Defend what you create

User Manual

Dr.Web® Anti-virus for Windows Mobile
Version 5.0.0
Administration Manual
20.02.2009

Doctor Web, Ltd. Head Office
2-12A, 3rd str. Yamskogo polya
Moscow, Russia
125124

Web site: www.drweb.com
Phone: +7 (495) 789-45-87

Refer to the official web site for regional and international office information.

Doctor Web, Ltd.

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

Doctor Web, Ltd. 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

Introduction 5

Dr.Web Anti-Virus Protection 6

System Requirements 7

Launching Dr.Web LiveCD 7

Dr.Web LiveCD Graphic Shell 8

Settings 11

Menu Configuration 11

NetWorks Configuration 12

Openbox Configuration Manager 12

File System Scanning 13

Starting a Scanning 13

Scan Results 16

Scanner Settings 17

Main Options 17

Advanced Options 28

Inbuilt Applications 37

Browser 37

Mail Client 38

File Manager 40

Console Scanner 41

Starting a Scanning 41

Command Line Options 42

Creating Boot Flash Drives 46

Introduction

Dr.Web® LiveCD is an software product based on the standard **Dr.Web®** anti-virus **Scanner**. It allows to restore the system in cases when loading a computer from a hard drive is impossible. Using the emergency anti-virus assistance disk, you can not only clean your computer from infected and suspicious files, but also attempt to cure infected objects.

Dr.Web LiveCD is distributed as a boot disk with a portable operating system based on Linux and inbuilt software intended to facilitate computer scanning and curing, working with the file system, viewing and editing text files, viewing web pages, and sending and receiving e-mail messages.

Thus **Dr.Web LiveCD** provides access to computer resources both in cases when it is impossible to load the system from a hard drive, and in normal cases when it gives a convenient customizable interface (for details about this variant of usage, see Creating Boot Flash Drives).

You can load **Dr.Web LiveCD** in one of the following modes:

- standard GUI mode;
- safe mode with the command-line interface (Console Scanner).

The standard mode is preferable because of its pictorial view and better functionality. The bigger part of this manual describes working in this GUI mode. The safe mode is intended for experienced users familiar with Unix-based systems and it is used if the GUI fails to load. Working with the console shell is described in the last part of this manual.

Dr.Web Anti-Virus Protection

Dr.Web® LiveCD is an anti-virus solution designed to restore the system after it was crippled as a result of virus or malware activity. To protect the system from such situations, it is vital to have constant reliable protection of the most advanced anti-virus technologies.

The **Dr.Web®** cutting-edge technologies provide solid anti-virus protection for your home computer, office network, and large corporate networks. The **Dr.Web** solutions are distinguished for their low system requirements, compactness, speed of operation and reliability in detection of all types of malware.

Dr.Web offers the following solutions for constant protection against viruses, malware and spam:

- Protection of corporate networks (**Dr.Web Enterprise Suite**)
- Protection of workstations (**Dr.Web Security Space 5.0**, **Dr.Web for Windows 5.0**, **Dr.Web for Linux**, **Dr.Web Console Scanners**);
- Protection of file servers (**Dr.Web for Windows**, **Dr.Web for Unix**, **Dr.Web for Novell NetWare**);
- Protection of mail (**Dr.Web for MS Exchange**, **Dr.Web for IBM Lotus Domino**, **Dr.Web for MIMEsweeper**);
- Protection of SMTP gateways (**Dr.Web Mail Gateway**);
- Protection of Internet gateways (**Dr.Web for Unix**);
- Protection of mobile devices (**Dr.Web for Windows Mobile**)
- Internet-service for providers (**Dr.Web AV-Desk**).

For more information about company products, please visit the official **Doctor Web, Ltd.** web site at http://products.drweb.com/?lng=en.

System Requirements

Minimum system requirements to start the **Dr.Web LiveCD** anti-virus solution:

- i386 processor
- Minimum 128 MB of RAM (64MB to load in safe mode)
- a CD-ROM, DVD-ROM or flash drive with minimum 64 MB of free space

Launching Dr.Web LiveCD

Make sure that your computer is set up to boot from the CD drive, in which the disk with **Dr.Web LiveCD** is inserted, or from any other data carrier, on which **Dr.Web LiveCD** is stored. At start a menu is displayed from which you can select the load mode.

Using the arrow keys on your keyboard select one of the following items and press ENTER:

- To launch the GUI version of **Dr.Web LiveCD**, select **DrWeb-LiveCD**.
- To launch the command line version (the Console Scanner), select **DrWeb-LiveCD (Safe Mode)**.
- To load your computer from the hard drive without launching **Dr.Web LiveCD**, select **Local HDD** (cancel launching of **Dr.Web LiveCD**, launch the system from the 0 partition of the 0 drive (hd0,0)).
- To test memory (for example, when you computer is extremely unstable and restarts at random), select **Test Memory**.

Dr.Web LiveCD Graphic Shell

The **Dr.Web LiveCD** software includes a graphic shell with a windowing interface similar to the Linux operating system GUI. See Figure 1.

By default, the desktop with the **Dr.Web** trademark for the background contains icons of applications included in **Dr.Web LiveCD**.

The taskbar (a horizontal bar in the bottom) contains

- System menu button 
- Quick Launch icons for inbuilt applications
- Desktop switching icons
- System clock (in the right corner)

Dr.Web LiveCD includes the following basic applications:

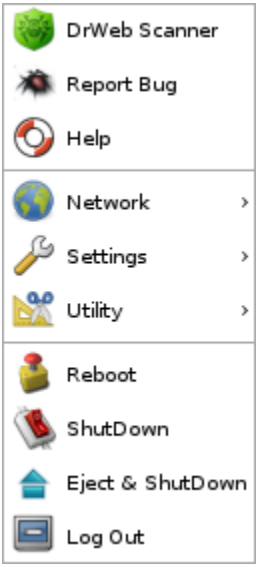
- **Dr.Web® Scanner for Linux**;
- **Firefox** browser;
- **Sylpheed** mail client;
- **Midnight Commander** file manager;
- command-line terminal to work directly from under the graphic shell;
- **Leafpad** text editor.

Figure 1. Graphical User Interface

You can start the main components by

- double-clicking the icon of the respective component on the desktop (by default, basic components are represented on the desktop);
- clicking the icon of the respective component in the taskbar (except for the file manager and **Dr.Web Scanner for Linux**).
- selecting the respective component on the system menu of the shell.

To open the system menu, click the system menu button in the taskbar.



You can access the desktop context menu named **Openbox** by right-clicking the desktop.

For information on how to use **Dr.Web Scanner for Linux**, select **Help** on the system menu or use the **Help** menu of the Scanner main window.

After the graphic shell has been loaded, by default the main window of **Dr.Web Scanner for Linux** opens. **Dr.Web Scanner for Linux** is designed to check all Windows root partitions of a computer for viruses.

Settings

The **Dr.Web LiveCD** settings are available through the **Settings** item of the system menu and include the following options:

- Menu Configuration which allows you to configure appearance of the taskbar
- NetWorks Configuration which allows you to configure network
- Openbox Configuration Manager which allows you to configure the GUI

To configure settings, select a corresponding item in the menu. The settings window opens.

