USER'S GUIDE

products

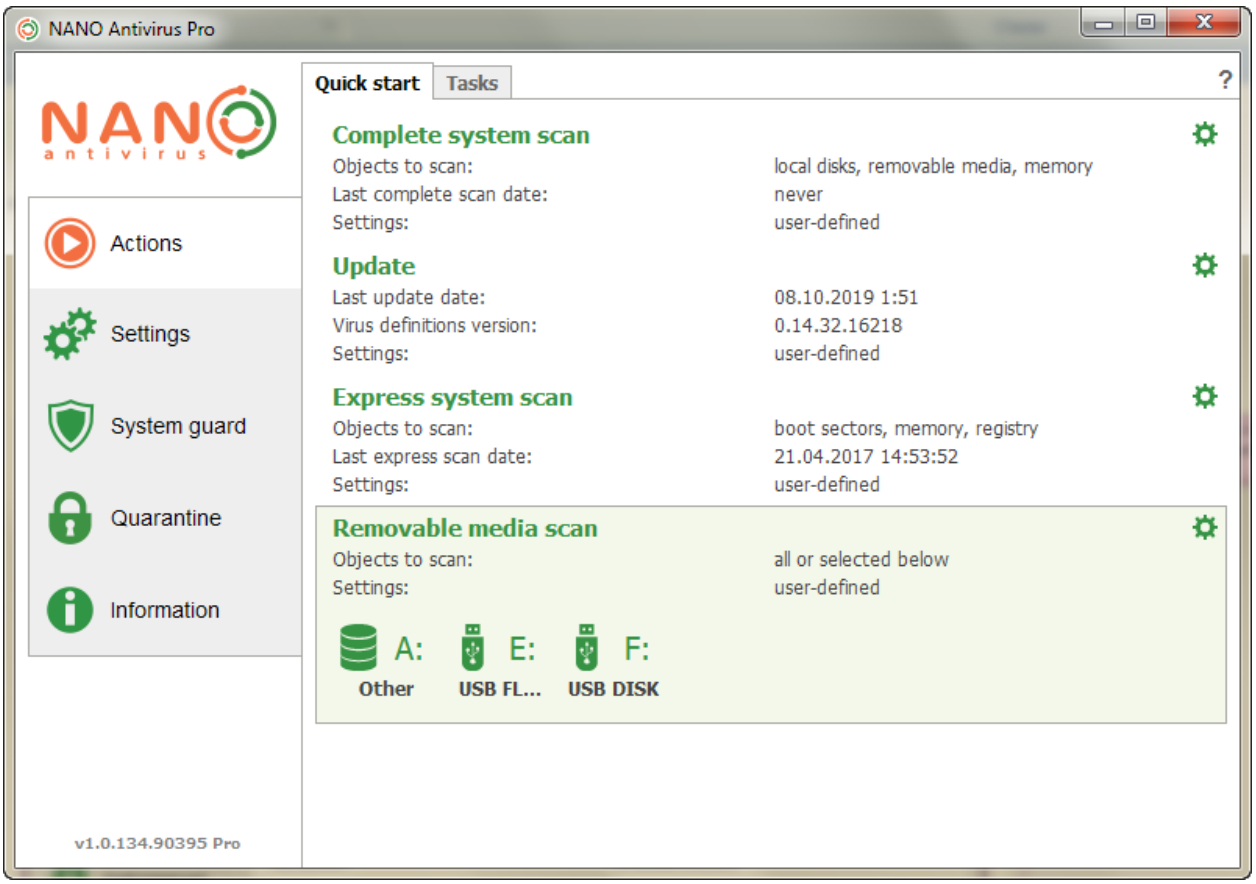
NANO Antivirus Pro and

NANO Antivirus

Table of contents

What is NANO Antivirus Pro?

NANO Antivirus Pro is a modern effective tool to protect your computer against all types of viruses, Trojans (binary, macro, script), worms and other malicious software.



When creating an antivirus complex, modern proprietary developments in the field of protection were used. This made it possible to create a product that works faster than most similar programs while ensuring high reliability in detecting any types of malicious programs. Deep emulation technology allows you to confidently find complex encrypted and polymorphic viruses that are not always reliably determined by other solutions. Implemented a powerful support for unpacking and working with archives, allowing to detect malicious objects processed by different packers (archivers), thereby providing protection against repeated epidemics caused by the same repacked objects.

