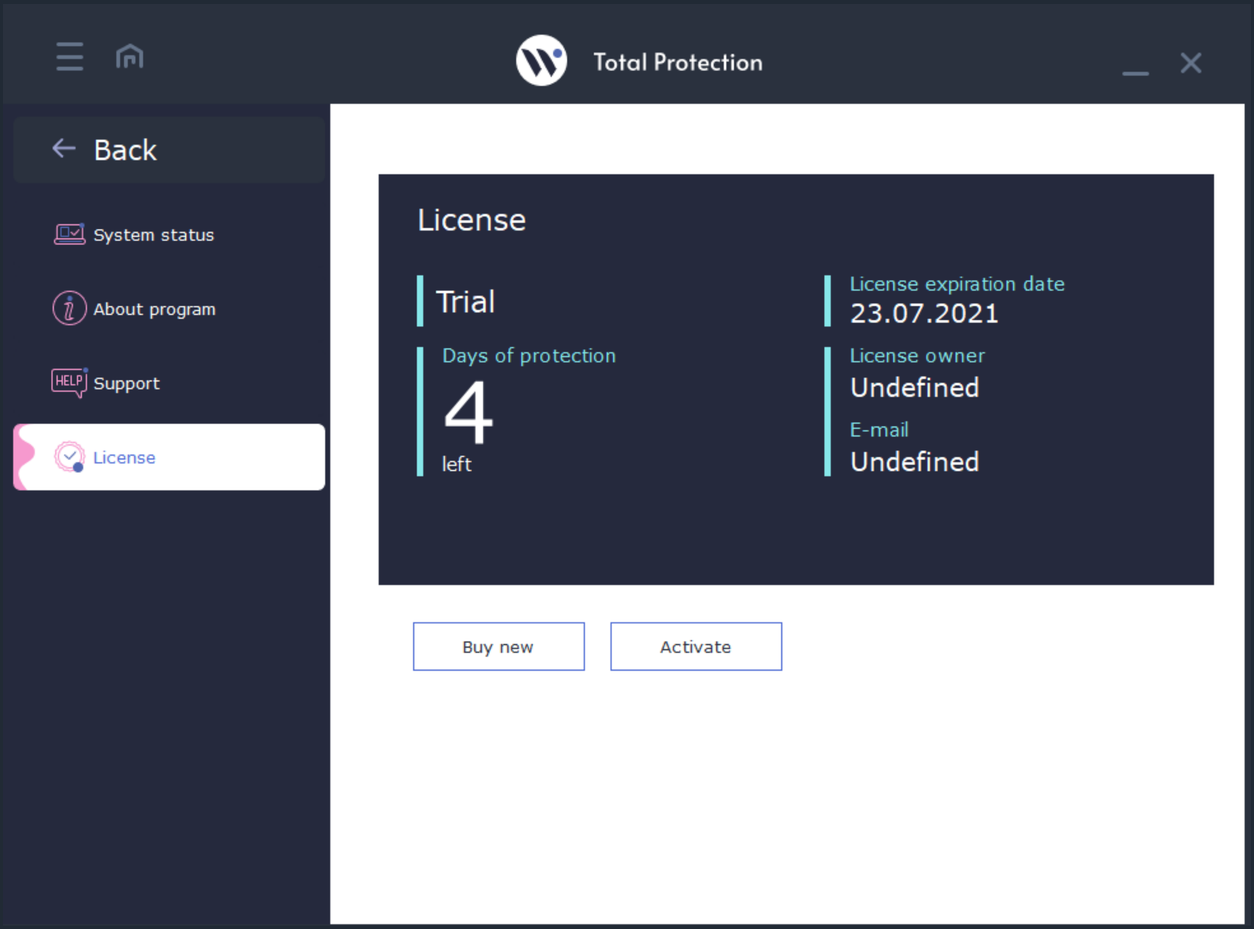
Antivirus updates automatically, but you can run updates manually, as well

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 Total Protection registration

This is how unregistered program window looks like:



License

Trial

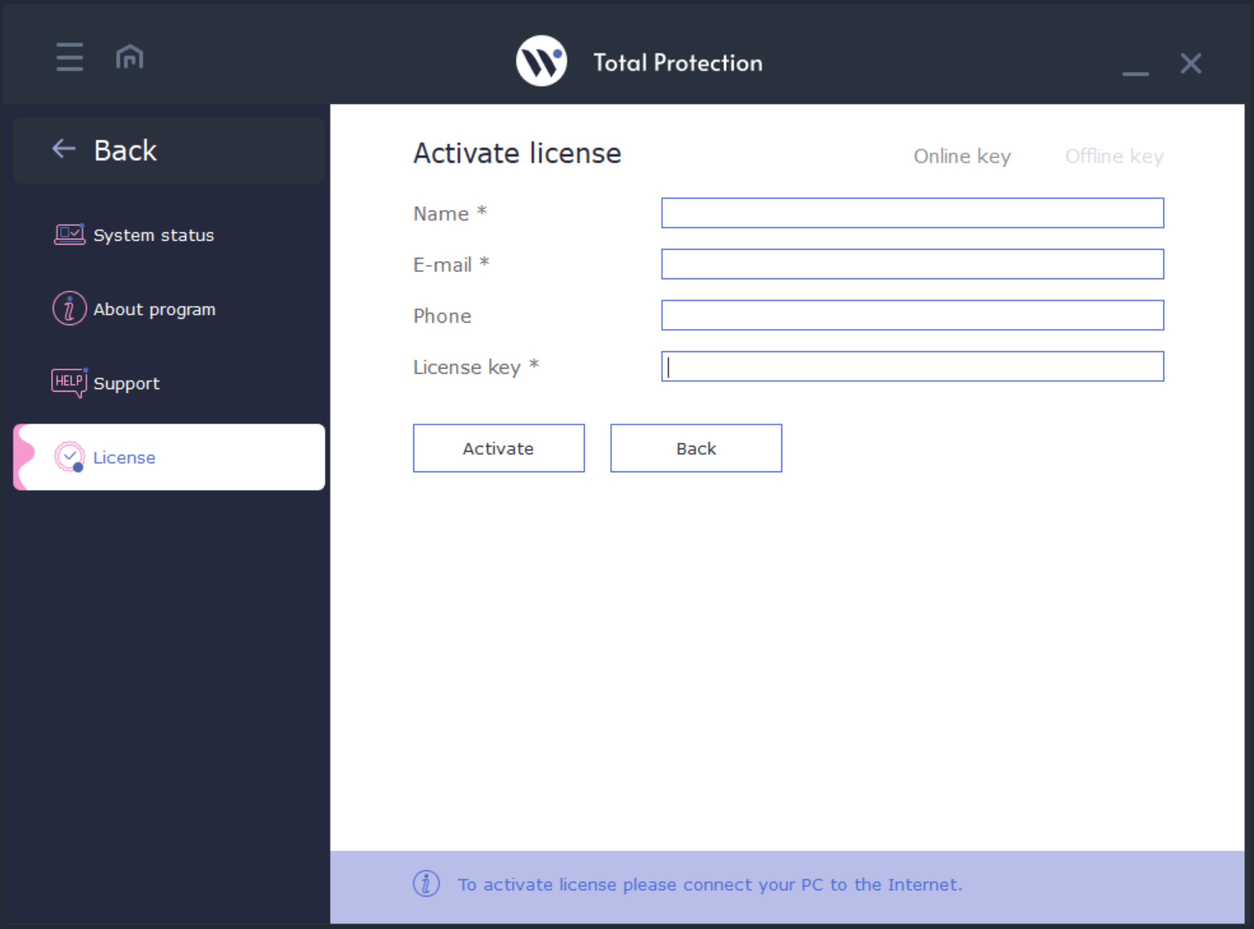
Days of protection
4
left

License expiration date
23.07.2021

License owner
Undefined

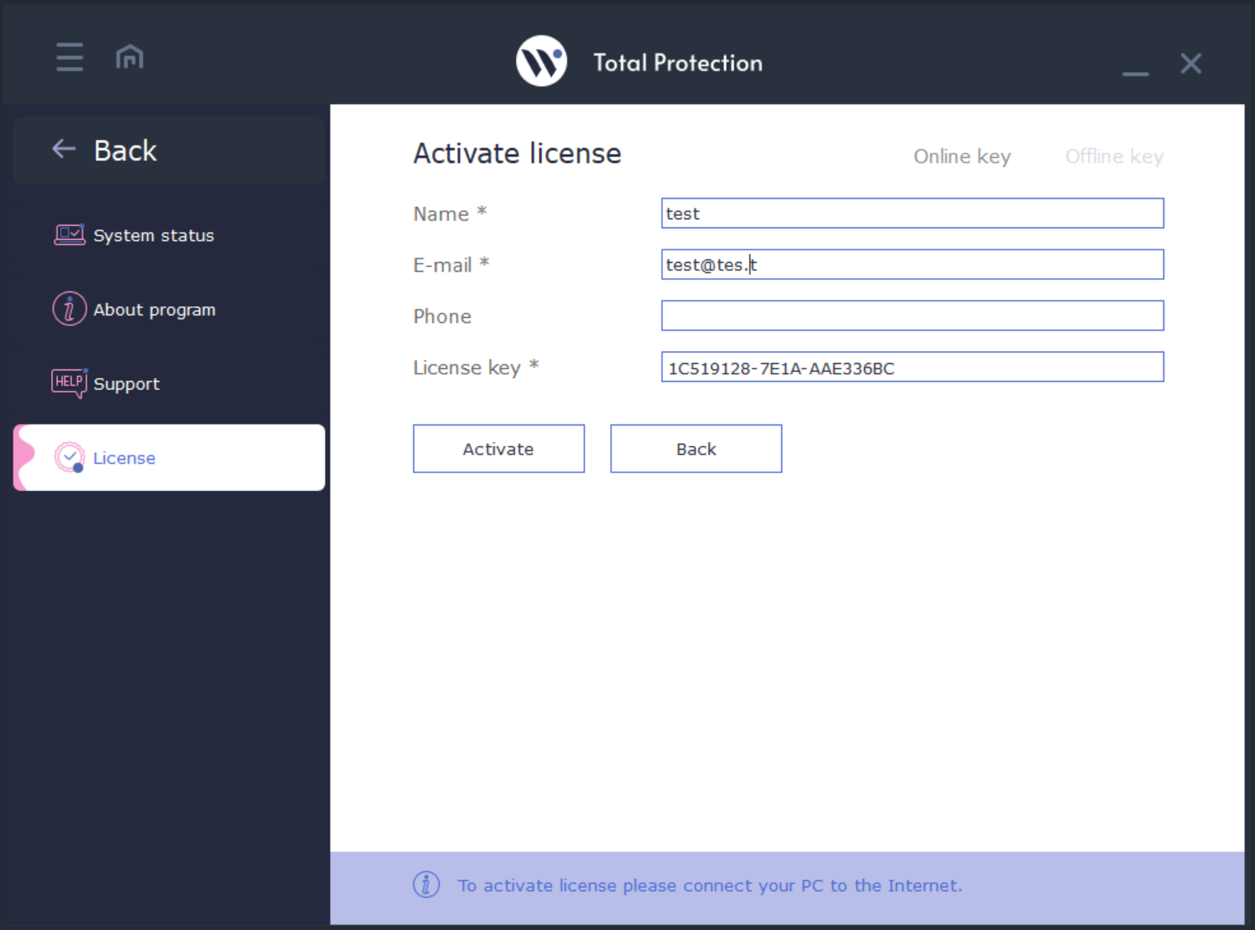
E-mail
Undefined

To register the program, open the main window of Waredot Total Protection, go to the tab **"License"** and click **"Activate"** button or "Buy new" if you need to buy the new License:



To activate license please connect your PC to the Internet.

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

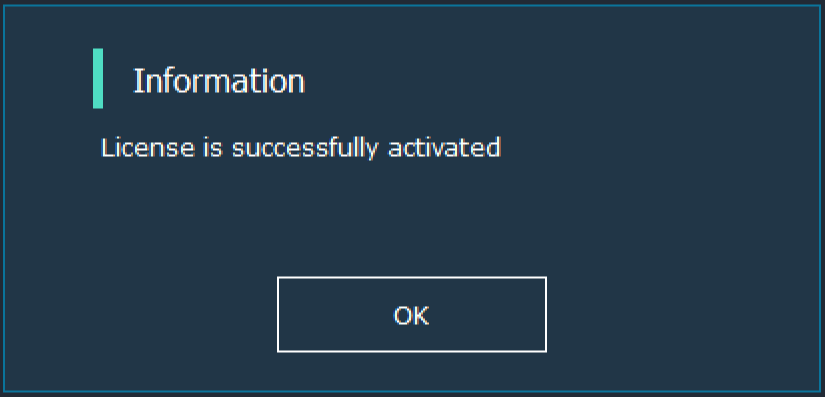


Activate license

Name *	test
E-mail *	test@tes.t
Phone	
License key *	1C519128-7E1A-AAE336BC

To activate license please connect your PC to the Internet.