Menu Configuration

This windows allows you to configure the position, size, and special effects in appearance of the taskbar on the **General** tab, as well as configure GUI plugins installed on the **Plugins** tab.

Setting	Description
Position	Select the following parameters: • the taskbar position on the screen (**Edge**) • alignment of the taskbar elements (**Alignment**) • the taskbar margine (**Margine**)
Size	Select the the taskbar width **Width** and **Height**.
Effects	Select the taskbar **Transparency** and **Color** settings.
Properties	Select other parameters: • type of the taskbar (**Set Dock Type**) • taskbar covering options (**Do not cover by maximized windows**) • hiding options (**Autohide**)

NetWorks Configuration

This window allows you to select a network **Interface** to use, configure IP protocol settings and select network configuration files.

Configure network

1. Select an **Interface** to use for network connection.
2. On the **Static IP** tab, select the following settings:

Setting	Description
Host	The computer name.
IP	The IP address.
Netmask	The network mask.
Gateway	The default gateway.
Name server	The name server.
Use DHCP	Select this option to receive network settings automatically using the DHCP protocol.

3. To save changes, click **Update**. To disable the network connection, click **Stop**.
4. On the **System wide** tab, select the network configuration files.

To edit a file, click the button next to an entry field.

5. To restart the network, click **Restart**.
6. To exit the settings window, click **Exit**.

Openbox Configuration Manager

This window allows you to configure the Openbox GUI including colour schemes, desktop parameters etc.

File System Scanning

This sections describes how to scan your file system for viruses.

Starting a Scanning

It is strongly recommended to update the **Dr.Web virus databases** before scanning. To do this, click the **Update** button.

Dr.Web® Scanner for Linux may be started in one of the following ways:

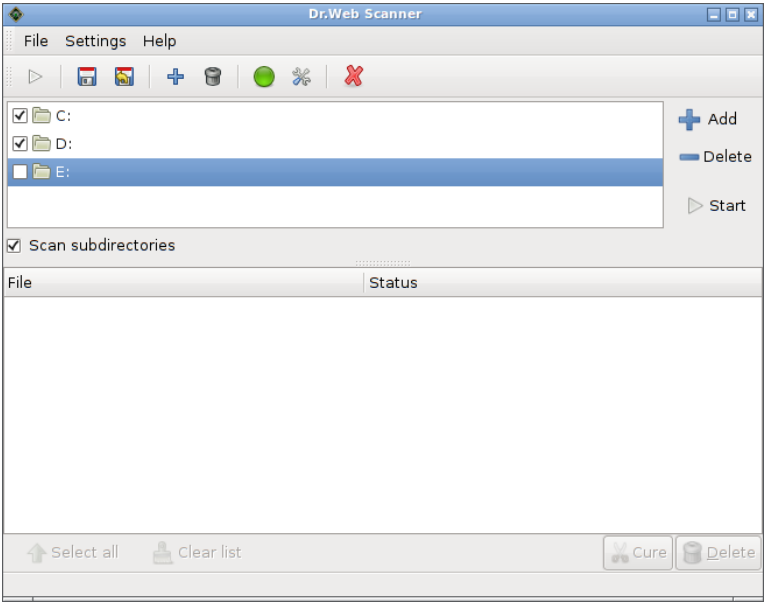
- Automatically after the graphic shell is loaded
- Using the desktop icon
- Using of the corresponding item of the system menu

After launching, the Scanner main window opens. See Figure 2.

The Scanner allows to check all types of Windows partitions (FAT, FAT32, NTFS) for viruses. By default, all partitions of the hard drive are selected for scanning.

By default, all the subdirectories in selected directories are scanned. If you want only files in certain selected directories and partitions checked, excluding the content of the nested directories (in spite it may be infected), clear the **Scan subdirectories** checkbox.

Figure 2. Main window



To add an object to or remove an object from the list of objects to scan, either click **Add** or **Delete**, or press INSERT or DELETE respectively.

The **Delete** button becomes available once you select an object.

If you do not want the Scanner to check a certain object, but you want it to remain on the scanning list, clear the checkbox next to this object.

When you click **Add**, a window opens where you can select objects to scan.

Initially the path selection pane (at the top) contains the following buttons:

-  **Type a file name** - open the file name entry field to add a file (to close the field, click the button again).
-  **File System** - open the list of **Dr.Web LiveCD** file system partitions.
-  **Win** - open the content of the Windows partition.

As you view file system objects, the buttons for the directories passed appear on the on the path selection pane (top of the window) ("bread crumbs"). Click a button to open the respective directory.

To add an object as a shortcut, select necessary directories in the file system explorer and click **Add**. To remove a shortcut, select the shortcut in the **Places** list and click **Delete**.

When done with selections, click **OK** to confirm the changes and close the window or click **Cancel** to close the window without saving the changes.

Shortcuts are added to the list of objects to scan automatically. You can use the shortcuts for navigation through the file system.

To start scanning the selected objects, click **Start** (it will turn to the **Stop** button and scanning will start).

During scanning the status bar in the bottom of the window reflects the current action, for example, virus databases loading or the full path to the file scanned at the moment.

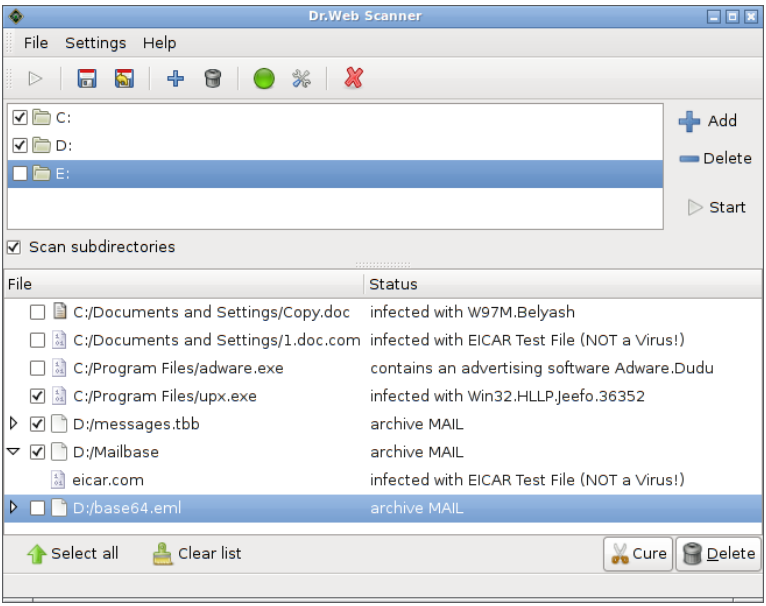
To terminate scanning, click **Stop** (it will turn to the **Start** button and scanning will stop).

Before scanning you can set additional parameters, such as: check mode (level of detail), actions over detected objects, etc. For more information on the settings, please see Main Options.

Scan Results

Scan results are shown as a table in the bottom of the Scanner main window. See Figure 3. There you can find information on infected and suspicious objects found during the scanning, their status, the path and actions performed by the program over these objects.