Our product is easy to use. The mechanism for optimizing the use of system resources provides a comfortable user experience with other applications in the process of antivirus scanning. It is possible to use the game mode. Access to the most frequent tasks is conveniently organized. Having performed the minimum number of actions, you can perform a full scan of the PC, any removable media, run an express scan (i.e., scan only potentially dangerous areas), and update the components of the antivirus complex.

If necessary, you can create tasks that are performed periodically according to the schedule you set, which allows you to automate most of the protection activities.

NANO Antivirus Pro has a built-in system protection feature that is necessary to ensure the security of your computer in real time. When working on a computer with system protection enabled, all files that are accessed (by the user or by the system) are immediately scanned for malware.

The web traffic scanner instantly checks all files downloaded from the Internet for possible maliciousness, as well as the websites you visit for the presence of malicious code. This additionally protects your computer from infection.

It is possible to organize a trusted zone, which is a set of objects selected by the user and listed in a special list, the contents of which are not subject to verification during scanning. This allows you to exclude from the scan objects you are sure of, thereby optimizing, for example, the processing of large volumes of archives.

The presence of the quarantine function allows you to provide reliable isolation of identified suspicious objects. You can quickly send the files added to the quarantine to our technical support service for further analysis.

NANO Antivirus Pro has a number of functions built in for greater convenience of integrating the complex into the existing software infrastructure of the enterprise and its further maintenance. The ability to mirror and configure the update source will help automate the process of regularly updating the complex in corporate networks. There is the function of starting on behalf of another user, as well as password protection of the complex settings against changes. It is possible to automate antivirus actions when detecting various types of threats. A number of the most common operations can be performed using the command line.

The program has a user friendly interface. Several design themes are available, allowing you to vary the appearance of NANO Antivirus Pro. It is possible to use both the Russian language interface, and English one.

Frequently Asked Questions and Answers

The current version of frequently asked questions and answers is published on our website.

The help system of the antivirus program

You can access help in several ways:

From the context menu: Right-click on the icon in the taskbar notification area. In the context menu that opens, select "Help".

From any active window: Press the F1 key.

From the main antivirus windows: Click on the question mark in the upper right corner of the window.

From the scan window: Click the "Help" button in the bottom left of the window.

Installing antivirus software on your PC, obtaining and subsequent license renewal

Online installation

For online installation, download from our website and run the online installer file. Then follow the installation wizard instructions. Internet connection required.

Offline installation

In case your PC is not connected to the Internet, you can install NANO Antivirus Pro offline. You must first obtain a license file to install NANO Antivirus Pro on a computer that does not have an Internet connection. You can receive the license file by email via support. To do this, you need to send an email request to support@nanoav.ru to obtain a license for offline activation. The letter should indicate how many PCs you plan to use this license on, the name and email address to which the license will be issued, and attach (specify) the activation key.

Next, download the version for offline installation on our website. Unpack the archive containing the NANO Antivirus Pro offline installer files. Run the setup file.exe. Then follow the installation wizard instructions.

Obtaining and renewing a license

During the installation process, you will need to activate your license in order to further use NANO Antivirus Pro. To obtain and renew the license, you must provide your name and e-mail. This is necessary for further identification of your copy of NANO Antivirus

when providing technical support, etc. If necessary, enter the settings for the proxy server. For more information about network settings, see the Network section.

After filling in the required fields, click **Get license.**

To get a license online

If you do not have a license file, you can immediately activate the antivirus online. Internet connection required.

Activation key

If you have a key, enter it to activate the version of NANO Antivirus Pro, which corresponds to this key.

Professional trial

Select this option if you want to install NANO Antivirus Pro in a trial 30-day mode. The option is available only in NANO Antivirus Pro.

Import license from file

If you have a license file, import it to activate the version of NANO Antivirus Pro, which corresponds to this license file.

The validity period of a license depends on the type of license and may vary. After the license expires, antivirus updates will become unavailable. 7 days before the license expiration term, a notification will appear, reminding you to renew the license and offering various options for further action.