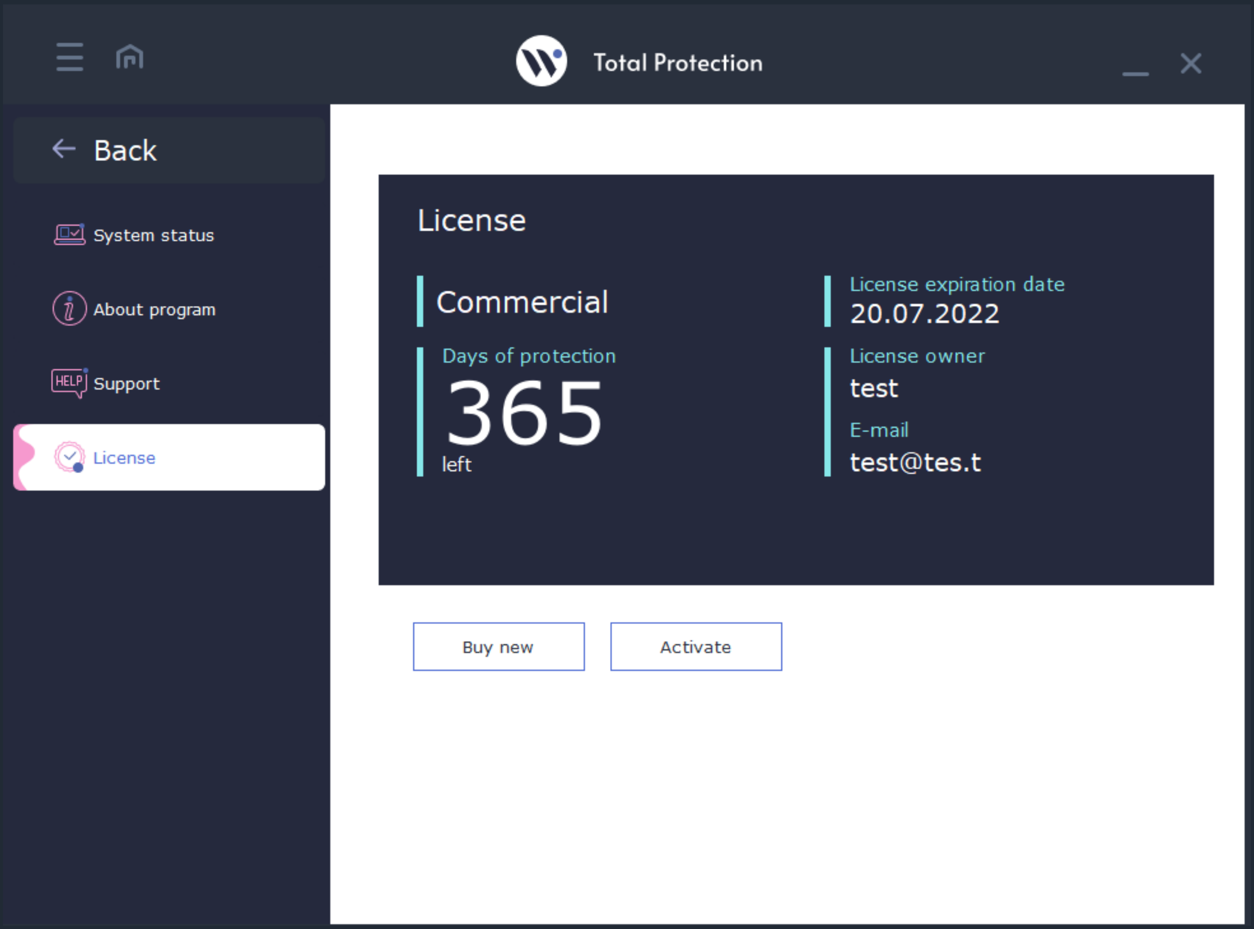
Waredot Total Protection will inform you about the result of activation of your License:



Information

License is successfully activated

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



License

Commercial

Days of protection
365
left

License expiration date
20.07.2022

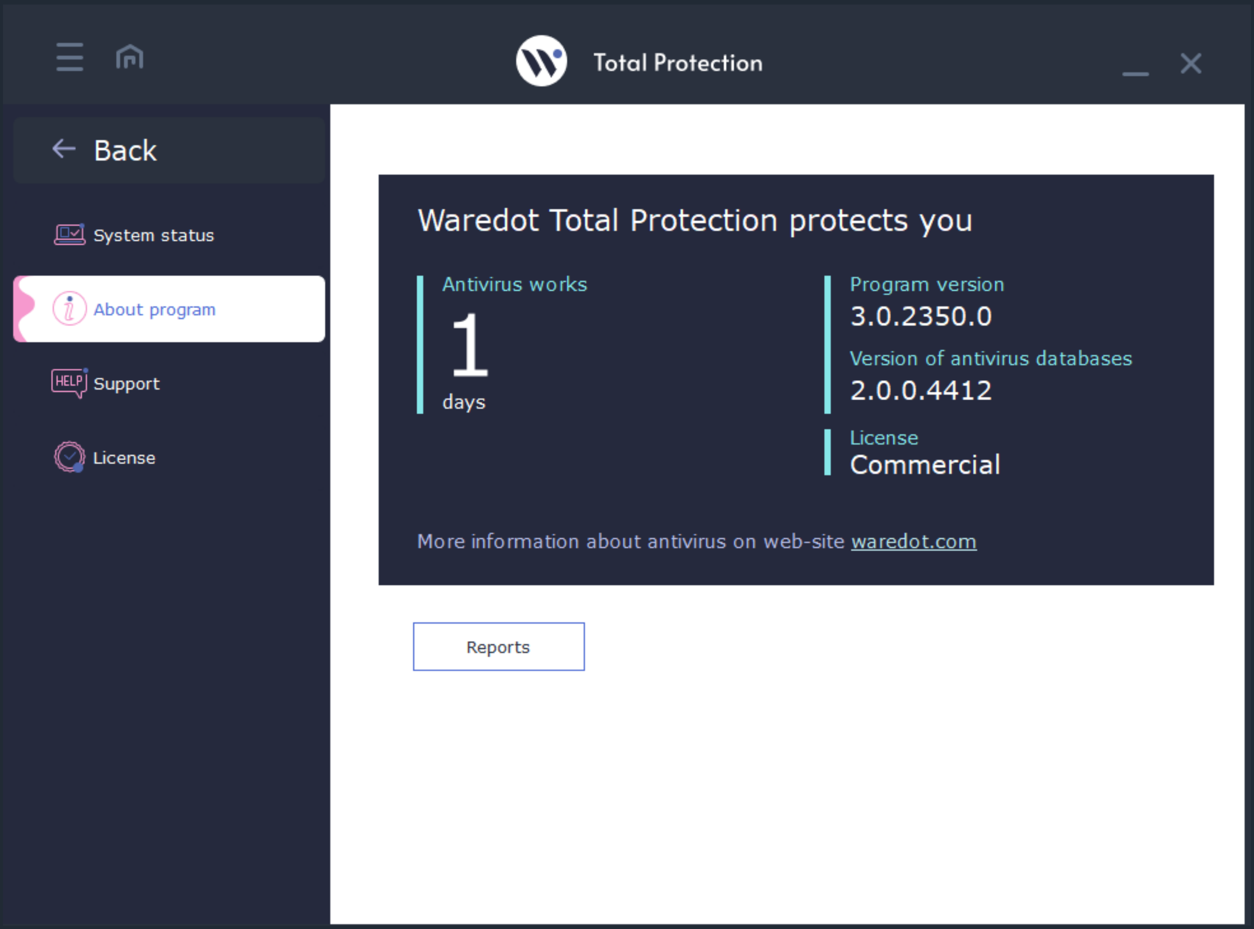
License owner
test

E-mail
test@tes.t

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



Waredot Total Protection protects you

Antivirus works
1
days

Program version
3.0.2350.0

Version of antivirus databases
2.0.0.4412

License
Commercial

More information about antivirus on web-site waredot.com

