Dr.WEB

LiveDisk

User Manual

Trademarks

Disclaimer

In no event shall Doctor Web and its resellers or distributors be liable for errors or omissions, or any loss of profit or any other damage caused or alleged to be caused directly or indirectly by this document, the use of or inability to use information contained in this document.

Dr.Web LiveDisk
Version 9.0
User Manual
1/27/2020

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125040

Website: https://www.drweb.com/

Phone: +7 (495) 789-45-87

Refer to the official website for regional and international office information.

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions which provide efficient protection from malicious software and spam.

Doctor Web customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards.

State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

We thank all our customers for their support and devotion to the Dr.Web products!

Table of Contents

1. About This Document

About Manual

Thank you for choosing Dr.Web LiveDisk free anti-virus solution. It will help you to restore an operating system when high virus activity has rendered it inoperable.

This manual is intended to help to use Dr.Web LiveDisk 9.0. Make sure you have the latest version of the manual. The manual is constantly updated and the current version can always be found at the official web site of Doctor Web company at https://download.drweb.com/doc/.

Before reading the document, please view the conventions.

Conventions

The following symbols and text conventions are used in this guide:

Convention	Comment
⚠	Warning about possible errors or important notes to which you should pay special attention.
Anti-virus network	A new term or an accent on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
`C:\Windows\`	Names of files and folders, code examples.
Appendix A	Cross-references on the document chapters or internal hyperlinks to web pages.

2. General Description of Dr.Web LiveDisk

Dr.Web LiveDisk is an anti-virus solution which allows to restore an operating system when high virus activity has rendered it inoperable.

Dr.Web LiveDisk is a bootable media (optical disk or USB flash drive) with a Linux-based portable operating system and pre-installed software which performs anti-virus scans of the computer, neutralizes detected threats and allows the user to work with the registry and file system as well as browse webpages.

Dr.Web LiveDisk is delivered as a ready-to-use disk, or as an .iso image (in this case, you need to burn the image to a blank disk), or as an executable—the utility which is started in Windows environment to create a bootable media (USB flash drive).

To prevent such situations, do not disregard the need to protect the operating system with anti-virus software that employs the most advanced technologies.

Technologies and features implemented in products of Doctor Web company provide for reliable anti-virus protection of both large corporate networks and computers for home use. Doctor Web company anti-virus solutions have low system requirements and deliver fast performance and reliable protection against all types of malware. On the Doctor Web company official website https://products.drweb.com/, you can find up-to-date information on products for resident protection of computers and mobile devices against viruses, malicious programs, and spam.

System Requirements

Dr.Web LiveDisk can be installed and run on a computer which meets the following minimum requirements:

Parameter	Requirement
CPU	x86-64-compatible
Random access memory	Minimum 1 GB of RAM (2 GB or more is recommended)
Other	A video card, a monitor, a keyboard, and a mouse (preferably)

> ⚠ Dr.Web LiveDisk no longer supports x86 CPUs.

Moreover, depending on the type of the media that contains Dr.Web LiveDisk, either an optical disk drive or a USB port is required.

To create a boot copy of Dr.Web LiveDisk, you can use any FAT32 USB flash drive with enough free space (not less than 1 GB).

Creating Dr.Web LiveDisk Bootable Flash Drive

You can create an original copy of Dr.Web LiveDisk to boot it from a USB flash drive. To do this, use `drweb-livedisk-900-usb.exe`, which is a special tool for Windows OS. In this case, Dr.Web LiveDisk can be used as a portable operating system, customized for the needs of a particular user, to access data on any computer regardless of the installed operating systems and other software.

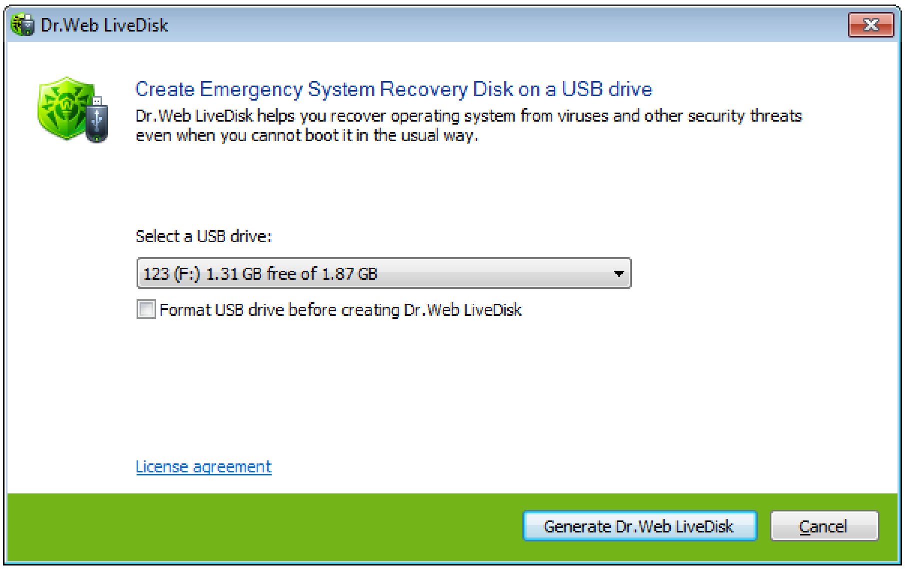
Note that when Dr.Web LiveDisk is loaded from a USB flash drive, it is still operating in RAM mode. Thus, no changes made to the system while Dr.Web LiveDisk is running are saved, as well as when CD/DVD media is used.

> ⚠ Despite the fact that `drweb-livedisk-900-usb.exe` does not change or delete drive's content, it is recommended to save the files of the flash drive you are going to use to another data carrier before starting the program.

All Dr.Web LiveDisk files are written to the `/boot` directory. The utility may change the configuration of the flash drive partitions, if necessary. The original configuration is saved to the `/boot/partition.backup` file. The `drweb-livedisk-900-usb.exe` program also creates a new MBR on the flash drive. The original master boot record is saved to the `/boot/mbr.backup` file.

To create a bootable flash drive

1. Connect a flash drive to the computer. It takes no longer than ten seconds to register the connection.
2. Run the executable file `drweb-livedisk-900-usb.exe`.
3. The program will automatically find all flash drives available in the system. Select the required drive.



Dr.Web LiveDisk

Create Emergency System Recovery Disk on a USB drive

Dr.Web LiveDisk helps you recover operating system from viruses and other security threats even when you cannot boot it in the usual way.

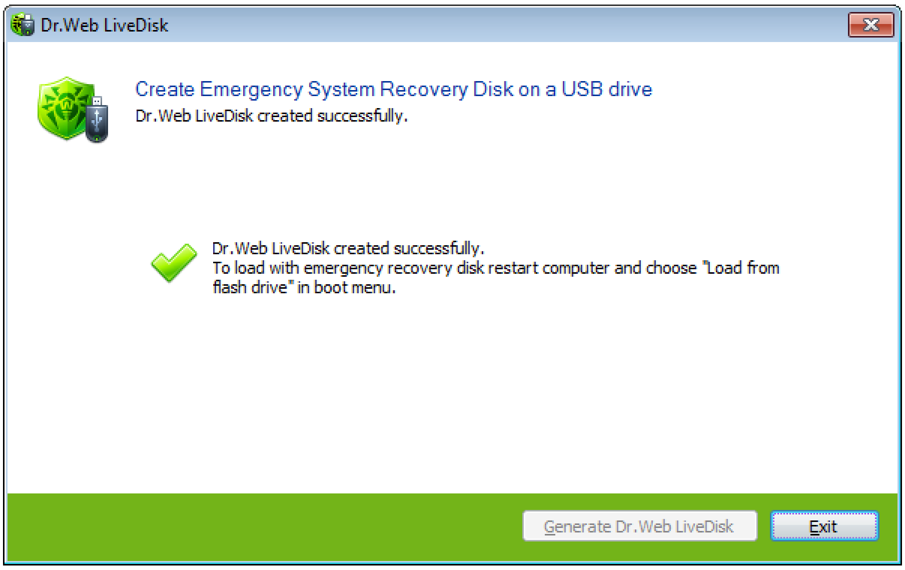
Select a USB drive:

123 (F:) 1.31 GB free of 1.87 GB

☐ Format USB drive before creating Dr.Web LiveDisk

License agreement

4. You can also format the selected drive (before the process starts, the program displays a warning message that all data stored on the drive will be deleted).
5. To view the License agreement, click the corresponding link in the window (the default browser opens and displays the text).
6. To create a bootable flash drive, click **Generate Dr.Web LiveDisk**.
7. File copying will start automatically.



Dr.Web LiveDisk

Create Emergency System Recovery Disk on a USB drive

Dr.Web LiveDisk created successfully.

Dr.Web LiveDisk created successfully.
To load with emergency recovery disk restart computer and choose "Load from flash drive" in boot menu.

8. After the process completes, click **Exit** to close the program.

Updating virus databases on your bootable flash drive

If it is necessary, you can save the up-to-date virus databases to your bootable flash drive without rewriting all the Dr.Web LiveDisk files. Complete the following steps:

1. Create a new directory `/zz.dir` in the `/casper` directory on your flash drive.
2. Create a new subdirectory hierarchy `/usr/local/lib/drweb` in the `/zz.dir` directory.
3. Copy the up-to-date virus databases to `/casper/zz.dir/usr/local/lib/drweb` directory.

After booting Dr.Web LiveDisk from a flash drive, you may download and install updates to the computer by the Dr.Web Updater component.

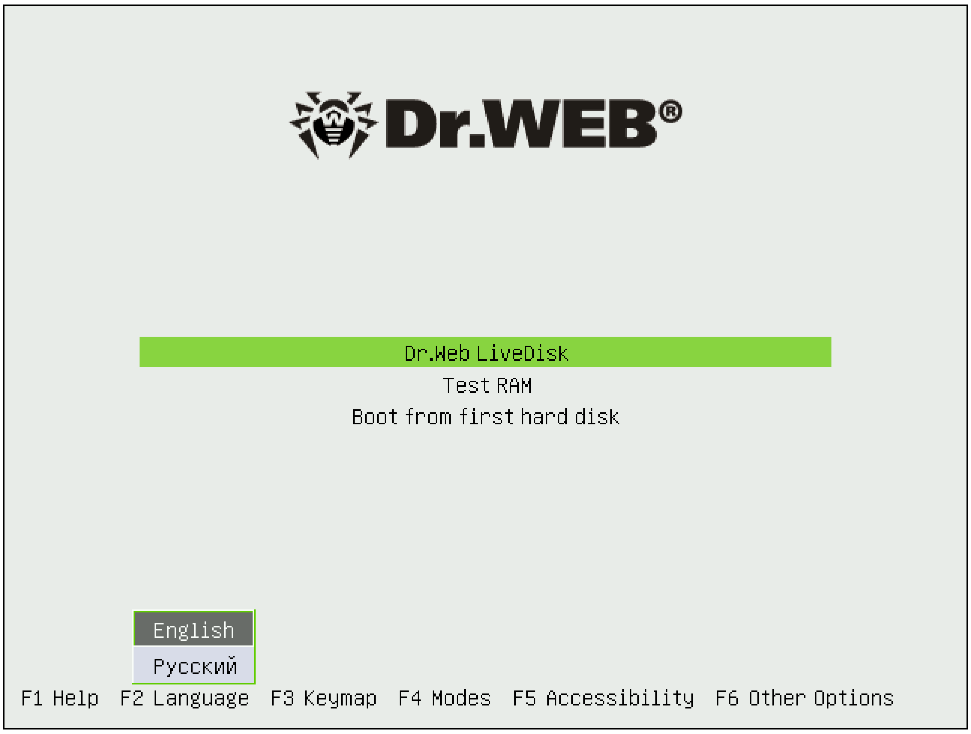
Starting Dr.Web LiveDisk

Make sure that your computer is set to start from the media with Dr.Web LiveDisk. Insert this media into the drive or USB port and turn on your computer (or restart the system if it is running).