Dynamic licenses

In NANO Antivirus Pro we use a fundamentally new - flexible and convenient type of licensing. Now you do not need to decide in advance how many devices need a license now or will be needed in the future. We provide sets of days of protection that you use at your discretion, distributing them to the desired number of devices. Moreover, when installing on an additional device, you get additional bonus days of protection!

Actual information about the bonus system can be found on our website.

Work with antivirus

Check the presence of malware

The antivirus provides the ability to carry out various types of scans. Below are listed the available types of verification and the procedure for their execution is described.

Complete system scan

The complete system scan process scans all areas, processes, files, and folders of your PC. It is recommended to run a complete system scan after the first installation of the antivirus. It is also recommended to carry out a complete system scan after each cured active infection. A complete system scan may take a long time.

Express system scan

With the express system scan, only the most vulnerable areas of the PC are scanned. We recommend scanning before starting work on a PC, as well as after each update of the antivirus. In addition, it is recommended to make a complete system scan if there are signs of the PC infection. You can enable automatic execution of the express scan when starting the antivirus in the **Settings** menu, the **Common** tab.

Removable media scanning

The scan process scan removable media connected to your PC. To avoid infection, it is recommended to scan all removable media before working with them. The scan request appears by default when removable media is connected. You can configure the automatic scan of removable media in the **Settings** menu, the **Common** tab.

Selective scan

When conducting a selective scan, you choose the objects (folders, files) and areas that will be scanned by the antivirus. You can set additional settings that will be scanned. Please note that the number of available settings and their appearance depend on the currently installed theme. You can also use the Windows Explorer context menu to scan a single file or folder. Right-click the folder or file you want to scan and select **Scan with NANO Antivirus/NANO Antivirus Pro** from the context menu that appears.

Below are the areas of the PC that can be selected for selective scan.

Files and folders

When this scan area is selected, only the files and folders you have selected will be scanned, located in the specified path on the user's computer or local network. This type of scan is useful for targeted scanning of specific files and folders.

Main memory

When you select this scan area, all of the computer's RAM, including all running processes and service data, is scanned. Checking this area is useful if you suspect a computer infection, which can result in the following symptoms: strange PC behavior, unstable operation, etc.

Boot sectors

When you select this scan area, the objects on the hard drives that are responsible for booting the computer are scanned. Scanning this area may be useful if you suspect that your computer has been infected with malware that runs before the operating system is loaded.

Desktop

When you select this scan area, all objects that are on the user's desktop, as well as programs that have shortcuts on the desktop will be scanned. Scan is useful if you use the desktop to save documents downloaded from the Internet, as well as if you find unknown shortcuts on your desktop that were previously missing.

Documents

The libraries will be scanned when this area is selected. This type of scan is useful for periodically checking your current documents.

Creating a scan task

You can also create a scan task with your own settings. **Attention!** The number of tasks to be created may be limited depending on your license type! On the **Tasks** tab of the **Actions** menu item, point the cursor on the **Scan Tasks** item. Select **Add scan task with preferences**. Next, apply the necessary settings to the new task.

Scan settings

You can customize the scan settings in most skin themes. Settings for the basic scan tasks, namely for a full scan, express scan, and removable media scan, are available on the **Quick Start** tab of the **Actions** menu item. To configure a custom task, select the desired task in the task tree, then select the **Configure selected scan task** command. The setting of the following task parameters is available:

Selection of scan areas

The following settings are responsible for the ability to control this option:

System task

Attention! The availability of this option depends on the type of your license!

If this option is selected, the scan task will be performed for all users of this PC. This option is useful if several users work on the same PC under different accounts.

Objects to scan

Add the files, folders, and scan areas you want to scan for this task.

File filtering while scanning

The antivirus automatically scans all files, regardless of their extension, type or size. Sometimes it is useful to specify specific parameters of the files you want to scan. This can significantly speed up scanning, but at the same time can reduce the detection of malicious files. You must consider this fact when applying filtering.

The following settings are responsible for the ability to control this option:

Scan all potentially dangerous extensions

The default list of extensions is used to ensure optimal protection mode.

Scan files with following extensions

It allows you to specify a list of extensions that will be used during scanning. You can either add or delete the desired values.

Scan NTFS streams

It allows you to scan the service attributes of files that are available on some file systems. Sometimes such attributes are used by malware for its own purposes.