Figure 3. Result window



The list of detected objects is generated in a hierarchical order; if a virus is found inside an archive, then the archive is displayed in the report field as a node, whose contents you can expand and collapse.

Below the report field is a row of buttons where you can select the desired action for every object in the list: **Cure** or **Delete**. The **Cure** action is not available for archives, containers, and mail files.

If an action other than informing is specified for this type of detected objects on the Actions tab, the result of this action will be shown in the **Status** column.

When the **Cure** action is assigned for an object, if the file proves to be incurable, then the action specified for incurable objects on the Actions tab will be applied.

To select a desired action for certain found objects manually, select objects (or click **Select all** to select all objects) and click **Cure** or **Delete**.

Scanner Settings

This section describes Scanner options.

Main Options

You can access the main options of the Scanner via the **Options** button  on the toolbar or via the menu in the Scanner main window: **Settings** -> **Options**. In this window you can adjust the Scanner GUI, its actions upon detection of infected or suspicious objects and its interaction with the OS and various modules of the anti-virus complex.

Main settings are divided between several tabs:

- General - general settings;
- Actions - customization of program's reaction upon detection of virus threats or malware;
- Checking - customization of check mode of files, saving of current settings/restoring of defaults;
- Programs - customization of interaction with anti-virus complex components and other programs;
- Support - updates and technical support.

In the bottom of the main options window, the following control buttons are located:

- **Set default** - discard the customized settings and set the default ones;
- **OK** - save the parameters and return to the main window of the Scanner;
- **Apply** - save the parameters and stay in the settings window;
- **Cancel** - return to the main window of the Scanner and discard the changes.

General Tab

By default, the main options window opens on the **General** tab. See Figure 4.

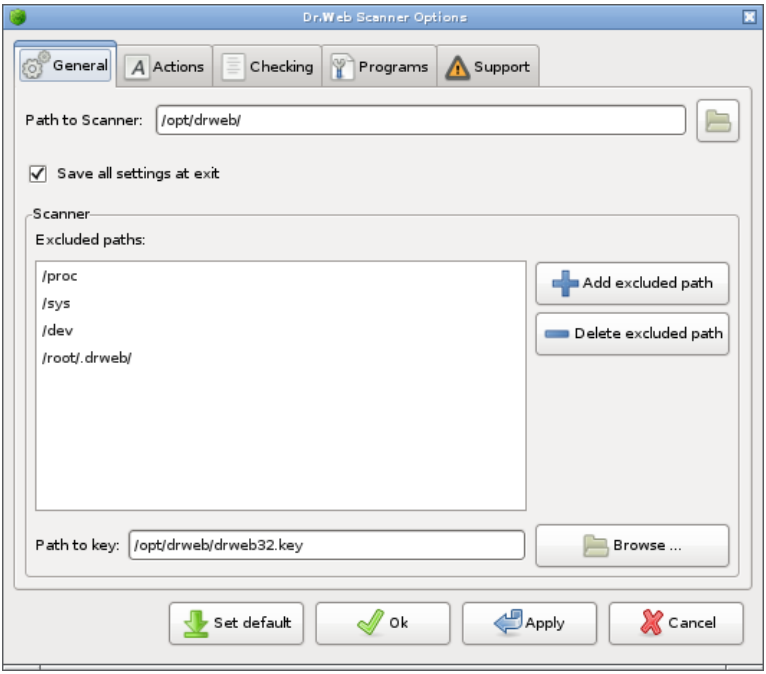
At the top of the **General** tab, you can specify the path to the Scanner. In the **Path to Scanner** entry field, type the path or click the button  and select the path via the file system explorer.

As a rule, the path to the Scanner specified by default is correct and there is no need to change it.

Similarly specify the path to the license key file in the **Path to key** entry field, if necessary.

Clear the **Save all settings at exit** checkbox, if you want the settings to be saved in the configuration file only by clicking the **Save settings** button. By default, this checkbox is selected and the settings are saved every time the Scanner is closed.

Figure 4. General options



You can specify the list of excluded paths which you do not what to scan. To add a certain directory, click **Add excluded path**. A window for selecting the path will open.

Initially the path selection pane (at the top) contains the following buttons:

- **Type a file name** - open the file name entry field to add a file (to close the field, click the button again).
- **File System** - open the list of **Dr.Web LiveCD** file system partitions.
- **Win** - open the content of the Windows partition.

As you view file system objects, on the path selection pane (top of the window) buttons corresponding to the directories passed appear ("bread crumbs"). Click such button to open the respective directory.

To add an object as a shortcut, select necessary directories in the file system explorer and click **Add**. To remove a shortcut, select the shortcut in the **Places** list and click **Delete**.

When done with selections, click **OK** to confirm the changes and close the window or click **Cancel** to close the window without saving the changes.

Shortcuts are added to the list of excluded paths automatically. You can use the shortcuts for navigation through the file system.

To delete an object from the list, select this object in the list of excluded paths and click **Delete excluded path**.

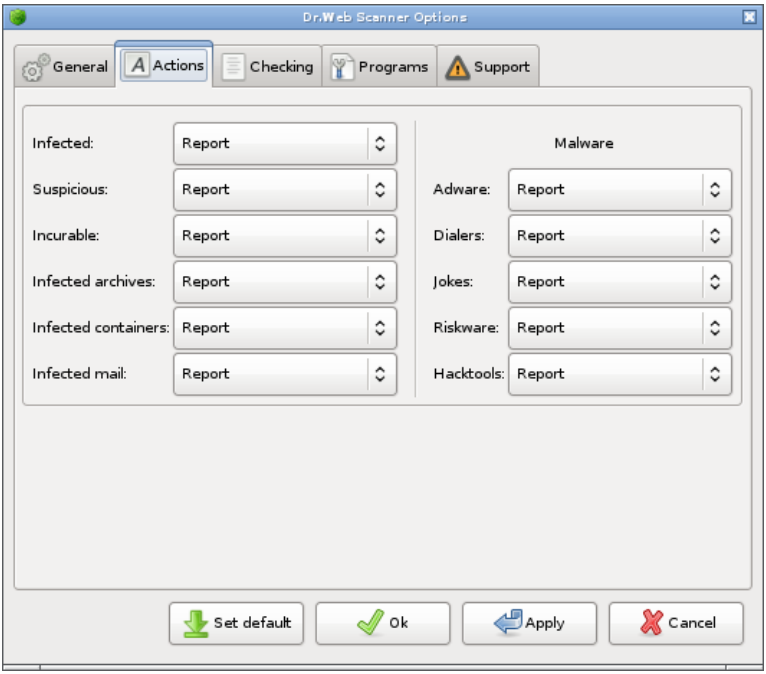
When you are done, click **Apply** to save the changes and leave the dialog box open.

Actions Tab

On the **Actions** tab, you can adjust the actions of the program upon detection of virus threats. See Figure 5.

By default, the **Report** action is set for all types of objects. Information on all the detected objects is displayed in the report field of the Scanner main window (see the Scan Results section). You can assign actions to the types of objects manually using the buttons under the report field.