By default, Dr.Web LiveDisk uses English language for the interface. If necessary, you can change it to Russian. For that, press any key once the Doctor Web company logo appears at the bottom of your screen (on a light background).

Once a key is pressed, the boot menu appears on the screen with the **F2 Language** section open.

To select the Russian language item, use the arrow keys ↓ and ↑ on your keyboard. Press ENTER. The interface language will change to Russian.



Test the memory if your computer is extremely unstable and restarts at random Using the arrow keys ↓ and ↑ on your keyboard, select the **Test RAM** menu item. The Memtest86+ program will start. The program has a feature to list bad RAM regions in the format expected by the BadRAM patch for the Linux kernel. The program supports dual-core and quad-core processors as well as a large number of various motherboard chipsets.

If you want to start your operating system from the hard drive without running Dr.Web LiveDisk, select **Boot from first hard disk.**

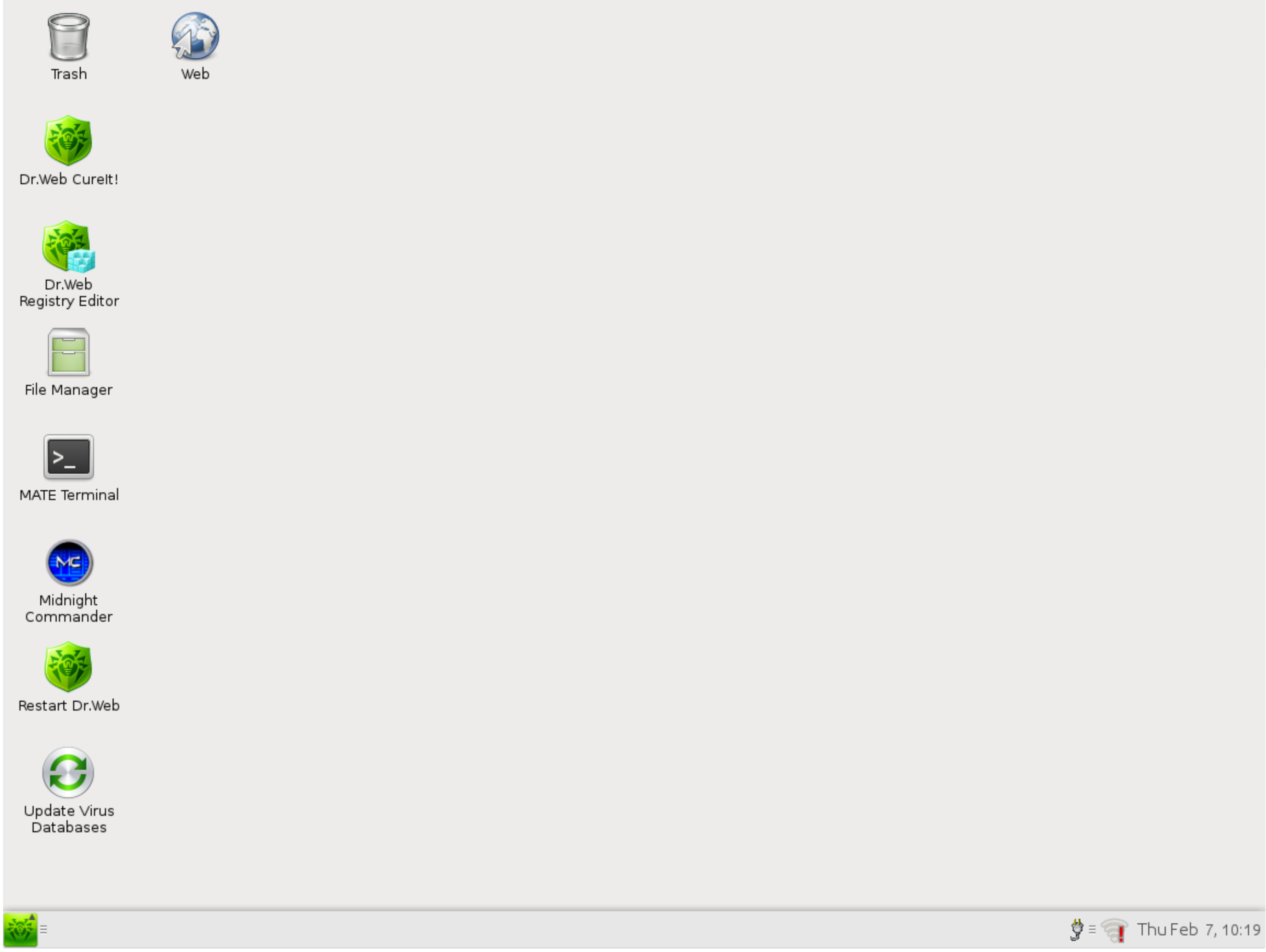
To start Dr.Web LiveDisk by using the arrow keys ↓ and ↑ on the keyboard, select the **Dr.Web LiveDisk** item menu and press ENTER.

The operating system will start to load. After that, Dr.Web CureIt! starts and displays the **License and updates** window. To go to the page where you can select a scanning mode, click **Continue**. If you want to start an anti-virus scan later, click **Exit** and you will see the desktop on the screen.

Desktop

Dr.Web LiveDisk includes a graphic shell with a window-based interface. Once Dr.Web LiveDisk is started, it automatically runs the scanner Dr.Web CureIt!.

If you decide not to scan your system with Dr.Web CureIt! after Dr.Web LiveDisk startup and click **Exit** or if you finish working with the scanner, the standard desktop appears on the screen.



On the desktop, you can see icons of main programs included in Dr.Web LiveDisk and the **Restart Dr.Web** icon for restarting Dr.Web components.

The taskbar (horizontal bar at the bottom of the screen) displays buttons of programs that are currently open as well as the following items:

	—button which opens the system menu
⇅	—network connection icon (if a connection is established)
Thu Feb 7, 13:56	—clock showing system date and time

Dr.Web LiveDisk is supplied with the following main components:

- Program Dr.Web Registry Editor
- Anti-virus scanner Dr.Web CureIt!
- Program Dr.Web Updater

Other auxiliary programs:

- Console file manager Midnight Commander (with a text user interface)
- Web browser (GNOME Web lightweight browser for viewing web pages)
- MATE Terminal (terminal emulator—program for working in the console)
- File Manager (PCManFM file manager with graphical interface)

You can start these programs by double-clicking the appropriate icon on the desktop.

The system menu provides access to system settings and its administration. The menu allows to launch the browser, run standard and system utilities, and shut down Dr.Web LiveDisk.

Moreover, Dr.Web LiveDisk provides you with an option to configure network connection settings and system date and time.

Shutting Down Dr.Web LiveDisk

To shut down operation of Dr.Web LiveDisk, open the system menu by clicking the button on the taskbar and select the **Shutdown** item. The program will display the corresponding message and prompt you to eject the removable boot media. After that, press ENTER and the computer will turn off.

Deleting Dr.Web LiveDisk from USB Flash

After you finished working with Dr.Web LiveDisk, you can delete it with formatting of the flash drive. In this case, all other files on the USB flash drive will be deleted as well. Complete the following steps:

1. Connect a flash drive to the computer. It takes no longer than ten seconds to register the connection.
2. Open the **Start** menu and click **My Computer**.
3. Right-click on the flash drive disk and choose **Format** in the context menu. If necessary, you can also choose formatting parameters.
4. Click **Start** to run the formatting procedure.

3. Basic Functions

> ⚠ During its operation, Dr.Web LiveDisk uses a temporary RAM drive created when the system is starting. Thus, all changes in Dr.Web LiveDisk program settings will be lost after the computer restarts.

Dr.Web LiveDisk can perform the following tasks:

Scan the system for viruses

Dr.Web CureIt! scanner allows to scan the system for viruses or malware.

Updating virus databases is described in the Dr.Web Updater section.

Edit Windows registry

Dr.Web Registry Editor allows to view, edit, and restore windows registry keys. The program automatically detects Windows registry hives upon Dr.Web LiveDisk startup. After that, you can work with registry keys as with ordinary text files (view their contents and edit them when necessary).

> ⚠ It is strongly not recommended to delete, move or rename system predefined registry hives and keys as this may lead to damage of the structure. In this case, Windows will not be able to read the registry and the operating system or some of its components will become inoperable.

View, edit, create and delete files

Inbuilt file managers allow to work with files and directories and perform such operations as viewing, editing, creating and deleting files.

- Midnight Commander is a console file manager with a text user interface.
- File Manager PCManFM is a file manager with graphical interface.

Work with Linux management console

Terminal emulator (MATE Terminal) provides access to Linux management console.

Configure network settings

A special inbuilt Network Configuration program allows to change computer network settings. This can be necessary to establish Internet connection and update virus databases. It is recommended to change network settings only if the configuration created upon Dr.Web LiveDisk startup is not valid.

Browse the Internet

The inbuilt browser allows to browse the websites and view Help file on Dr.Web LiveDisk components.

Dr.Web CureIt! Scanner

Dr.Web CureIt! is the ideal solution for situations when installation of an anti-virus is impossible due to virus activity or some other reason. It does not require installation and is constantly supplemented with the latest virus databases to ensure its effectiveness against all virus threats and other malicious programs.

Dr.Web CureIt! allows you to run anti-virus scans of disk boot sectors and both separate files and objects enclosed within complex structures (archives, email files, installation packages). Dr.Web CureIt! uses all detection methods to detect viruses and other malicious software.

> ⚠ By default, Dr.Web CureIt! does not check archives. You can enable scanning of archived files in Dr.Web CureIt! settings.

Dr.Web CureIt! detects and neutralizes the following types of malicious programs:

- Worms
- Viruses
- Trojans
- Rootkits
- Spyware
- Dialer programs
- Adware
- Hacktools
- Joke programs
- Riskware

On detection of a malicious object Dr.Web CureIt! only informs you about the threat. Information on all infected or suspicious objects displays in the table where you can manually select a necessary action.

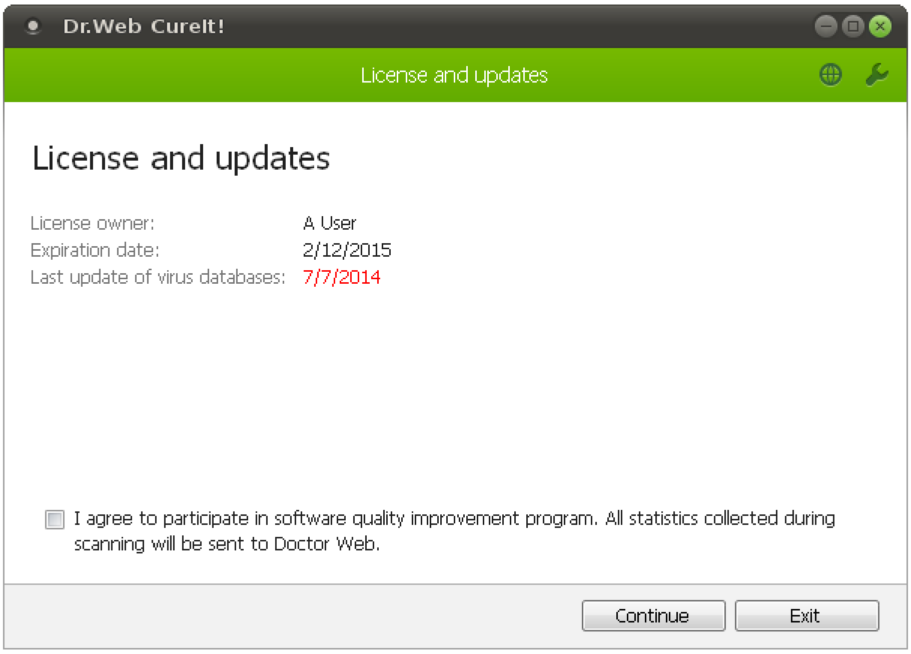
The default settings are optimal for most cases. However, if necessary, you can modify actions suggested upon threat detection by using Dr.Web CureIt! settings window. Please note that you can set a custom action for each detected threat after scanning is completed, but common reaction for a particular threat type should be configured beforehand.