Do not scan objects with size more than N MB

It allows you to set the size of the scanned object. In some cases, this is useful to speed up the scanning. It should be borne in mind that the malicious program may be located in a large file.

Nesting level

Allows you to set limits on the depth of archives scanning. Decreasing the scan depth can speed up the scanning process. However, it should be borne in mind that the malware can be at a fairly deep level of nesting.

The scan mode of protected objects

It allows you to specify the actions of the antivirus when scanning the object protected by a password. As a rule, it can be password-protected archives. In this case, the antivirus can use a pre-defined in task settings password, or skip the object.

Miscellaneous settings

The list of miscellaneous settings may vary depending on the currently installed theme.

Optimize processor usage

This option is useful if the antivirus is installed on a PC with a multi-core processor. In this case, processor optimization enables scanning by evenly distributing the load, which speeds up the scanning process.

Do not show window when the task is started

If this option is enabled, the scan window will not be displayed when the task starts. This option is useful if you want the task to run in the background without distracting from work on the PC.

Do not show error messages

This option allows you to disable the display of information about possible errors that occurred during the scanning of some files in the scan window.

Show window when the task is finished

If this option is enabled, the scan window will be activated after the task is completed. This option is useful if you want to view detailed information about the scan results when the scan is complete.

Show messages about password-protected archives

This option activates the output of information about detected password-protected archives to the scan window.

Forbid task start when on battery

This option is for laptops. It is useful for saving battery power if the laptop is not connected to the network at the time of the task start.

Antivirus actions when dangerous objects are detected

You can configure actions to be performed by the antivirus when malicious, suspicious or potentially dangerous objects are detected. Select the desired action for each object type to do this. You can also enable the option to save the original backup for all modified (deleted or disinfected) files in a special secure storage. This can be useful, for example, in the case of a false reaction on a file.

Scheduled run

You can set a convenient schedule for you to execute the scan task.

Scanning process

After running a scan for malicious software, the scan process window appears on the screen. The window contains general information about the scan task, information about objects detected during the scan process, as well as process controls that allow you to put the scan into the background mode, pause or stop it. The scanning process dynamically displays a list of objects detected during the scanning process. In the scan settings, you can disable the display of the names of objects on which errors occurred, as well as password-protected archives. In this case, only malicious, suspicious and potentially dangerous objects will be displayed in the list. When you click on the object name with the right mouse button, a context menu is displayed, giving you the opportunity to perform a series of actions on the detected object, such as cure, quarantine, etc.

Antivirus update

You need to regularly update the virus database to ensure proper protection of your PC. By default, after antivirus installation, an automatic update task is created with settings that are optimal for most users. You can also optionally update the antivirus manually. Manual update is available from the **Actions** menu of the main menu, **Quick Start** tab. Click on the **Update** field. The current update settings will be applied.

You can also create an update task with your own settings. **Attention!** The number of tasks you create may be limited depending on the type of your license!

On the **Tasks** tab of the **Actions** menu item, point the cursor on the “Update tasks” item. Choose **Add new update task with user settings**. Next, apply the necessary settings to the new task. Similarly, you can change the default update task settings.

In most skin themes, you can customize the update settings. For the main task of updating, settings are available on the “Quick Start” tab of the **Actions** menu item. To configure a custom task, select the desired task in the task tree, then select the command **Configure selected update task**. The setting of the following task parameters is available:

Task settings

System task

Attention! The availability of this option depends on the type of your license!

> If you select this option, the update task will be performed for all users of this PC. This option is useful if several users work on the same PC under different accounts.

Show window when the task is finished

If this option is enabled, the update window will be activated after the task is finished. This option is useful if you want to view detailed information about the upgrade process after the upgrade is complete.

Update source

This option allows you to configure the source that will be used to receive antivirus updates.

Attention! The availability of these options depends on the type of your license! The following sources are available:

Official update servers

Using the official update server is convenient if the PC has a stable unlimited Internet access.

Folder

This option is useful if Internet access is limited, unstable, or unavailable. In this case, the update files can be received on another PC connected to the Internet and transferred to the designated folder.

Server

The option is intended primarily for use in corporate networks. Updating from a custom server allows you to optimize the use of resources when updating a large number of PCs.