Figure 5. Actions settings



You can change the program's reaction upon detection of virus threats or malware on the **Actions** tab. To do this, select the necessary action from the drop-down list near the respective type of object. The lists contain different sets of actions subject to the threat type:

- **Report** - report about the file in the report field in the Scanner main window.
- **Cure** - attempt to cure the file and restore it to the state before the infection. If curing is impossible, then the action specified for incurable objects will be applied.
- **Delete** - delete the file.

When infected or suspicious files are found in archives, emails or containers, the program applies the assigned action to the whole object and not to a single file inside the object.

The Scanner treats the following types of malware:

- **adware** (display advertisements);
- **dialers** (create a connection to the Internet or another computer network over the analog telephone or Integrated Services Digital Network (ISDN) without the user's intention and full knowledge as to cost);
- **jokes** (may scare or distract the user);
- **riskware** (potentially harmful programs which may be used to harm);
- **hacktools** (programs intended to facilitate unauthorized access to computers and other electronic devices).

When you are done, click **Apply** to save the changes and leave the dialog box open.

Checking Tab

All main scan settings are located on the **Checking** tab of the Scanner main window. See Figure 6. Here you can save necessary settings, load the settings from the configuration file, and restore the default settings.

The **Checking** tab includes

- **Check mode** pane;
- check modes description pane;
- settings control buttons.

Figure 6. Checking settings

A group of radio buttons named **Check mode** determines the mode of scanning (the checking thoroughness level):

- **Fast check** - only the files whose internal layout allows them to contain virus codes are scanned; archives and symlink objects are not scanned; the heuristic analyser is disabled. The scanning is a lot quicker than in the **Full check** mode, at the expense of reduced protection reliability.
- **Full check** - all selected objects are scanned, including archives and symlink objects; the heuristic analyzer is enabled. This mode is recommended for everyday computer scanning. It is slower than the **Fast check** mode, but has a much higher level of protection.

- **Advanced mode** - in this mode you can manually adjust the parameters which determine the checking thoroughness level. It is intended primarily for experienced users. When this mode is selected, the **Advanced Options** button becomes available in the bottom-right of the tab. Click the button to customize the parameters (see the Advanced Options section).

When you select any mode, its detailed description is given in the right part of the tab.

To save changes to the settings in the configuration file, click **Save Settings** (or press CTRL+S). The new settings will now be used at each program start or settings loading from the configuration file.

If you restart without saving the introduced settings, any changes to the configuration file will be deleted and all the parameters will be reset to the default, as when **Dr.Web LiveCD** was written to the disk or another medium. Please mind that if you select the **Save all settings at exit** checkbox on the **General** tab, the settings will be saved automatically every time the Scanner is closed.

To load the settings from the configuration file, click **Load Settings** (or press CTRL+L).

At program start the settings from the configuration file are loaded automatically. Use the **Load Settings** button only to discard the changes to the settings you have made.

In the program's configuration file in the `[GUI]` section, settings of the GUI module are stored. For more about the configuration file see **Dr.Web Anti-virus for Linux** documentation.

Programs Tab

On the **Programs** tab, you can adjust interaction of the anti-virus complex components. See Figure 7.

The **Programs** tab includes three panes:

- **Updater** - contains info necessary for the Updater;

- **Mail** - contains info necessary for the mail client;
- **Browser** - contains info necessary for the web browser.

On the top **Updater** pane

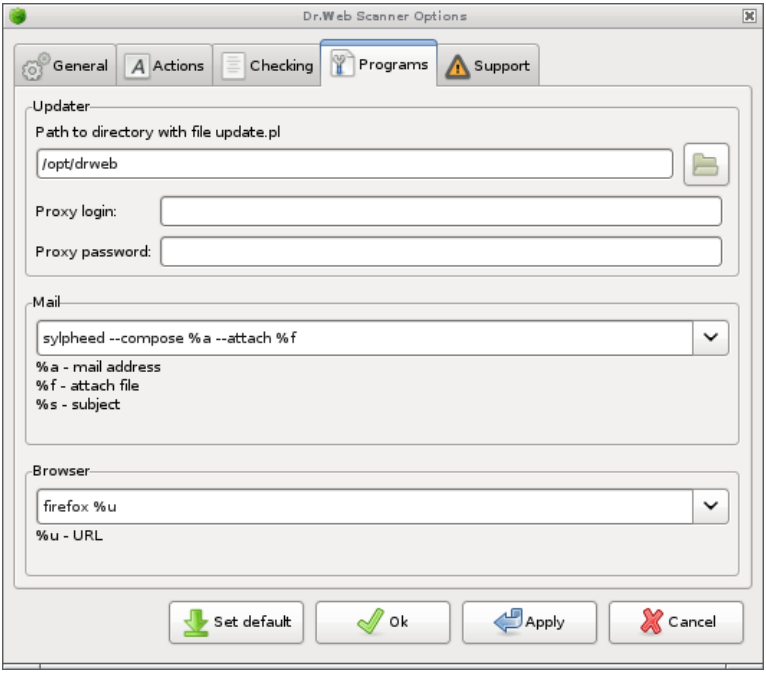
- If necessary, you can edit the path to the directory with the updating utility. To do this, specify the path in the **Path to directory with file update.pl** entry field or click the button  and select it via the file system explorer.
- If a proxy server is used to receive updates, type the login and password to the proxy server in the **Proxy login** and **Proxy password** entry fields correspondingly.

On the **Mail** pane, you can type a command line to launch the mail client and edit it, if necessary. Under the entry field, you can find possible parameters of the start command and their descriptions.

On the **Browser** pane, you can type a command line to launch the browser and edit it, if necessary. Under the entry field, you can find possible parameters of the start command and their descriptions.

When you are done, click **Apply** to save the changes and leave the dialog box open.

Figure 7. Programs settings



Updating and Technical Support

On the **Support** tab, you can update virus databases, contact technical support, send information about a bug or a suspicious file for check to **Doctor Web, Ltd.**, and view program info. See Figure 8.

The left pane of the **Support** tab contains buttons to facilitate the following actions:

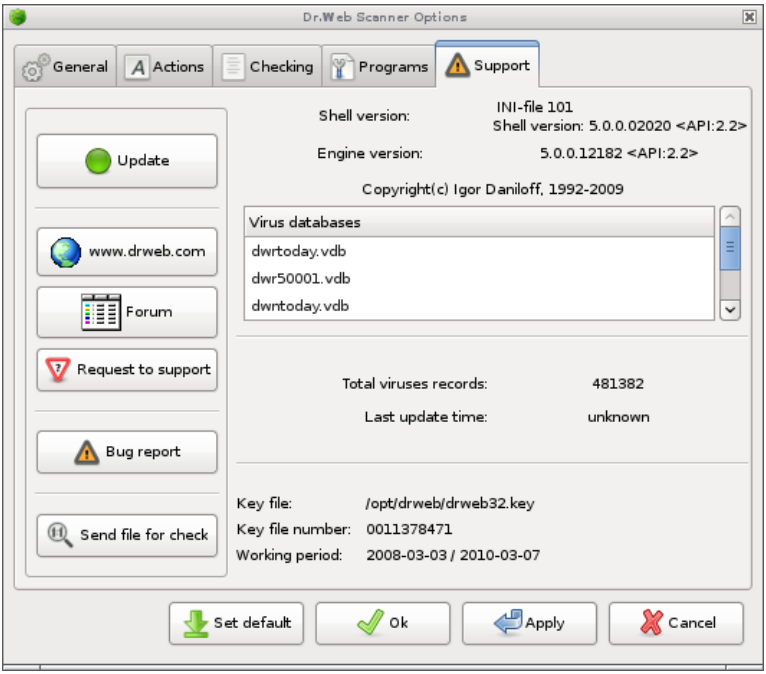
- Start the Updater. Click **Update**.
- Open the **Doctor Web, Ltd** official Web site. Click **www.drweb.com**.
- Open the Dr.Web for Unix forum in a window of the web browser. Click **Forum**. The inbuilt browser will open at the page of the **Doctor Web, Ltd.** forum.
- Send a request to the technical support. Click **Request to support**. The inbuilt browser will open at the page of the **Doctor Web, Ltd.** support service.
- Report a bug by e-mail. Click **Bug report**. The inbuilt mail client will open to send a mail message.
- Send files that are probably infected by unknown viruses for analysis to the **Doctor Web, Ltd.** laboratory. Click **Send file for check**. A window to select files will open.

The right pane of the **Support** tab contains info about the version of the program, loaded virus databases, last update time and license key number. This information is refreshed after every updating.

To update **Dr.Web virus databases**, visit the said Web sites, send e-mail messages and files, a connection to the Internet is required.

In case you see a message that the browser or the mail client is not found, when you click any of the links above, set the paths to the executable files of the browser and mail client. To do this, on the **Settings** menu select **Options -> Programs** and type necessary data.

Figure 8. Support



Advanced Options

Experienced users may want to choose the Advanced mode of scanning.

To set individual scanning parameters

1. On the Scanner **Settings** menu, select **Options** and the select the **Checking** tab.
2. On the **Check mode** pane, select **Advanced mode**.
3. The **Advanced Options** button in the bottom-right of the window will become available. Click the button to access the settings.

The advanced options menu allows to adjust manually the paths to directories used by the program, types of scanned files, modes of logging, etc.

The advanced options are divided in several sections (tabs):

- Paths - specify the paths to main modules.
- File Types - set the file types to be checked.
- Log File - set logging.
- Archive - set limitations to actions over archives for reasons of safety.
- Other - set parameters to adjust the computer workload, select Updater's timeout and enable the heuristic analyser.

In the bottom of the advanced options window, the following controls are located:

- **Set default** - discard user's changes to the settings and set the default;
- **OK** - save the settings and return to the Scanner main window;
- **Apply** - save the settings and and leave the dialog box open;
- **Cancel** - return to the main options window without saving the changes.

Paths Tab

By default, the advanced options window opens on the **Paths** tab. See Figure 9.

In the **Virus databases** list, the location of databases with virus records is specified. By default, the databases are located in the directory preset during the program installation. The Updater automatically places updated databases to this directory. However, if you wish to enable additional databases manually, you must add them to the **Virus databases** list. The database files which have a non-standard extension should also be added to this list even if they are located in the default directory.

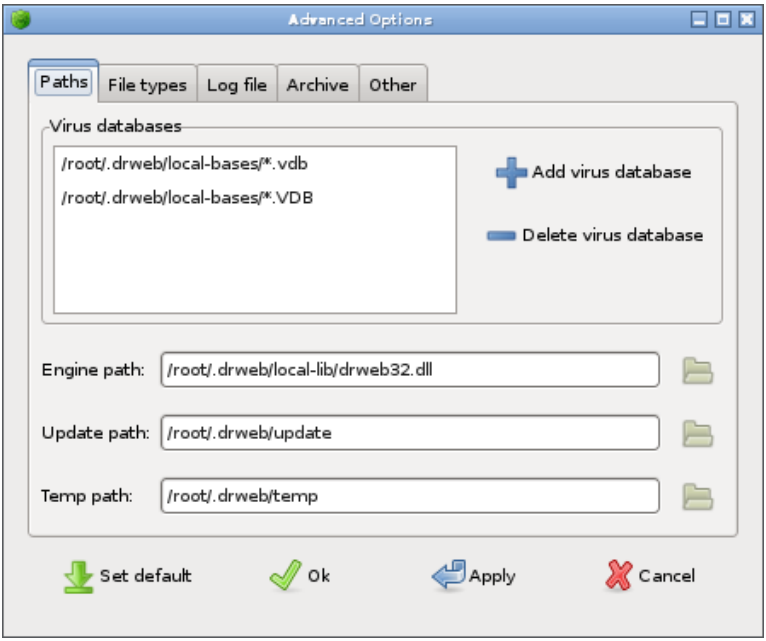
To add a database to the **Virus databases** list, click **Add virus database**. A window for adding a database will open.

By default, the list contains only two file masks: `*.vdb`; `*.VDB` (i.e. files with the `.vdb` or `.VDB` extensions only). You can specify just the character `*` (i.e. files with any extensions).

To delete a database from the **Virus databases** list, select it and click **Delete virus database**.

If necessary, you can edit the paths to the engine, the update directory and the temporary files directory, or select the paths via the file system explorer by clicking the button  next to the relevant line below the **Virus databases** list.

Figure 9. Paths.



File Types Tab

On the **File Types** tab, you can restrict the types of files to be checked

by the Scanner. See Figure 10.

On the **Scan mode** pane, set the method of files selection for scanning using the group of radio buttons:

- **All** - all files are scanned regardless of the names and the internal structure. This mode is set by default when you select **Full check** on the Checking tab of the settings.
- **By type** - only files with the extensions specified in the **File types** list are scanned. Executable files and files containing macros are on the list by default. To add an extension to the list, click **Add file type**, specify the desired extension in the opened window and then click **OK**. To delete an extension from the list, select it and click **Delete file type**.

The **Add file type** and **Delete file type** buttons are active only when the **By type** check mode is selected.

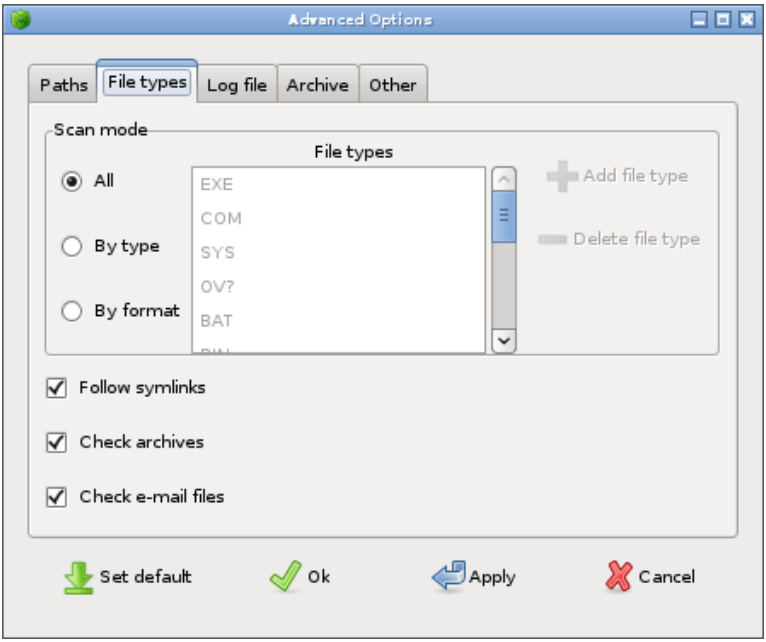
- **By format** - files, whose internal structure allows them to carry viruses, are scanned regardless of the names and extensions. This mode is set by default when you select **Fast check** on the Checking tab of the Scanner settings.