> ⚠ While scanning your system, Dr.Web CureIt! can send general information on your computer and its state of information security to Doctor Web company servers. This statistics gathering is optional.

Startup, Restart and Shutdown

Starting Dr.Web CureIt!

After Dr.Web LiveDisk is started and the operating system is ready, the anti-virus scanner Dr.Web CureIt! automatically displays the **License and updates** window on the screen.



License and updates

License owner: A User
Expiration date: 2/12/2015
Last update of virus databases: 7/7/2014

□ I agree to participate in software quality improvement program. All statistics collected during scanning will be sent to Doctor Web.

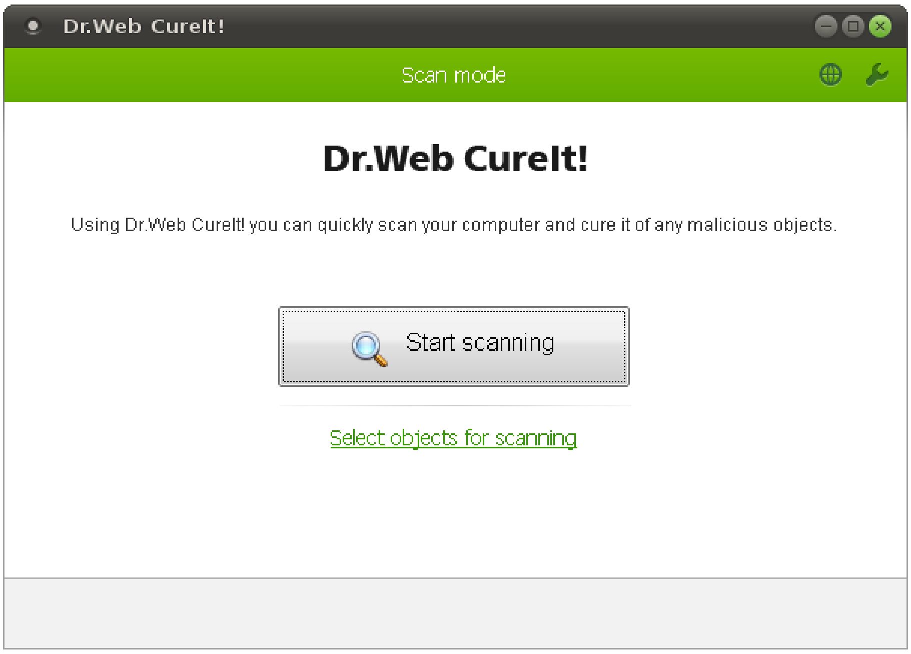
To run an anti-virus scan after Dr.Web LiveDisk startup or rescan you system, click the **Dr.Web CureIt!** icon on the desktop.

In the **License and updates** window, you can view information about the license owner, the license expiration date, and the date when the virus databases were last updated.

> If an update to virus databases is required, you can start Dr.Web Updater by clicking the **Update Virus Databases** icon on the desktop.

You can also read the conditions of statistics gathering and, if you want to participate in the improvement program, select the appropriate check box. In this case, statistics collected while scanning your system will be sent to Doctor Web company servers. By default, this option is disabled.

Click **Continue**. It opens a window, where you can select a scan mode.



Dr.Web CureIt!
Scan mode
Dr.Web CureIt!
Using Dr.Web CureIt! you can quickly scan your computer and cure it of any malicious objects.
Start scanning
Select objects for scanning

Restarting Dr.Web CureIt!

To reinitialize all Dr.Web components and restart the scanner, click the **Restart Dr.Web** icon on the desktop.

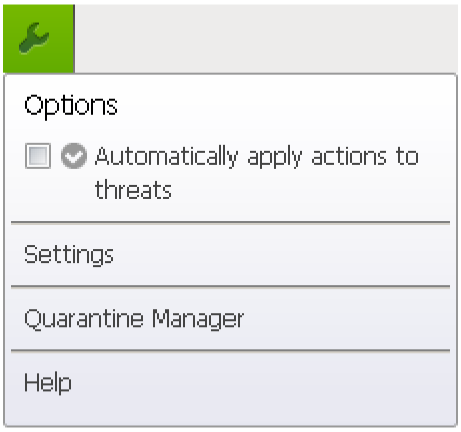
If you want to run a new anti-virus scan without restarting all anti-virus components, click the **Dr.Web CureIt!** icon on the desktop.

Exiting Dr.Web CureIt!

To finish working with Dr.Web CureIt!, close the program window.

General Settings

If you want to configure scan settings, click **Preferences** icon on the toolbar in the Dr.Web CureIt! window.



Options

□ Automatically apply actions to threats

Settings

Quarantine Manager

Help

Option	Description
Automatically apply actions to threats	By default, if known viruses or computer threats of other types are detected during scanning, Dr.Web CureIt! informs you about them. If enable this option, all detected threats will be neutralized automatically according to default settings or user-specified settings (if the user changed actions set by default). Select this check box to apply actions to detected threats automatically.
Settings	Click this item to open the window with Dr.Web CureIt! settings, where you can configure parameters of anti-virus scanning.
Quarantine Manager	Click this item to open the window of Quarantine manager, where you can view information on quarantined objects.
Help	Opens the Help file.

To change the interface language

Click the **Language** icon on the toolbar and then select the necessary option.

Express Scan

Dr.Web CureIt! provides a pre-installed template for anti-virus scanning of the most vulnerable objects of your operating system.

To run express scans

1. If Dr.Web CureIt! is not running, start the program.
2. In the **Scan mode** window, click **Start scanning**.
3. During scanning, Dr.Web CureIt! displays general information on its progress and lists detected threats.

   To manage scanning process, use the following options:

   - To pause scanning, click **Pause**.
   - To continue with the scanning, click **Resume**.
   - To stop scanning, click **Stop**.
4. Once scanning completes, the program displays detailed information on detected threats. Review scan results.
5. If scanning reveals viruses or other threats, you need to secure your system by neutralizing them. To apply predefined actions to all detected threats at once, click **Neutralize**. If necessary, you can select custom actions for particular threats.

Additional Tasks

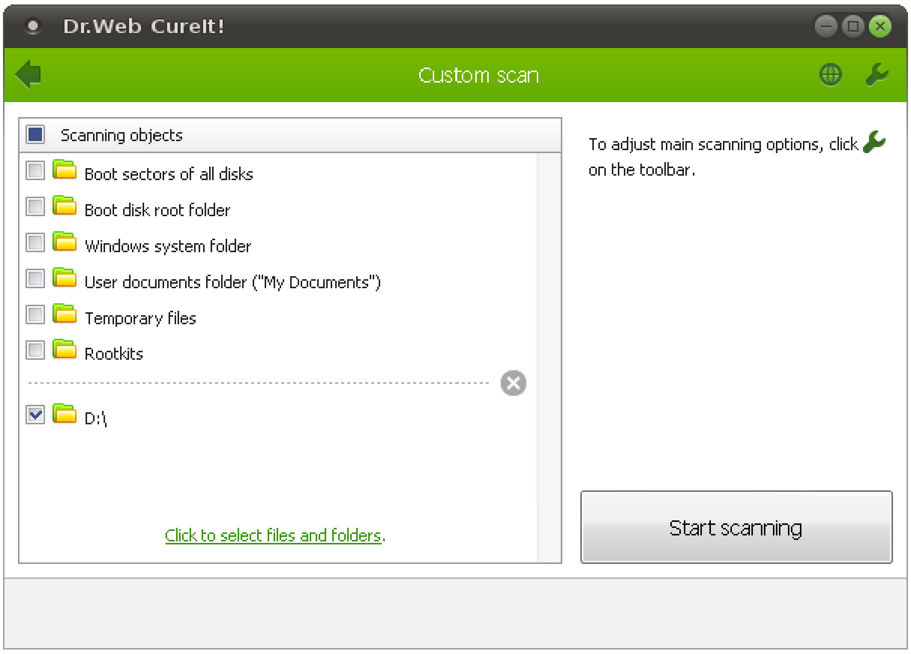
For most cases, express scanning is enough to cure your computer from infections and malicious programs. In rare cases, when subtle tuning is necessary, use the following options:

- Perform custom scans, which allows you to select particular operating system objects or files and directories to scan.
- Select custom actions to apply to detected threats.
- Configure settings of anti-virus scanning.

Custom Scan

Apart from the pre-installed scanning template that helps running an express scan of the most vulnerable objects, Dr.Web CureIt! also provides you with custom scan mode that allows configuring scanning in accordance with your particular needs.

To start scanning in custom mode, in the **Scan mode** window, click **Select objects for scanning**.



□ Scanning objects

□ Boot sectors of all disks
□ Boot disk root folder
□ Windows system folder
□ User documents folder ("My Documents")
□ Temporary files
□ Rootkits
☑ D:\

Click to select files and folders.

To adjust main scanning options, click on the toolbar.

This mode allows you to select objects for scanning:

- Boot sectors of all disks
- Root folders of all the boot disks found
- Windows system folder (of all detected operating systems)
- Folders "My Documents" of all computer users
- Temporary files
- Rootkits

To check all listed objects for viruses, select the **Scanning objects** check box in the table heading.

To check a particular file of folder, click the link at the bottom of the table, and then select objects for scanning in the **Browse** window.

If necessary, configure Dr.Web CureIt! settings before starting the scan.

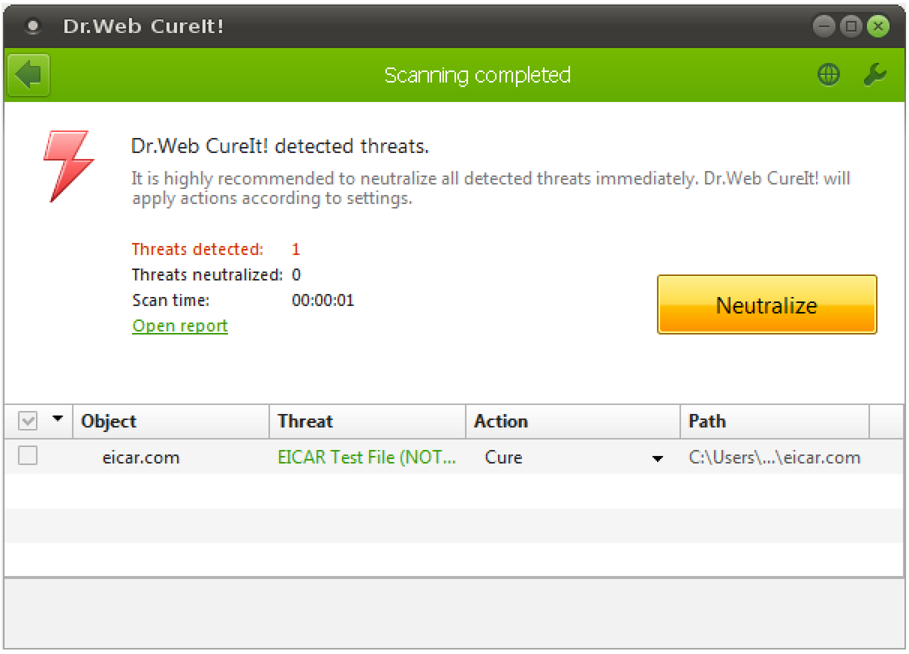
Click **Start scanning**.