Authorization

If authorization is required to access the user server, enter the username and password that will be used when accessing updates.

Mirroring

This option is useful for setting up the update process in the corporate network. When this option is enabled, the update files will be automatically saved in the specified folder, which can be installed as an update source.

Scheduled run

You can set a convenient schedule for you, according to which the update will be performed.

Update automatically

It is recommended to install the "Automatic" mode, offering the optimal update rate.

Tasks history

Antivirus can save detailed information about scan tasks. To manage the task history, select the **Tasks** tab of the **Actions** item of the main menu. You can view the completed task, perform it again or delete it from the list.

Active tasks

To manage tasks currently running, select the **Tasks** tab of the **Actions** item of the main menu. Next, use the **Active Tasks** item. In addition, active tasks are available from the context menu in the notification area.

Advanced antivirus settings

Attention! The availability of these options depends on the type of your license!

Settings protection

You can protect your antivirus settings with a password. This option is useful when it is necessary to prevent unauthorized users from changing important settings. When activating the mode, without entering the password, it will be impossible to disable system protection, change scan and update settings, delete or modify user tasks, etc.

Activate game mode automatically

When this option is enabled, the game mode will be activated when launching full-window applications. In game mode, notifications are not displayed on the screen, and no sound alerts are played.

Do not run scheduled updates

When this option is enabled, if the game mode is active, the scheduled update tasks will not run until the game mode is turned off.

Participate in the experience improvement program

We would appreciate your participation in the quality improvement program. In the case of activating this option, we will receive anonymous, not bound to a specific user error information, etc., which will help us troubleshoot and improve our product.

Interface

Antivirus has several themes available that differ in appearance and feature set. In addition, you can select the interface language.

Information messages

You can specify the location of the notifications displayed on the PC screen that do not require user action. In addition, you can choose the appropriate mode for displaying notifications. It is possible to set the mode in which all or only important notifications are displayed – about an error that occurred during the update, as well as about the completion of the scan task in which malware was detected.

Notify me when virus definitions are out of date

Timely updating of virus databases is necessary to ensure a proper level of protection. Turn on the notification in order not to miss the moment when the databases will need to be updated.

Sound notifications

You can enable or disable the sound notification of antivirus events. You can choose to be notified of all events, or only when malicious, potentially dangerous, or suspicious software is detected.

Network

If you are connected to the Internet through a proxy server, add the necessary parameters to the network settings. These settings will be used for all antivirus actions that involve working with the network, namely: updating the antivirus, sending suspicious files for further analysis, obtaining a license, etc. You can also set the maximum size of suspicious files sent from the quarantine folder for additional research.

Permanent system guard

The antivirus has a built-in function of permanent protection of the system, which is responsible for the security of your computer in real time. Comprehensive system protection is provided by file and web protection. When working on a computer with file protection enabled, all files that are accessed by the user or the system are immediately scanned for malicious code. Web protection ensures safe operation of the Internet, initiating a scan for the presence of malicious content of all downloaded files, as well as visited sites. If a threat is detected, an alert immediately appears. You can enable or disable security features in the corresponding tabs of the main window. We do not recommend disabling system protection, as this will increase the risk of infection of your PC. A number of settings are available to protect the system:

Deny access to infected files automatically

If this option is enabled, all detected malicious files will be automatically blocked immediately.

Monitor HTTP traffic

Disable this option if you do not want the web protection to check the web pages you visit.

Monitor e-mail traffic

Disable this option if you do not want your email traffic to be checked.

Monitor FTP traffic (passive mode)

Disable this option if you do not want FTP traffic to be checked.

Block FTP active mode

Enable the option to block active FTP traffic.

Event log

Information about threats detected using file and web protection is displayed in the system protection log. Select the appropriate item from the drop-down menu to view information related to the event source you are interested in.

Notification area icon and context menu

After installing the antivirus, a program icon appears in the notification area. The icon appearance may vary depending on the antivirus mode and the installed theme. The current status of the antivirus is highlighted by the icon animation in order to visually inform the user about the tasks performed or to warn about problems. Right-clicking on the antivirus icon in the task bar notification area opens the context menu. The menu allows you to get quick access to a number of antivirus functions:

Open NANO Antivirus / NANOAntivirus Pro

The main antivirus window will open.