Below the pane you can select the following options to impose additional restrictions to files:

- Select the **Follow symlinks** checkbox if you want the Scanner to check the files symbolic links to which are to be scanned.
- Select the **Check archives** checkbox if you want the Scanner to unpack archives and check the files inside (in the **By format** mode, they should have a suitable format; in the **By type** mode, the extension of both the archive and the scanned file should be on the **File types** list).
- Select the **Check e-mail files** checkbox if you want the Scanner to check attachments to e-mail messages.

All three of the above checkboxes are automatically selected in the **Full check** mode and cleared in the **Fast check** mode (selected on the Checking tab of the settings).

Figure 10. File types



Log File Tab

On the **Log file** tab, you can adjust logging options.See Figure 11.

On the **Log File Name** pane, select whether the log should be kept by **Dr.Web LiveCD** or by the system service:

- **File name** - **Dr.Web LiveCD** will log events to the file specified in the entry field. You can edit the path to the log file in the entry field or click the button and choose the path via the file system explorer.
- **Syslog** - the log will be kept by the Syslog service. If you select this method, you can specify the logging facility and priority in the two drop-down lists below.

The following log facilities are available: **Daemon | Local0 .. Local7 | Kern | User | Mail**

You can select any of the variants below as the priority of events: **Info | Notice | Alert | Warning**

A selected **Limit log file size** checkbox instructs that the log file may not exceed the size specified in the entry field to the left. After the maximum has been reached, old entries will be gradually deleted to give space to the new ones. Clearing the checkbox will remove any limitation to the log file size.

It is recommended to keep the default **Limit log file size** option selected and the default value in the **Max log file size** (512 Kb) unchanged.

In the **Updater** section you can edit the path to the log file of the updating utility. Specify it in the **Log file** entry field or click the button  and choose the path via the file system explorer.

In the **Level of log** drop-down list, you can select the necessary level of logging detail. The following levels of detail are available: **Debug | Verbose | Info | Warning | Error | Quiet**

Figure 11. Log file

Archive Tab

On the **Archive** tab, you can set limitations to actions over archives for reasons of safety. See Figure 12.

The settings on the **Archive** tab are meant to protect the Scanner from 'mailbomb' attacks. They specify values of various archive characteristics, excess of which will lead to skipping these archives from scanning in order to avoid exhaustion of system resources.

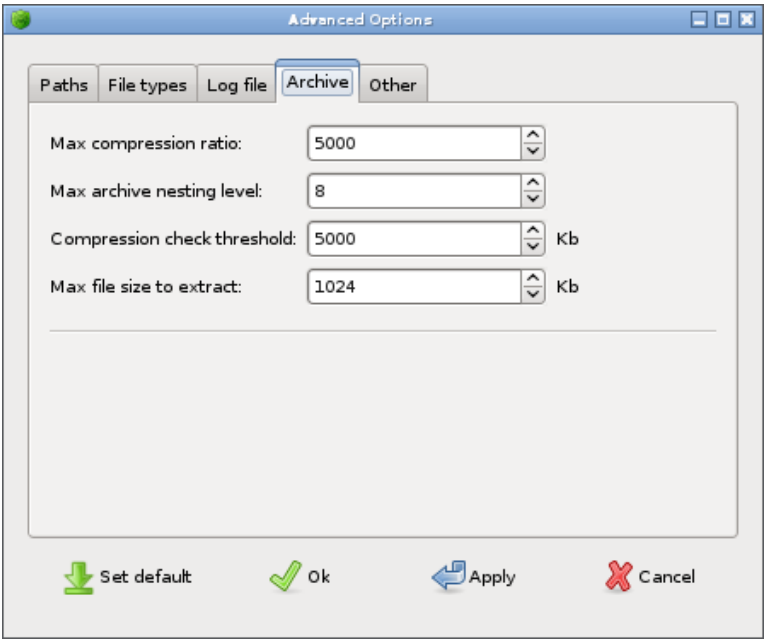
If it is necessary to change the default settings, edit the values in the following entry fields:

- **Max compression ratio** (by default 5000);
- **Max archive nesting level** (by default 8);
- **Compression check threshold** (by default 5000 Kb) - smaller

archives are scanned regardless of the compression ratio;

- **Max file size to extract** (by default 1024 Kb; the archive will not be unpacked, if it is larger).

Figure 12. Archive



Other Tab

On the **Other** tab, you can set parameters to adjust the computer workload, select Updater timeout and enable the heuristic analyser. See Figure 13.

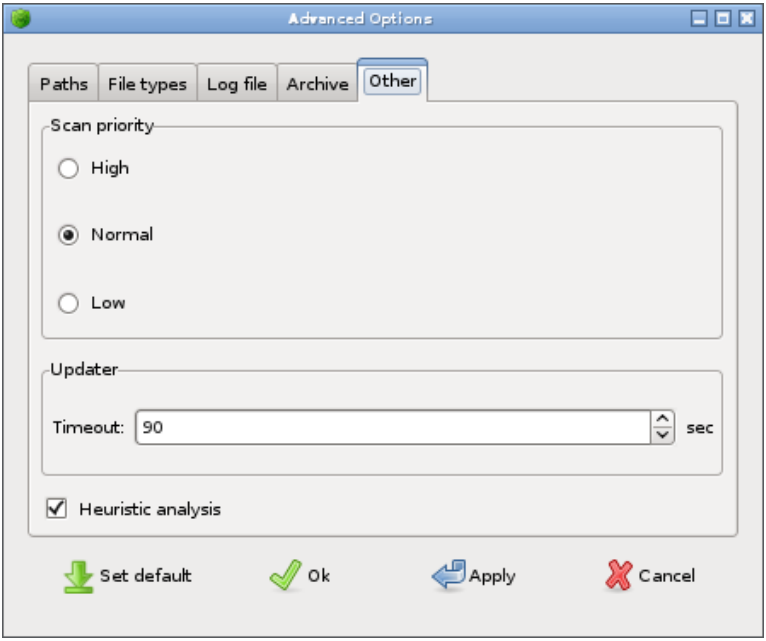
In the **Scan priority** group of radio buttons, you can select the priority of the scanning process compared to other system processes.

In the **Timeout** entry field, you can edit the default awaiting time of the updating utility when trying to connect to the update server.

Selecting the **Heuristic analysis** checkbox enables the heuristic analyser mode (a method of virus detection based on the analysis of actions specific for viruses).