Once scanning completes, the program displays detailed information on detected threats. Review scan results.

If scanning reveals viruses or other threats, you need to secure your system by neutralizing them. To apply predefined actions to all detected threats at once, click **Neutralize**. If necessary, you can select custom actions for particular threats.

Configuring Threat Neutralization

By default, if known viruses or computer threats of other types are detected during scanning, Dr.Web CureIt! informs you about them. You can neutralize all detected threats at once by clicking **Neutralize**. In this case Dr.Web CureIt! applies the most effective actions according to its configuration and threat type.



Dr.Web CureIt! detected threats.

It is highly recommended to neutralize all detected threats immediately. Dr.Web CureIt! will apply actions according to settings.

Threats detected: 1
Threats neutralized: 0
Scan time: 00:00:01
Open report

☑	Object	Threat	Action	Path
□	eicar.com	EICAR Test File (NOT...	Cure	C:\Users\...\eicar.com

By clicking **Neutralize** you apply actions to objects selected in the table. Dr.Web CureIt! selects all objects by default once scanning completes. When necessary, you can customize selection of objects to be neutralized by using check boxes next to object names or threat categories from the drop-down menu in the table header.

Moreover, you can apply an action individually to a particular threat. You can also attempt to *cure* an infected file and, if curing failed, neutralize the threat by *removing* the object.

To select an action

1. Where necessary, select a custom action from the drop-down list in the **Action** field. By default, Dr.Web CureIt! selects the action recommended for this type of threat.
2. Click **Neutralize**. Dr.Web CureIt! applies all selected actions at once.

There are the following limitations:

- For suspicious objects, curing is impossible.
- For objects which are not files (for example, boot sectors), moving and deletion is impossible.
- For files inside archives, installation packages, or attachments, no actions are possible.

Configuring Scanning

The default settings are optimal for most uses. Do not change them unnecessarily.

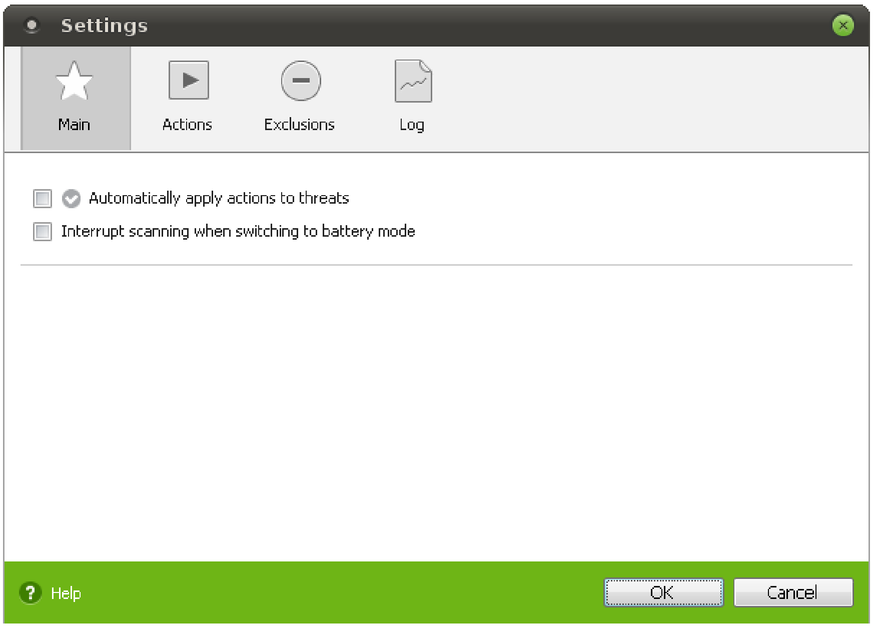
To configure Dr.Web CureIt!

1. If Dr.Web CureIt! is not running, start the program. This opens Dr.Web CureIt! window.
2. Click the 🔧 **Preferences** icon on the toolbar, and then select **Settings**. This opens the window which contains the following pages:
    - The Main page, where you can configure general parameters of Dr.Web CureIt! operation.
    - The Actions page, where you can configure reaction of the Dr.Web CureIt! on detection of infected or suspicious files and archives or other malicious objects.
    - The Exclusions page, where you can specify files and folders to be excluded from scanning.
    - The Log page, where you can set logging options for Dr.Web CureIt!.
3. To get information on options available on the page, click ? **Help**.
4. After editing, click **OK** to save the changes or **Cancel** to cancel them.

Changes in the settings of Dr.Web CureIt! are retained only in the current program session. New session resets program settings to their default values.

Main Page

On this page, you can set main parameters of Dr.Web CureIt! operation.



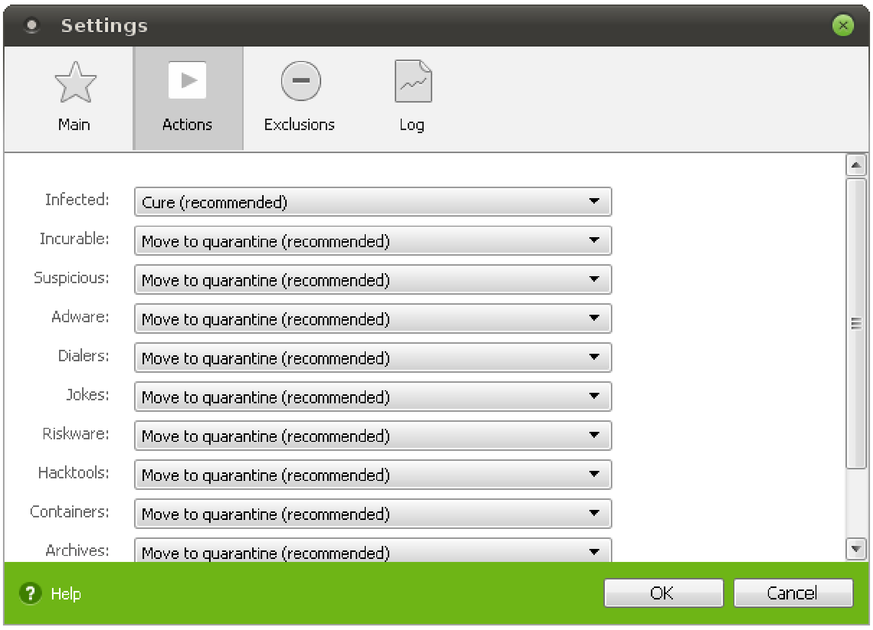
□ Automatically apply actions to threats

□ Interrupt scanning when switching to battery mode

You can instruct Dr.Web CureIt! to apply recommended actions to detected threats automatically, and select an option to interrupt scanning when on battery power.

Actions Page

By default, if known viruses or computer threats of other types are detected during scanning, Dr.Web CureIt! informs you about them. These actions are suggested in accordance with the settings on this page.



Infected: Cure (recommended)

Incurable: Move to quarantine (recommended)

Suspicious: Move to quarantine (recommended)

Adware: Move to quarantine (recommended)

Dialers: Move to quarantine (recommended)

Jokes: Move to quarantine (recommended)

Riskware: Move to quarantine (recommended)

Hacktools: Move to quarantine (recommended)

Containers: Move to quarantine (recommended)

Archives: Move to quarantine (recommended)

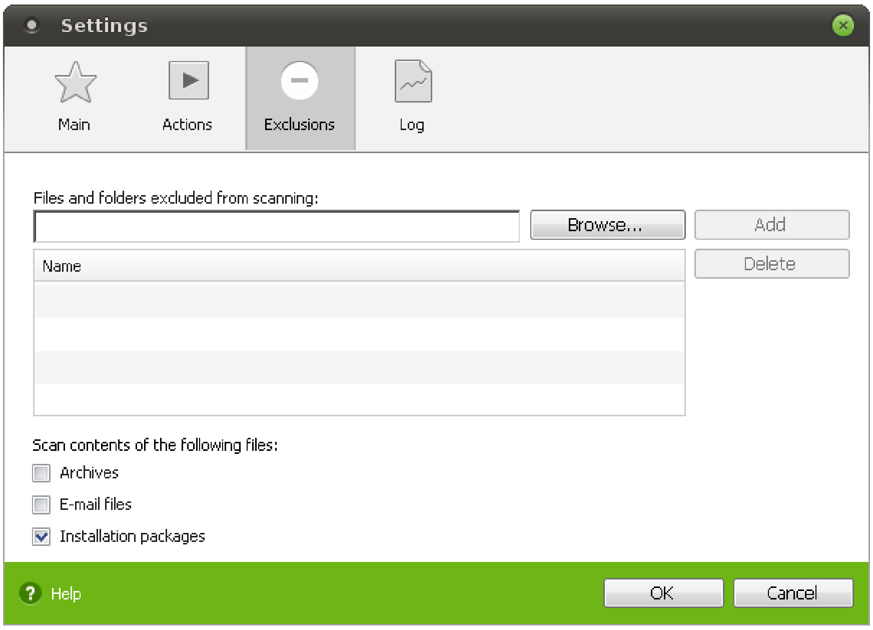
The best action for curable threats (for example, files infected with known viruses) is curing, since it allows to restore the infected file completely. It is recommended to move other threats to quarantine in order to prevent loss of potentially valuable data. You can select one of the following actions:

Action	Description
Cure	Instructs to restore the original state of an object before infection. If the object is incurable, or an attempt of curing fails, the action set for incurable viruses is applied. This action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects (archives, email attachments, file containers). Trojan programs are deleted on detection. This is the only action available for boot sectors.
Move to quarantine	Instructs to move the object to a specific directory for isolation. This action is impossible for boot sectors.
Delete	Instructs to delete the object. This action is impossible for boot sectors.
Ignore	Instructs to skip the object without performing any action or displaying a notification. The action is available only for potentially dangerous files: adware, dialers, jokes, hacktools and riskware.

⚠ Threats within complex objects (archives, email attachments, file containers) cannot be processed individually. The threat neutralization action is applied to the entire object, and not just to the infected part. By default, the program is set to inform on detection and move the object to quarantine.

Exclusions Page

On this page, you can specify files and folders that should be excluded from scanning and determine whether to scan contents of archives, email files, and installation packages.



Files and folders excluded from scanning:

Name

Scan contents of the following files:

☐ Archives

☐ E-mail files

☑ Installation packages

Here you can list names or masks for the files to be excluded from scanning (this option is appropriate for temporary files, swap files, etc.).

To configure excluded files list

Complete the following steps:

- Enter the name (mask) of a file that should be excluded from scanning. To add a file residing on your system, you can click **Browse** and select the file in the standard file chooser. You can also use masks.

  A mask denotes the common part of object names, at that:

  - The asterisk (`*`) character replaces any, possibly empty, sequence of characters.
  - The question mark (`?`) replaces any character (one).
  - Other mask characters should be treated literally.