Update

The default update task will be performed.

Disable system guard

The system protection will be turned off completely. To disable file protection and web protection separately, go to the main antivirus window, the system guard menu item.

Enable system guard

The system protection will be turned off completely. To disable file protection and web protection separately, go to the main antivirus window, the system guard menu item.

Enable / Disable Game Mode

A special mode that restricts the actions of NANO Antivirus Pro while running full-screen applications for greater user convenience will be enabled/disabled.

Objects to scan

Quick access to scan any disk in the system.

Scan tasks

Quick access to the start of any custom scan task.

Active tasks

Quick access to manage current scan and update tasks.

Help

Switch to the antivirus help system.

Exit

Shut down the visual part of the antivirus. At the same time, after the completion of the visual part, the antivirus continues to protect your PC, scheduled tasks will be performed at the scheduled time. To restart, use the menu item: “Start-> All Programs-> NANO Antivirus / NANOANtivirus Pro”.

Trusted zone

A trusted zone is a set of objects selected by the user and listed in a special list, the contents of which are not subject to verification during scanning. There are various reasons for placing an object in a trusted zone. For example, a large volume archive is stored in the scanned folder, and you are sure that it is safe. Such objects can be excluded from the scan to speed up the work of the antivirus. There may also be a case when you are aware of the risk, use a conditionally dangerous program, and antivirus perceives it as malicious software. Putting such an object in the trusted zone will help solve the problem. To form a trusted zone, go to the appropriate window. You can add, delete and edit rules for files and folders, applications and web addresses.

Quarantine

Quarantine is a storage of potentially dangerous objects detected during scanning, added manually for further analysis, or stored in the form of backups with the possibility of subsequent restoring. Additional actions on files are available in quarantine using the context menu, which is invoked by right-clicking on the file lists.

A number of settings are available for quarantine:

Actions if suspicious object is found in quarantine

You can select actions to be performed by the antivirus for suspicious objects in quarantine at the time they are added or as a result of rescanning.

Ask user

> In the event that the object in quarantine is found to be suspicious, a notification will appear with a request for further action.

Send to Virus Lab for analysis

> The suspicious object will be sent to the virus lab for further analysis. Internet connection required.

Do not send

> The suspicious object will not be sent for analysis to the virus lab, the request for action on the object will no longer be displayed. You can further send this suspicious object to the virus lab yourself, by going to the Quarantine menu and using the context menu.

Other settings

Rescan quarantine after update

> Enable this option if you want the antivirus to automatically rescan the entire quarantined files using the latest virus database.

Automatically restore clean objects from quarantine

> If according to the results of rescanning with the updated virus database, the object is declared clean, it will be automatically removed from quarantine and restored to its original location.

Automatically cure infected objects in quarantine

> If according to the results of rescanning with the updated virus database, the object is recognized as infected, its treatment will be automatically launched.

If a malicious file is added to quarantine, a request will be displayed for further actions with the file.

Work in the command line

NANO Antivirus Pro provides the ability to run some operations from the command line. In order to get basic help on the available types of operations, type in the command line:

nanoavcl --help. To get detailed information on all keys available for a specific operation of interest to you, type in the command line: nanoavcl %operation name% --help.

Notifications displayed by antivirus and work with them

Various notifications may appear during the operation of the antivirus. There are two types of notifications - informational and interactive.

Informational notifications inform, respectively, some information about the work process of the antivirus and do not require any user response. Such notifications automatically disappear from the screen after a while, you can also close them by right-clicking in the notification area.

Interactive notifications offer the user to perform certain actions to continue the work of the program.

Work with interactive notifications

Interactive notifications can appear when a threat is detected during the scan, during the operation of the permanent protection of the system, if it is necessary to update the antivirus, restart the antivirus and in a number of other situations when the user needs to choose further action to continue working.

The following actions are available for threat notifications:

Cure

An attempt to cure the detected malicious file will be made. The original backup copy of the file will be stored in a secure quarantine store with the possibility of subsequent restoring if necessary.

Cure all

Each malicious file detected in the current scan will be cured. The original backup copies of the files will be stored in a secure quarantine store with the possibility of subsequent restoring if necessary.