In the heuristic analyser mode false positives are possible. All objects detected by the heuristic analyser have the 'suspicious' status. The analyser is automatically enabled, if you choose the **Full check** mode, and disabled in the **Fast check** mode.

Figure 13. Other



Inbuilt Applications

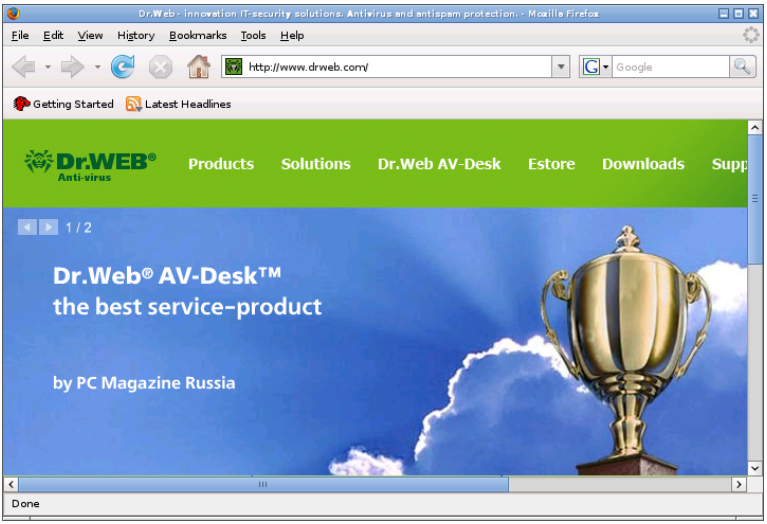
This section describes auxiliary tools available within the **Dr.Web LiveCD** anti-virus solution.

Browser

Even though your computer cannot be loaded from the hard drive, the Mozilla Firefox web browser included in **Dr.Web LiveCD** will allow you to view web sites and save the pages. You will be able to view the saved pages after the OS is fully restored and loaded.

An Internet connection via the local LAN is necessary to access the web with the inbuilt browser.

The browser default start page is the official web site of Doctor Web, Ltd.



Mail Client

The inbuilt **Sylpheed** mail client will enable you to maintain e-mail correspondence in full volume. See Figure 15.

An account at the server mail.drweb.com is preinstalled in the **Sylpheed** mail client to send messages. You can create other accounts to maintain correspondence.

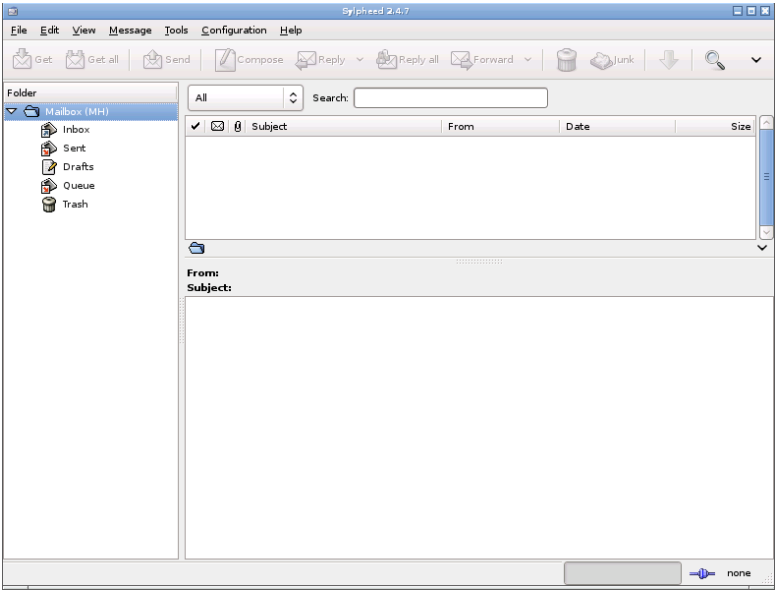
To create a new account, select **Configuration** menu -> **Create new account**. Enter all information necessary to enable mail transfer, such as sender's e-mail address, mail sending and receiving parameters (SMTP and POP3 protocols respectively), and accompanying information.

To work with several accounts, you can create extra mailboxes. To do this, select **File** menu -> **Mailbox** -> **Add mailbox**. In the e-mail box properties, specify what account is to be used: on the context menu of the mailbox, select **Properties** -> **Compose** tab -> **Account** drop-down list -> specify the account.

Sylpheed provides a secure connection to the mail server through the SSL and TLS protocols encoding.

When your OS is damaged and you cannot use your customary tools, this mail client included in **Dr.Web LiveCD** will allow you to continue normal correspondence through your registered e-mail account until the problem is solved.

Figure 15. Mail client

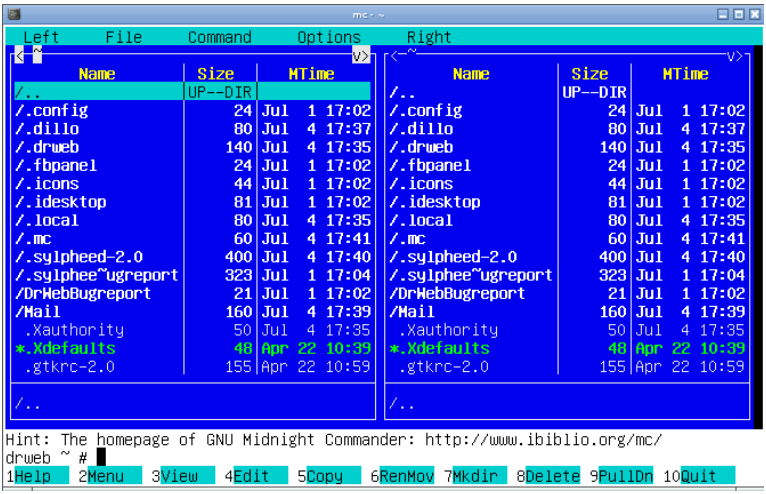


File Manager

The inbuilt **Midnight Commander** file manager is similar to the Norton Commander file manager. See Figure 16. By using full screen space of the terminals, it provides an intuitive user interface to the operating system, aiming to be a useful tool for users with any level of experience, from a newbie to a guru.

Homepage: http://www.ibiblio.org/mc/

Figure 16. File manager



Console Scanner

This section helps you get started using the Console Scanner.

Starting a Scanning

After launching **Dr.Web LiveCD** in the safe mode, the **Start Menu** appears.

Using the arrow keys, select one of the following items of the menu and press **ENTER**:

- **Start Xorg** - to launch the GUI version of the Scanner;
- **Start Shell** - to bring up the command line;
- **Start Midnight Commander** - to launch the inbuilt file manager;
- **Start Dr.Web Scanner** - to start scanning all hard disk partitions with default settings;
- **Start Dr.Web Update** - to update the virus databases;
- **Bugreport** - send information about a bug in the product to the developers;
- **Restart** - to reboot the computer;
- **Shut Down** - to shut down the computer without ejecting the disk;
- **Eject & Shut Down** - to eject the disk and shut down the computer.