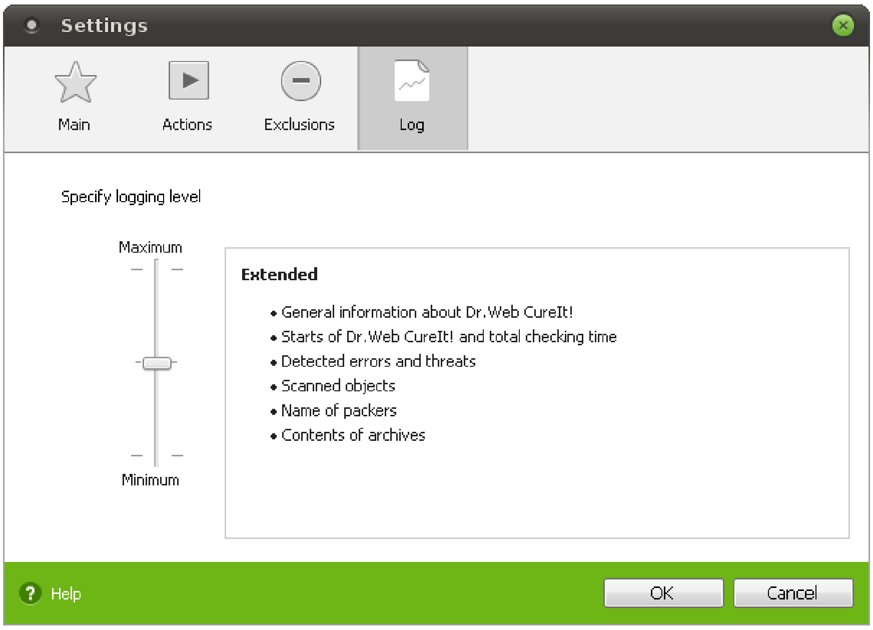
  Examples:

  - `Report*.doc` defines all DOC documents which names start with the word "Report" (`ReportFebruary.doc`, `Report121209.doc`, etc.).
  - `*.exe` defines all executable files; that is, files with the EXE extension (`setup.exe`, `iTunes.exe`, etc.).
  - `photo????09.jpg` defines all JPG images which names start with the word "photo", end with "09" and contain exact number of 4 other characters in the middle (`photo121209.jpg`, `photoJoe09.jpg`, `photo----09.jpg`, etc.).

- Click the **Add** button on the right. The file (or file mask) will be added to the list below.
- To remove a file from the list, select it and click **Delete**. The file will be checked during the next scan.

Log Page

On this page, you can specify logging parameters.



Specify logging level

Extended

- General information about Dr.Web CureIt!
- Starts of Dr.Web CureIt! and total checking time
- Detected errors and threats
- Scanned objects
- Name of packers
- Contents of archives

You can specify one of the following verbosity levels for logging:

- **Standard**—in this mode, the most important events are logged, such as time of Dr.Web CureIt! starts and stops or information on detected threats.
- **Extended**—in this mode, in addition to the most important events, names of packers and content of scanned archives is logged. If required, you can add such objects to the list of exclusions, which can reduce system load. If necessary, you can add these objects to the list of exclusions, which will help to increase computer performance. This logging mode is set by default for Dr.Web CureIt!.
- **Debugging (not recommended)**—in this mode, all details on Dr.Web CureIt! operation are logged, which may result in considerable log growth. It is recommended to use this mode only when errors occur in Dr.Web CureIt! operation or by request of Doctor Web company technical support.

Sending Statistics

If you want to participate in the improvement program of Doctor Web company, select the appropriate option when running Dr.Web CureIt!.

In order to provide analysis of information security threats and overall viral situation around the globe as well as to ensure continuous development and improvement of Doctor Web company products, Dr.Web CureIt! collects and sends to Doctor Web company servers impersonal statistics while it scans and cures your system.

This statistics contain only the following general information:

- Information on each detected threat including its name and type, the name and type of infected object, and hash of the infected file when necessary.
- Scan summary including scanning time, number of scanned files and objects, number of suspicious objects, and number of detected threats per type.
- Summary on applied actions including number of unmodified objects as well as number of cured, deleted, moved, renamed, and ignored objects.

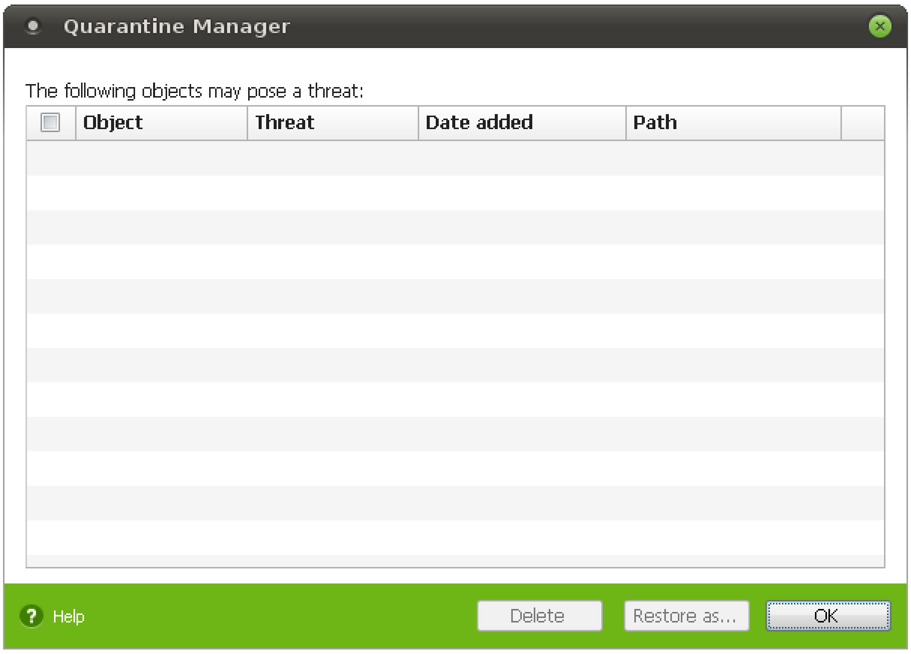
The privacy statement from Doctor Web company is available on the official website https://company.drweb.com/policy/.

To connect to the Internet, the program uses the network connection on your computer.

Quarantine Manager

Quarantine Dr.Web CureIt! serves for isolation of files that are suspected to be malicious. It also store backup copies of files processed by Dr.Web CureIt!. The directory `DrWeb CureIt Quarantine` is created in the root of the drive where an infected object is located. Such objects are moved to appropriate directories and then the quarantined files located on hard drives are encrypted.

To open the **Quarantine Manager** window, click **Preferences** 🔧 on the toolbar and then select the **Quarantine Manager** item on the Dr.Web CureIt! settings menu.



The following objects may pose a threat:

□	Object	Threat	Date added	Path

The central table lists the following information on quarantined objects that are available to you:

- **Object**—name of the quarantined object
- **Threat**—malware class of the object, which is assigned by Dr.Web CureIt! when the object is quarantined
- **Date added**—the date and time when the object was moved to Quarantine
- **Path**—full path to the object before it was quarantined.

In the **Quarantine Manager** window, the following buttons are available:

- **Restore as**—removes selected objects from the quarantine and restores them to selected location.

  ⚠ Use this option only when you are sure that the selected objects are not harmful.

- **Delete**—deletes selected objects from the quarantine and from the system.

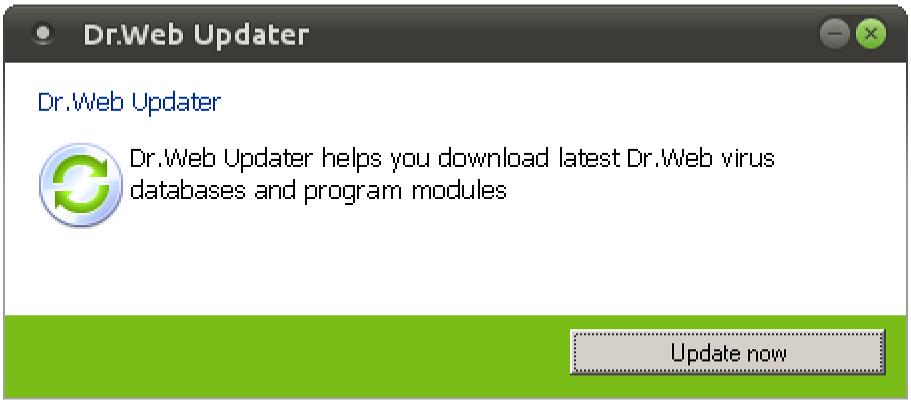
To apply an action to several files simultaneously, select the check boxes next to the object names and then click the corresponding button.

When you finish working with Quarantine manager, click **OK.**

Dr.Web Updater

New types of computer threats with more perfect masking techniques are constantly appearing worldwide. Updating virus databases guarantees an up-to-date protection for your computer. Updates are downloaded and installed by a specially designed component Dr.Web Updater.

You can run this component by clicking the **Update Virus Databases** icon on the desktop. **Dr.Web Updater** window opens.

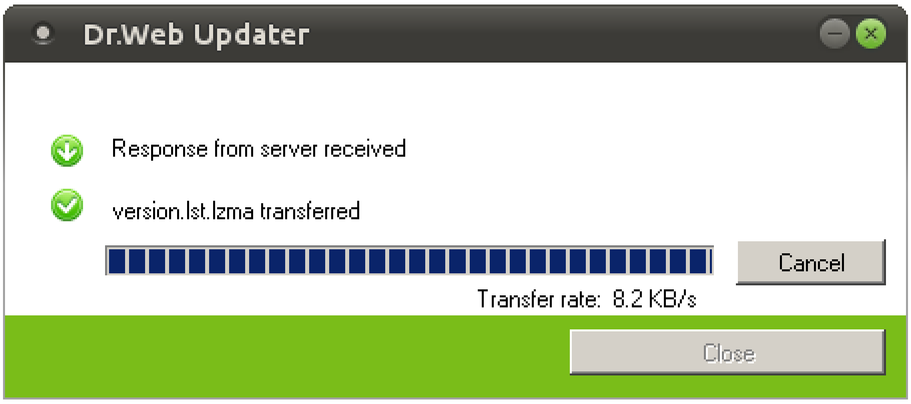


Dr.Web Updater

Dr.Web Updater

Dr.Web Updater helps you download latest Dr.Web virus databases and program modules

To receive an update for virus databases, click **Update now**. After the Doctor Web company server response is received, transfer of new files starts.



Dr.Web Updater

Response from server received

version.lst.lzma transferred

Transfer rate: 8.2 KB/s

When the component notifies you that all required files are received, click **Close** to finish working with Dr.Web Updater.

Registry Editor

Registry stores information that is necessary to ensure proper operation of Windows. This information includes profiles for each user, applications installed on the computer, types of documents created by them, folder properties, application icons, hardware that exists on the system, and used ports.