Remove

The detected malicious file will be deleted. The original backup copy of the file will be stored in a secure quarantine store, which can be restored if necessary.

Remove all

All malicious files detected by the current scan will be deleted. The original backup copies of the files will be stored in a secure quarantine store with the possibility of subsequent restoring if necessary.

Deny access

The malicious file accessed by the system will be blocked one-time for this access.

Deny access all objects

The malicious file accessed by the system will be blocked for this and further accesses. The ban will be valid until the antivirus is restarted. The settings for actions on infected files detected using system protection will be changed to “Deny access”.

Postpone

The malicious file detected during the scan will be skipped without processing. You can later apply the necessary actions to it by using the context menu in the scan window.

Postpone all

All malicious files detected during the scan will be skipped without processing. You can later apply the necessary actions to the detected files using the context menu in the scan window.

Allow access

One-time access to the detected malicious file will be allowed.

Add to trusted zone

This file will be added to the trusted zone.

Mark as false positive

If you are sure of the security of the file detected by the antivirus as malicious, mark it as a false positive, send it to us for analysis of the situation.

Isolate

The detected suspicious file will be moved to quarantine.

Isolate all

All suspicious files detected during the current scan will be moved to quarantine.

When you connect the removable media to your PC, you will be prompted for further action if you have selected the appropriate setting in the General settings. Select the action you want to apply to the removable media.

Always perform selected action

If you select this option, the applied action will be performed each time the removable media is connected.

Antivirus removal

To remove antivirus from a computer, select the Uninstall NANO Antivirus / NANOAntivirus Pro command (Start menu> All programs> NANO Antivirus / NANO Antivirus Pro). Then follow the instructions of the uninstaller.

Technical support

Our technical support specialists are always ready to help. If you have any questions, please contact us in a convenient way:

- Through the system of sending messages on our website.
- Via e-mail support@nanoav.ru.
- Via Skype “nanoav.support” (text chat only).
- You can also ask a question on our forum (registration is required to post messages on the forum).

Attention! The number of channels available for communication with technical support depends on the type of your license!

In some cases, when antivirus problems occur, technical support needs more information to analyze and solve the problem.

To collect and send logs that contain the necessary information, select the **Report a problem to Support Service** command (Start menu>All Programs>NANO Antivirus/NANO Antivirus Pro). This command will start the NANO Reporter utility.

Please describe your problem in detail in the appropriate field. This will help us understand the causes of problems.

Be sure to include your contact details. After analyzing the logs you sent, we will contact you and explain how to fix the problem.

You can choose exactly what information you want to send us. If you do not wish to send any information, uncheck the appropriate boxes. However, remember that the more complete the information we receive, the greater the likelihood that the problem will be quickly detected and fixed.

You can send us logs directly using the option **Send to technical support**, or by e-mail. Select **Save to disk** and attach the resulting archive to the letter to send logs by e-mail. If you have configured an email client, use the item **Send by mail**.

Each technical support request is assigned a number that you can use to track the process of resolving the problem that the request was created about.

System requirements

To use NANO Antivirus and NANO Antivirus Pro, your computer must meet the following system requirements:

*Minimum requirements **

- Operating system: Windows 7 and higher.
- CPU: 2 GHz or faster with SSE2 support.
- RAM: 2 GB or more.
- Disk space: at least 2 GB of free space on the system drive.
- Internet connection*.

Recommended Requirements

- Operating system: Windows 10 / Windows Server 2016 and higher.
- CPU: at least 3 GHz or faster with SSE2 support.
- RAM: 4 GB or more.
- Disk space: at least 2 GB of free space on the system drive.
- Internet connection.

Supported operating system

- Windows 10 (32-bit and 64-bit).
- Windows 8 / 8.1 (32-bit and 64-bit).
- Windows 7 (32-bit and 64-bit).
- Windows Server 2008 R2 and higher (32-bit and 64-bit).

*** Note:**

If your PC does not meet the specified minimum requirements, we do not guarantee the correct operation of NANO Antivirus / NANO Antivirus Pro.

An internet connection is required for:

- trial version activation,
- the use of dynamic licenses,
- the program update. It is possible to update NANO Antivirus Pro without connecting to the Internet using the Offline Update functionality.

Attention: Administrator rights are required to install the program.