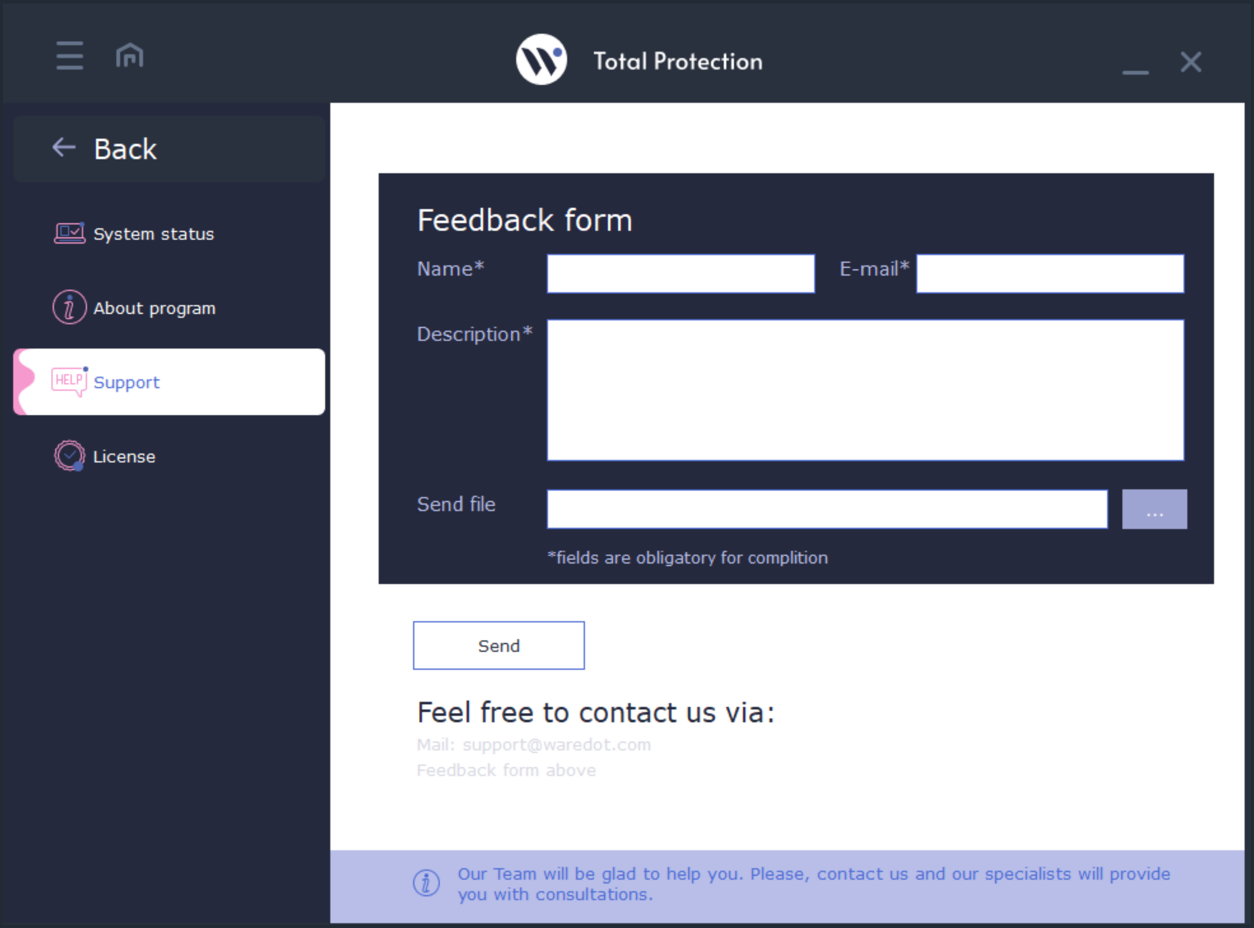
From the License tab user can go to Reports of Waredot Total Protection by clicking the button Reports.

Customer Support

If you have any questions about Waredot Total Protection 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.



Feedback form

Name*

E-mail*

Description*

Send file

*fields are obligatory for complition

Feel free to contact us via:

Mail: support@waredot.com

Feedback form above

Our Team will be glad to help you. Please, contact us and our specialists will provide you with consultations.