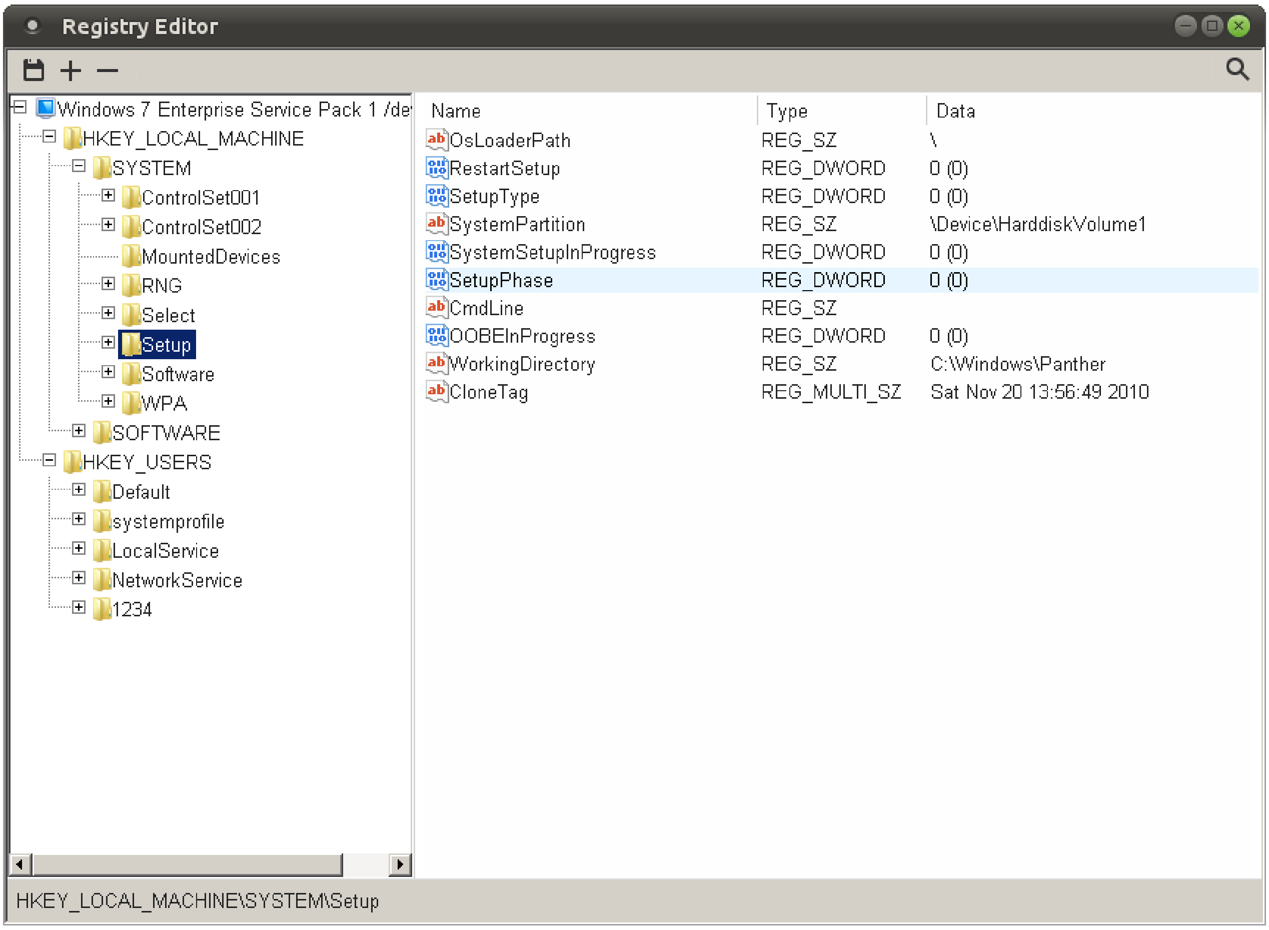
If you want to edit the registry manually, use the Dr.Web Registry Editor program, which is an analogue of the registry tool for Windows.

Starting registry editor

On Dr.Web LiveDisk startup, Dr.Web Registry Editor automatically detects registry keys of installed Windows operating systems. After that, you can work with registry keys the same way as in the standard registry tool for Windows (view their contents and edit them when necessary).

To start the program, double-click the **Dr.Web Registry Editor** icon on the desktop.

The window of the registry editor is shown in the picture below.



```
⊟ Windows 7 Enterprise Service Pack 1 /de
  ⊟ HKEY_LOCAL_MACHINE
    ⊟ SYSTEM
      ⊞ ControlSet001
      ⊞ ControlSet002
        MountedDevices
      ⊞ RNG
      ⊞ Select
      ⊞ Setup
      ⊞ Software
      ⊞ WPA
    ⊞ SOFTWARE
  ⊟ HKEY_USERS
    ⊞ Default
    ⊞ systemprofile
    ⊞ LocalService
    ⊞ NetworkService
    ⊞ 1234
```

Name	Type	Data
OsLoaderPath	REG_SZ	\
RestartSetup	REG_DWORD	0 (0)
SetupType	REG_DWORD	0 (0)
SystemPartition	REG_SZ	\Device\HarddiskVolume1
SystemSetupInProgress	REG_DWORD	0 (0)
SetupPhase	REG_DWORD	0 (0)
CmdLine	REG_SZ	
OOBEInProgress	REG_DWORD	0 (0)
WorkingDirectory	REG_SZ	C:\Windows\Panther
CloneTag	REG_MULTI_SZ	Sat Nov 20 13:56:49 2010

HKEY_LOCAL_MACHINE\SYSTEM\Setup

At the top of the window, you can see a bar with the following control buttons:

+	—opens *insert menu* which allows to add a key, a subkey or a particular value
−	—removes a key, a subkey or a particular value
💾	—saves the current registry state
🔍	—opens the search box where you can find an object in registry keys by the object name

On the left pane of the editor window, you can see registry keys. If the program detects several operating systems, it displays a separate register for each of them.

Every key can contain data that is called a value. On the right pane of the editor window, you can see a table which displays values of the selected key.

Description for registry keys

HKEY_LOCAL_MACHINE

This key contains configuration parameters for the computer (for all users), including data on the hardware and operating system (bus type, system memory, device drivers, and startup settings).

HKEY_USERS

This key contains information on all user profiles on the computer, including environmental variables, desktop settings, network connection settings, and parameters of printers and installed applications.

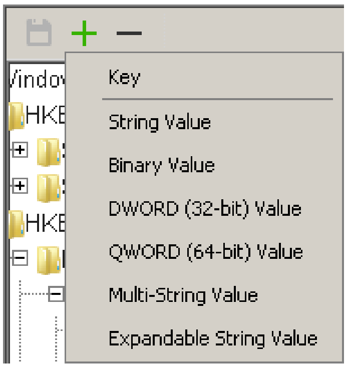
Working with registry

⚠ Use the Dr.Web Registry Editor program only if you are confident that the changes are correct. Exercise caution when editing the registry.

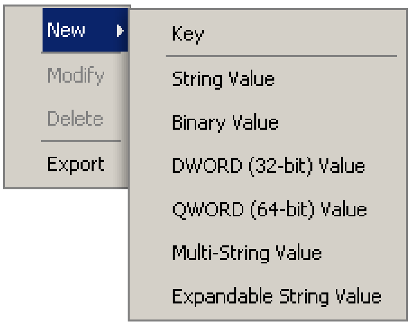
For additional protection, back up registry keys before you start editing them. If a problem occurs, you can then restore the registry to its previous state.

To add a new key

1. On the left pane, select the group of keys where you want to add a new key.
2. Select the **Key** item in one of the following ways:
   - Via the *insert menu* by clicking the + icon on the control bar (at the top of the editor window).



   - Open the *context menu* by right-clicking anywhere in the window and select **New**.



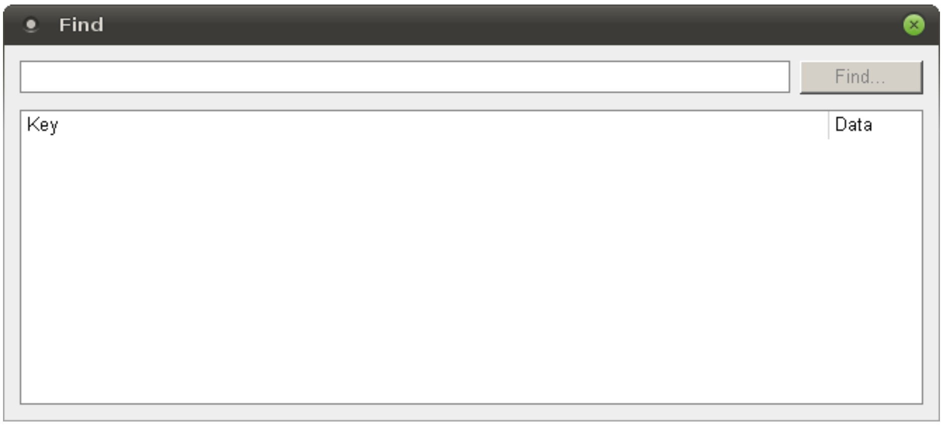
3. Enter a new key name and press ENTER.

To add a new key value

1. Select the key which value you want to change.
2. Via the insert menu or via the context menu select the type of the value to be added.
3. Enter the new name in the **Value name** box and, if necessary, change its default value specified in the **Value data** box.
4. Click **OK** or press ENTER to save the changes.

Searching for keys and values

1. Click the 🔍 icon on the control bar (at the top of the editor window). The **Find** window appears on the screen.



2. Enter data to search for and click **Find**.
3. If found, objects will be displayed in the table below.
4. At that, the **Find** button label changes to **Stop**. Click it if the required object is already found.
5. To open it in the editor, double-click the appropriate row and close the **Find** window.
6. The selected object is displayed on the left pane of the editor window. If the search object was a value, it is highlighted in the right pane.

Modifying key values

1. Select the key which value you want to change.
2. Select the required value in the table.
3. Either select **Modify** on the context menu or double-click the appropriate table row.
4. Modify the value in the **Value data** box.
5. Click **OK** or press ENTER to save the changes.

Removing keys and values

1. Find and select the registry element which is to be removed (key or value).

   ⚠ If you select a key, all its subkeys and values will be also removed.

2. Either select **Delete** on the context menu or click the icon of the removal tool − on the control bar.
3. The program displays a warning message. To confirm the removal, click **Yes**; to abort the process, click **No**.

Backing up a registry key

1. Open the context menu by right-clicking the key that you want to back up.
2. Select **Export**.
3. Choose file name.
4. Specify file path.
5. Click **Save**.

If necessary, you can send the `.reg` file to technical support or to the official forum.

Exiting registry editor

To finish working with Dr.Web Registry Editor, close the editor window. If any changes have not been saved, a window suggesting to save or discard changes will appear; choose the appropriate option to exit the editor.

Auxiliary Programs

Dr.Web LiveDisk is supplied with the following software tools that allow the user to work with the file system, configure network and browse the websites:

- Browser,
- Graphical File Manager,
- Console File Manager,
- Network Configuration Program,
- Terminal Emulator,
- System Date and Time Configuration.

This document provides you with short description of the tools listed above. For details on how to work with the programs, you may refer to the developers' websites.

Browser

Even though your computer cannot be started from the hard disk, the Web browser, included in Dr.Web LiveDisk, allows you to view websites and save the pages. You will be able to view saved pages after the operating system is fully restored and loaded.

⚠ A valid Internet connection is required to access web pages with the inbuilt browser. By default, the browser start page is the one of Doctor Web company official website https://www.drweb.com/.

Starting browser

To start the inbuilt browser double-click the **Web** icon on the desktop or use the system menu.

⚠ During its operation, Dr.Web LiveDisk uses a temporary RAM drive created when the system is starting. Thus, all saved webpages and browser history will be lost after the computer reboots. To save viewed webpages, use a subdirectory of one of the file system disks residing in the `/mnt/disk/..` directory.

For more information on working with the browser, visit the website of the developer at https://wiki.gnome.org/Apps/Web/.

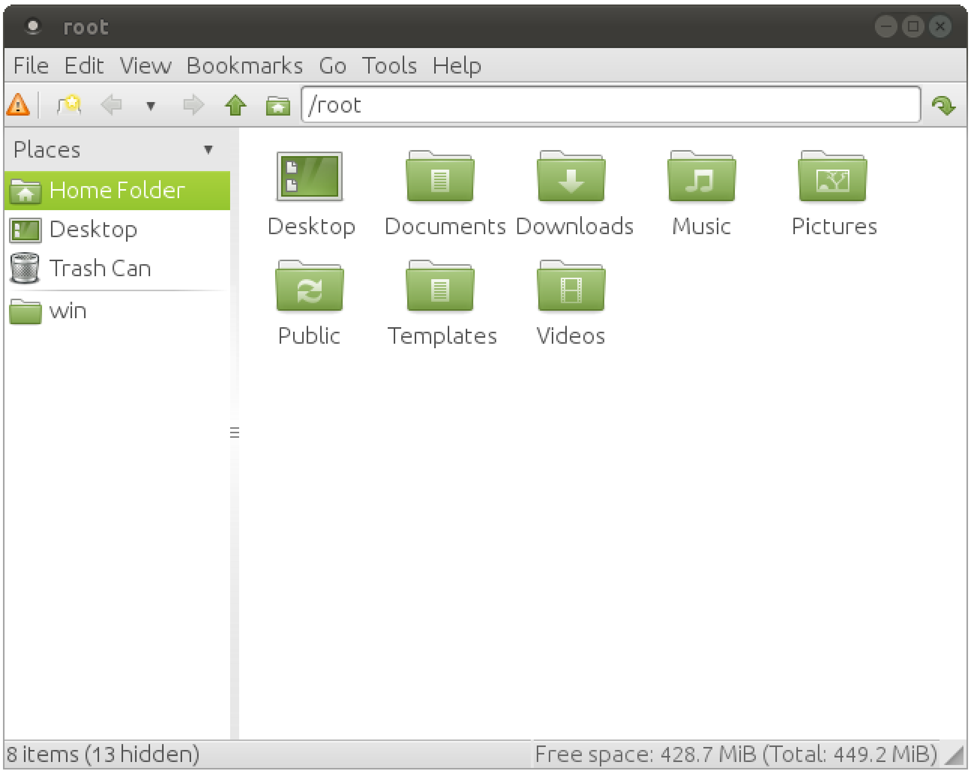
To finish working with Web browser, close the browser window.