If you want to start scanning with special options, select **Start Shell**. This will bring up the command line in the bottom of the screen. The general format of the scan start command is as follows:

```
/opt/drweb/drweb -path=<path> [options]
```

where `<path>` is the path to the directory or file which needs to be scanned.

If scanning is launched without any options with just the path specified, then the default options are used. Here is the command line for scanning of drive C: with default settings:

```
drweb -path=/win/C:
```

Command Line Options

Like any other Unix program, the **Dr.Web** Scanner provides a lot of command line options (or switches, which set additional parameters for a command). They are separated by blanks and begin with the character '-' (hyphen). The full list of options can be viewed by calling the `drweb` command with the `-?` or `-help` options.

The most commonly used options can be grouped as follows:

- scanning area options
- diagnosing options
- actions options
- interface options

The scanning area options define what is to be scanned for viruses. These are:

- `@[+]<file>` — scanning of objects listed in the specified file; the character '+' means that the list file should not be deleted after the scanning; the list file can contain paths to regularly scanned files and directories;
- `sd` — recursive search and scanning of files in subdirectories, beginning from the current one;
- `fl` — follow the links for files and directories; links which lead to 'looping' are ignored.

The diagnosing options, which define the types of objects to be scanned, are as follows:

- `al` — scanning of all files in the specified drive or

directory;

- `ar[ d/m/r][ n]` — scanning of files in archives (ARJ, CAB, GZIP, RAR, TAR, ZIP);
  `d` – deletion, `m` – moving, `r` – renaming of archives which contain infected files;
  `n` – disable output of the archiver name;
  not only archives proper (e.g. `*.tar`) are understood as archives here, but also their compressed formats (e.g. compressed TAR archives `*.tar.gz` and `*.tgz`);
- `cn[ d/m/r][ n]` – scanning of files in containers (HTML, RTF, PowerPoint);
  `d` – deletion, `m` – moving, `r` – renaming of containers which contain infected files;
  `n` – disable output of the container type;
- `ml[ d/m/r][ n]` — scanning of mail client files;
  `d` – deletion, `m` – moving, `r` – renaming of containers which contain infected files;
  `n` – disable output of the mail client name;
- `up[ n]` — scanning of executable files packed with LZEXE, DIET, PKLITE, EXEPACK;
  `n` — disable output of the packing utility name;
- `ex` — scanning of files, whose names conform to the specified masks (they are set in the `FilesTypes` string of the configuration file);
- `fm` — scanning of files which have an internal structure of program modules;
- `ha` — heuristic analysis of files, detection of unknown viruses.

The actions options define the actions to be carried out by the Scanner over infected and suspicious files. These options are:

- `cu[ d/m/r]` — curing of infected files; additional options instruct as follows: `d` – deletion, `m` – moving, `r` – renaming of infected files;
- `ic[ d/m/r]` — actions for incurable files: `d` – deletion, `m` – moving, `r` – renaming of incurable files;

- `sp[ d/m/r]` — actions for suspicious files: `d` – deletion, `m` – moving, `r` – renaming of suspicious files;
- `adw[ d/m/r/i]` — actions for files containing adware: `d` – deletion, `m` – moving, `r` – renaming of adware files;
- `dls[ d/m/r/i]` — actions for files containing dialers: `d` – deletion, `m` – moving, `r` – renaming of dialers;
- `jok[ d/m/r/i]` — actions for files containing jokes: `d` – deletion, `m` – moving, `r` – renaming of jokes;
- `rsk[ d/m/r/i]` — actions for files containing riskware: `d` – deletion, `m` – moving, `r` – renaming of riskware;
- `hck[ d/m/r/i]` — actions for files containing hacktools: `d` – deletion, `m` – moving, `r` – renaming of hacktools.

The interface options, which determine the manner of scan results display, are the following:

- `ot` — standard output of information on stdout;
- `oq` — disable output of information;
- `ok` — display an 'Ok' message for non-infected files;
- `log=<file>` — log the report to the specified file;
- `ini=<file>` — use an alternative INI file;
- `lng=<file>` — use an alternative language resources file.

Some options can act as the opposite parameter if they end with the character '-'. Such options are:
`-ar -cu -ha -ic -fl -ml -ok -sd -sp -up`

E.g. if we launch a scanning with the `drweb -path=<path> -ha-` command, the heuristic analysis, which is enabled by default, will be disabled.

The following options are enabled by default if the Scanner is launched without any additional parameters and the configuration file was not changed:
`-ar -fm -ha -fl- -ml -sd -up`

These options are considered the most rational for everyday scanning purposes. However, they do not determine any automatic actions for infected, suspicious and incurable files. You can specify different types of actions for such files, but the recommended ones are:

- `cu` — attempt to cure infected files without deletion, moving or renaming;
- `icd` — deletion of incurable files;
- `spm` — moving of suspicious files;
- `spr` — renaming of suspicious files (by default, the extension of the file is changed to `.#??`, i.e. the first character of the extension is replaced by the character `#`).

Creating Boot Flash Drives

Dr.Web LiveCD may be used as a portable operating system customized according to a user's needs to access data on any computer regardless of the OS and software installed. To save and reuse individual settings created during a session in **Dr.Web LiveCD**, it is necessary to write **Dr.Web LiveCD** files to a flash memory. For this the `CreateLiveUSB` command is used.

In spite that CreateLiveUSB does not change or delete the content of devices, it is advisable to save the files of the flash drive you are going to use on another data carrier, before launching the command.

To load **Dr.Web LiveCD**, you need not necessarily write the product to a CD disk and have a CD drive available. You may use a virtual machine with a CD drive emulator instead.

All **Dr.Web LiveCD** files are written to the `/boot` catalog. `CreateLiveUSB` changes the configuration of the partitions of the flash drive, if necessary; the original configuration is saved to the file `/boot/partition.backup`. `CreateLiveUSB` copies the MBR on the flash drive storing the original master boot record to the file `/boot/mbr.backup`.

To create a boot flash automatically

1. In the graphic shell, double-click the **Create Live USB**  icon on the desktop.

   CreateLiveUSB will switch to the waiting mode of a device connection through the USB port.

2. Connect the flash drive. It takes maximum ten seconds for a connection to be registered. If the connected flash drive has several partitions, LiveCD files will be written to the bootable partition, the bootable flag will be removed from other partitions.

To create a boot flash drive manually

3. Open the command-line terminal:
   - In the graphic shell, click the icon of the application on the desktop.
   - In the safe mode, select **Start Shell** on the main menu.
4. (Optional.) To check drives mounted on the computer, and partitions on flash drives, issue the `mount` command: `/bin/mount` or `mount`.
5. Execute the command `create_usb [device]` or `CreateLiveUSB [device]`.

   For example, `create_usb sda1`

   The command works in two modes:

   - When issued with the device, on which the files are to be written, explicitly specified. In this mode it is necessary to specify the name of the flash drive and the partition on which **Dr.Web LiveCD** is to be written.
   - When issued without specifying the device. CreateLiveUSB will switch to the waiting mode of a device connection through the USB port. It takes maximum ten seconds for a connection to be registered. If the connected flash drive has several partitions, LiveCD files will be written to the bootable partition, the bootable flag will be removed from other partitions.