Graphical File Manager

PCManFM is a file manager with graphical interface.

Starting graphical file manager

To start the file manager double-click the **File Manager** icon on the desktop or use the system menu. The window of the graphical file manager is shown in the picture below.



Working with graphical file manager

The *sidebar* allows you to switch quickly between the directories of your file system. To view the folder contents, click the appropriate folder icon on the sidebar and the objects contained in the folder will be listed in the right pane.

With the mode switcher on the top of the sidebar, you can switch to viewing the places or the directory tree.

In the **Places** mode, the sidebar displays fixed bookmarks: **Home Folder**, **Desktop** and **Trash Can**, and custom bookmarks which you can create to quickly access particular folders. Clicking the **Home Folder** bookmark opens the folder where user files are stored (created or downloaded by the user while Dr.Web LiveDisk is running).

To add a bookmark to the sidebar, open the required folder and click **Bookmarks** → **Add to Bookmarks** on the program menu.

In the **Directory Tree** mode, the sidebar displays the hierarchy tree structure of folders. To show or hide subfolders, click the arrow icon to the left of the folder icon.

The right pane of the window displays the folder contents. To open a subfolder, double-click its name.

Right-clicking a file or folder opens a context menu which offers several actions for the selected object.

If required, adjust file manager settings to meet your needs. For that, click **Edit** → **Preferences**. In the appeared window, you can configure the following: behavior and default view of the file manager, display options of the icons, volume management, advanced options.

Working with files and folders

⚠ To find a required object, view all file system disks in the `/mnt/disk/..` directory.

Opening files

When opening a file, the file manager applies the action recommended to this file type. For example, text files are opened in a text editor and graphics files are opened in a graphics viewer.

The file manager checks the extension of a file to detect the file type. If file has no extension or the extension in unknown to the program, the file manager attempts to determine the type by its contents.

You can change the application set by default to run files of a particular type. For that purpose, select a file of the appropriate type, right-click it and select **Open With**. In the appeared window, select the required application or add a new application manually (if it is not in the list). If you selected the appropriate check box, the specified application will be used to open all files of this type by default.

Folder and file options

To open the file property sheet, right-click the required file or folder and in the context menu select **Properties**.

File property sheets show information on any file or folder. In these window, you can change file or folder permissions, and select an application to be used for opening files of this type.

For details on how to work with the program, refer to the PCManFM project page at https://wiki.lxde.org/en/PCManFM.

Exiting graphical file manager

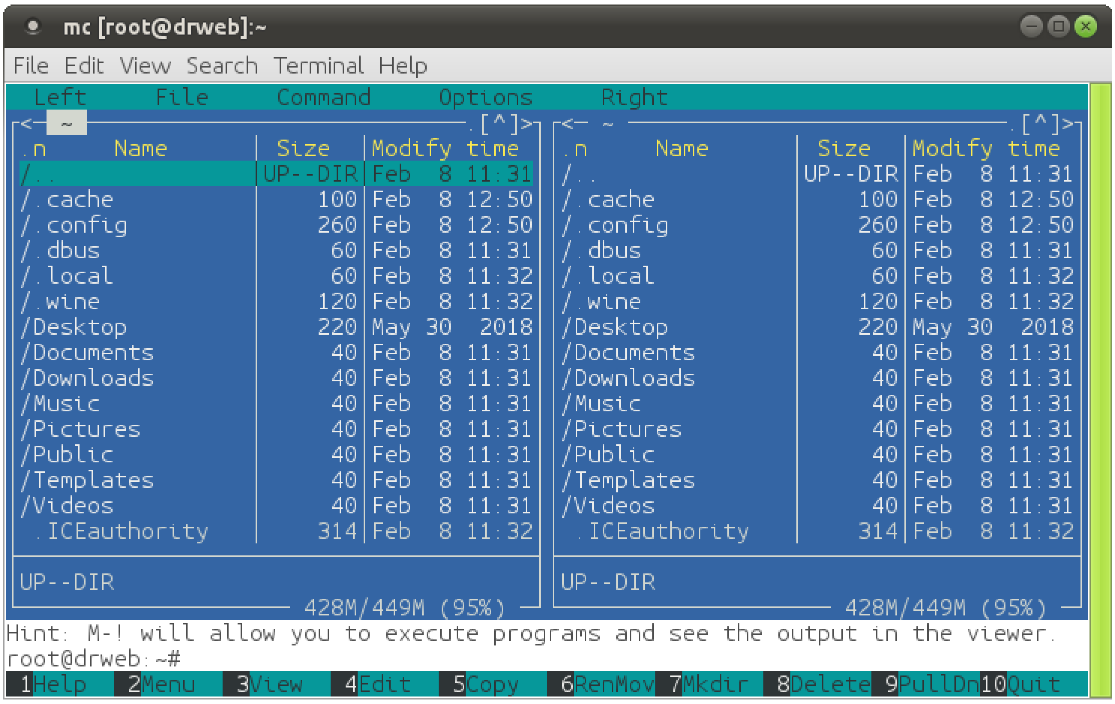
To finish working with the file manager, close the program window or on the **File** menu click **Close Window**.

Console File Manager

The inbuilt Midnight Commander file manager is similar to those used in MS-DOS and Windows operating systems and works in the console.

Starting console file manager

To start the console file manager double-click the **Midnight Commander** icon on the desktop or use the system menu. The following picture shows the window of the console file manager:



```
  Left     File      Command      Options      Right
┌<─ ~ ──────────────────────────.[^]>┐┌<─ ~ ──────────────────────────.[^]>┐
│.n       Name         │ Size  │Modify time │.n       Name         │ Size  │Modify time │
│/..                   │UP--DIR│Feb  8 11:31│/..                   │UP--DIR│Feb  8 11:31│
│/.cache               │    100│Feb  8 12:50│/.cache               │    100│Feb  8 12:50│
│/.config              │    260│Feb  8 12:50│/.config              │    260│Feb  8 12:50│
│/.dbus                │     60│Feb  8 11:31│/.dbus                │     60│Feb  8 11:31│
│/.local               │     60│Feb  8 11:32│/.local               │     60│Feb  8 11:32│
│/.wine                │    120│Feb  8 11:32│/.wine                │    120│Feb  8 11:32│
│/Desktop              │    220│May 30  2018│/Desktop              │    220│May 30  2018│
│/Documents            │     40│Feb  8 11:31│/Documents            │     40│Feb  8 11:31│
│/Downloads            │     40│Feb  8 11:31│/Downloads            │     40│Feb  8 11:31│
│/Music                │     40│Feb  8 11:31│/Music                │     40│Feb  8 11:31│
│/Pictures             │     40│Feb  8 11:31│/Pictures             │     40│Feb  8 11:31│
│/Public               │     40│Feb  8 11:31│/Public               │     40│Feb  8 11:31│
│/Templates            │     40│Feb  8 11:31│/Templates            │     40│Feb  8 11:31│
│/Videos               │     40│Feb  8 11:31│/Videos               │     40│Feb  8 11:31│
│ .ICEauthority        │    314│Feb  8 11:32│ .ICEauthority        │    314│Feb  8 11:32│
├──────────────────────────────────────────┤├──────────────────────────────────────────┤
│UP--DIR                                   ││UP--DIR                                   │
└─────────────────── 428M/449M (95%) ──────┘└─────────────────── 428M/449M (95%) ──────┘
Hint: M-! will allow you to execute programs and see the output in the viewer.
root@drweb:~#
 1Help   2Menu   3View   4Edit   5Copy   6RenMov 7Mkdir  8Delete 9PullDn10Quit
```

Working with files in Midnight Commander

In addition to the file system navigation bars, the file manager contains the inbuilt text editor that enables you to view and edit text files.

- To view a file, select its name and press F3; to edit the file, press F4.
- To delete the selected file, press F8.
- The bottom pane of the window displays actions corresponding to the functional keys.
- Additional functions of the file manager are available on the main program menu. To open the menu, press F9.

The input line that enables you to enter commands to the operating system is displayed between the bottom menu and navigation bars (similar to working in the console).

⚠ To find a required object, view all file system disks in the `/mnt/disk/..` directory.

For details on the program, visit the developers' website at https://www.midnight-commander.org/. You can also take advantage of the Help file provided with Midnight Commander. To open the program Help, either click **Help** on the bottom menu or press F1.

Exiting console file manager

To shut down Midnight Commander, do one of the following:

- Close the program window.
- Type `exit` at the command prompt.
- Press F10 and select **YES** when you are prompted to confirm exit.
- Select **Quit** on the bottom menu and then select **YES** when you are prompted to confirm exit.

Terminal Emulator

With MATE Terminal program, you can access Linux management console and work in text mode.

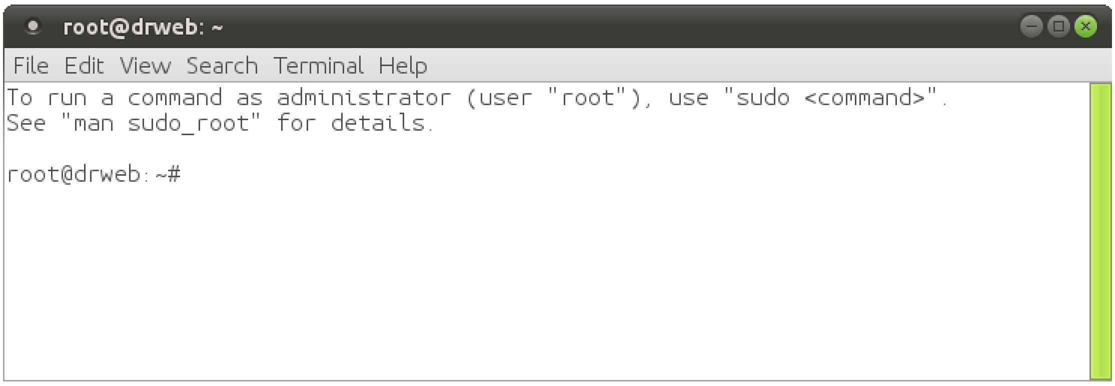
> ⚠ Working with the console requires basic knowledge of Unix-based operating systems and is recommended only to experienced users.

Starting terminal emulator

To start the terminal emulator double-click the **MATE Terminal** icon on the desktop or use the system menu.

When you start the terminal emulator for the first time, the program operates with its default settings.

The window of the terminal emulator is shown in the picture below.



```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@drweb:~#
```

Working with terminal emulator

To enter a command, type it at the command prompt marked with the prompt character `#`. Before the prompt character, the program shows the user name, the current system name (always `root@drweb`), and the current working directory.

You can scroll through the window contents bottom-up, as in teletype systems.

For details on the program, visit the developers' website at https://mate-desktop.org/.

To finish working with the terminal, either close the program window, or type `exit`, or on the **File** menu click **Close Window**.

Network Configuration Program

Dr.Web LiveDisk uses a network connection on your computer to connect to the Internet. A valid Internet connection is primarily required to update virus databases used by Dr.Web CureIt!. Moreover, it allows you to view websites (including documentation on particular components) in the browser supplied with Dr.Web LiveDisk.

Dr.Web LiveDisk automatically detects network connection settings on its startup. In most cases, the parameters are detected correctly and do not require manual modification. However, if a network connection is not found or the network is not available, you can specify correct connection parameters manually via the network configuration program.

> ⚠ The network configuration program can work only with accessible network devices.

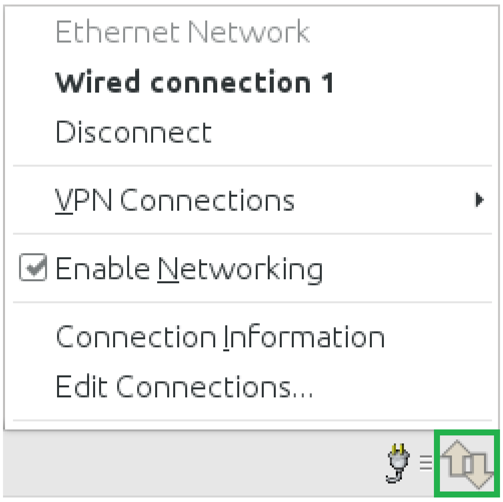
The program monitors the state of network interfaces and can automatically switch to a connection with higher speed. If a wired network interface is found, the program connects to this interface.

In the lower-right corner of the desktop, you can see a network connection icon which indicates the connection state:

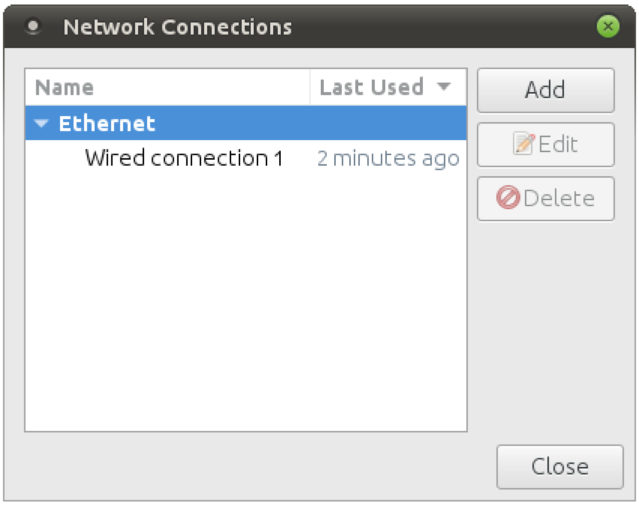
⇅	—connection is established
📶!	—networking is disabled
📶	—the program is searching a connection

Configuring network connections

1. To adjust the configuration settings, click the ⇅ icon and select **Edit Connections**.

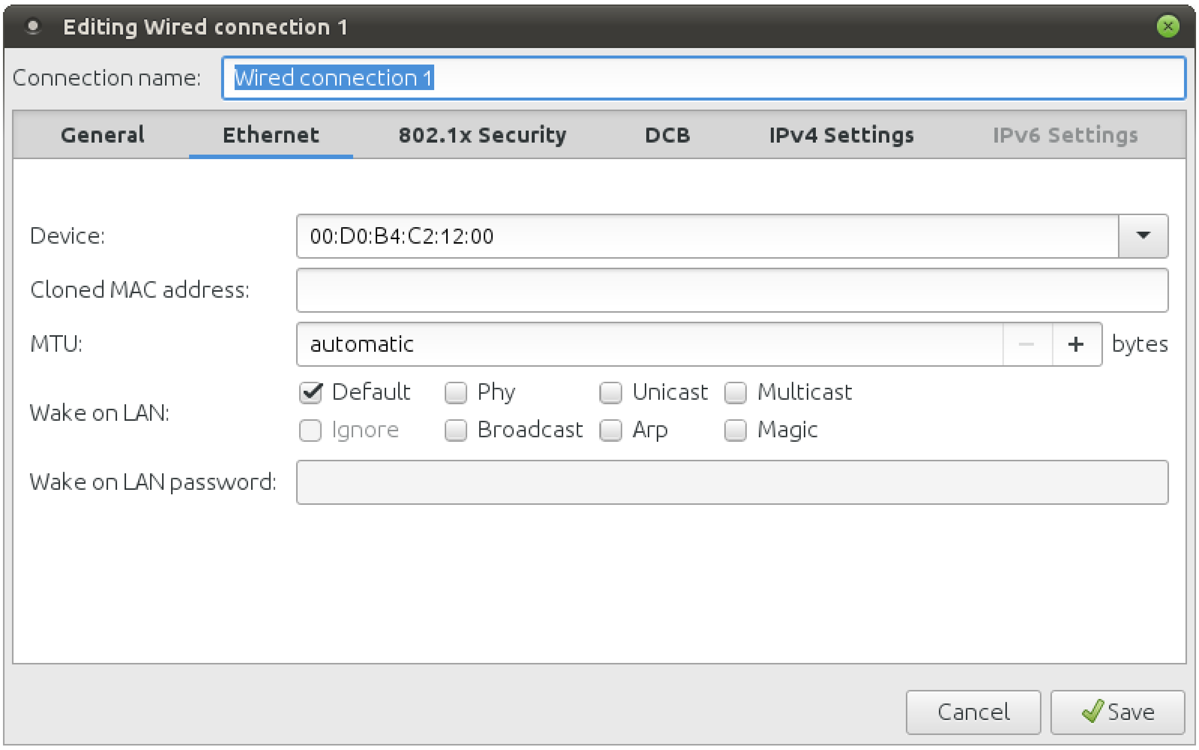


2. The **Network Connections** window appears on the screen.



Name	Last Used
Ethernet	
Wired connection 1	2 minutes ago

3. To add a new connection, click **Add** and in next window select type of connection you wish to create. If you want to adjust already specified settings, select the required connection and click **Edit**. This opens the edit window.



Connection name: Wired connection 1

Device: 00:D0:B4:C2:12:00

Cloned MAC address:

MTU: automatic bytes

Wake on LAN: ☑ Default ☐ Phy ☐ Unicast ☐ Multicast ☐ Ignore ☐ Broadcast ☐ Arp ☐ Magic

Wake on LAN password:

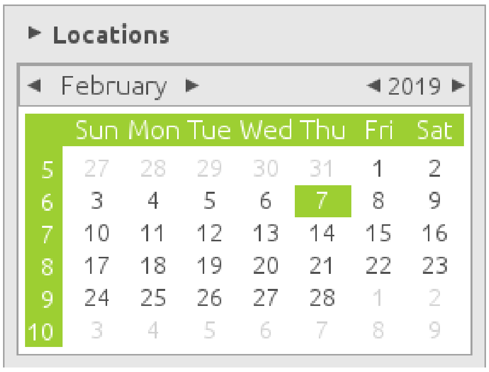
4. Configure settings as necessary.

> ⚠ You can move the cursor by using the TAB key and select/clear check boxes (when a required check box has focus) by pressing ENTER.

5. If required, select the **General** tab and select **Automatically connect to this network when it is available**.
6. Click **Save**. If you click the **Cancel** button, provided data are not saved.
7. To exit the network configuration program, click **Close**.

System Date and Time

To view the calendar, click the clock Thu Feb 7, 13:56 in the lower-right corner of the desktop.

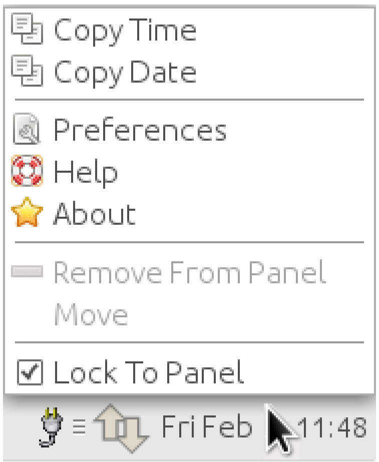


▶ Locations

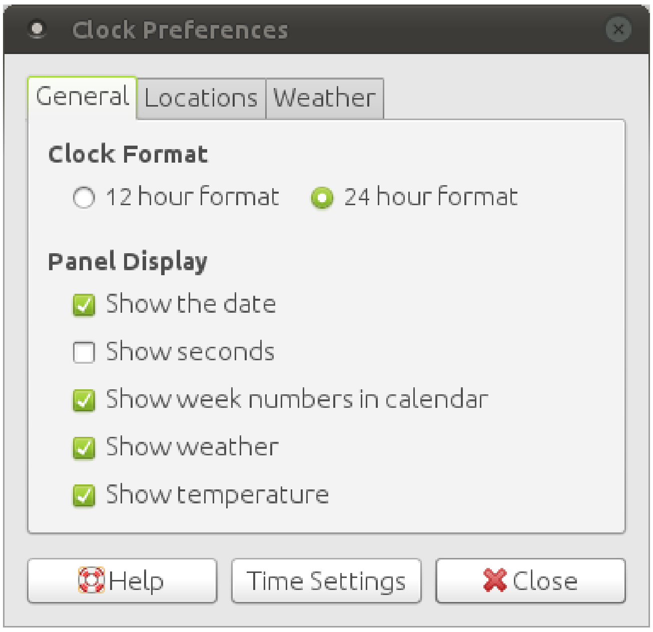
◀ February ▶ ◀ 2019 ▶

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
5	27	28	29	30	31	1	2
6	3	4	5	6	7	8	9
7	10	11	12	13	14	15	16
8	17	18	19	20	21	22	23
9	24	25	26	27	28	1	2
10	3	4	5	6	7	8	9

To change the system date and time, right-click the clock and then, in the context menu, click **Preferences**.



In the open window **Clock Preferences**, click **Time Settings**.



Clock Preferences

General | Locations | Weather

Clock Format

○ 12 hour format ● 24 hour format

Panel Display

☑ Show the date

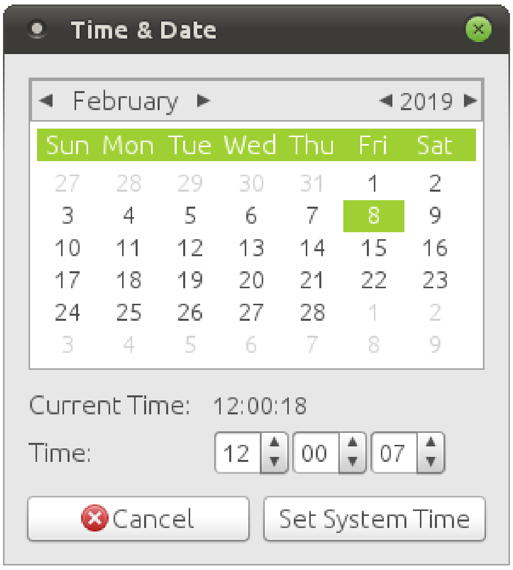
☐ Show seconds

☑ Show week numbers in calendar

☑ Show weather

☑ Show temperature

Set the required date and time values.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	1	2
3	4	5	6	7	8	9

Current Time: 12:00:18

Time: 12 00 07

To save your changes and close the **Time & Date** window, click **Set System Time**. After you finish using the program, click **Close** in the **Clock Preferences** window.

4. Technical Support

If you encounter any issues installing or using company products, before requesting for the assistance of the technical support, take advantage of the following options:

- Download and review the latest manuals and guides at https://download.drweb.com/doc/.
- Read the frequently asked questions at https://support.drweb.com/show_faq/.
- Browse the Dr.Web official forum at https://forum.drweb.com/.

If you have not found solution for the problem, you can request direct assistance from Doctor Web company technical support by one of the following ways:

- Fill in the web form in the corresponding section at https://support.drweb.com/.
- Call by phone in Moscow: +7 (495) 789-45-86.

Refer to the official website at https://company.drweb.com/contacts/offices/ for regional and international office information of Doctor Web company.