



**Dr.WEB®**  
**LiveCD**

Defend what you create

## **User Manual**

**© 2003-2010 Doctor Web. All rights reserved.**

This document is the property of Doctor Web. No part of this document may be reproduced, published or transmitted in any form or by any means for any purpose other than the purchaser's personal use without proper attribution.

#### TRADEMARKS

Dr.Web, the Dr.WEB logo, SpIDer Mail, SpIDer Guard, CureIt!, the Dr.WEB INSIDE logo are trademarks and registered trademarks of Doctor Web in Russia and/or other countries. Other trademarks, registered trademarks and company names used in this document are property of their respective owners.

#### 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® LiveCD  
Version 5.0.2  
User Manual  
04.02.2010**

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

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

Refer to the official web site 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

|  |           |
|--|-----------|
| <b>1. Introduction</b>                     | <b>6</b>  |
| <b>1.1. Dr.Web Anti-Virus Protection</b>   | <b>6</b>  |
| <b>1.2. System Requirements</b>            | <b>7</b>  |
| <b>1.3. Launching Dr.Web LiveCD</b>        | <b>8</b>  |
| <b>2. Dr.Web LiveCD Graphic Shell</b>      | <b>9</b>  |
| <b>2.1. Settings</b>                       | <b>12</b> |
| 2.1.1. Taskbar Configuration               | <b>13</b> |
| 2.1.2. NetWorks Configuration              | <b>14</b> |
| 2.1.3. Openbox Configuration Manager       | <b>16</b> |
| 2.1.4. X Window Configuration              | <b>17</b> |
| <b>2.2. Inbuilt Applications</b>           | <b>18</b> |
| 2.2.1. Browser                             | <b>18</b> |
| 2.2.2. Mail Client                         | <b>19</b> |
| 2.2.3. File Manager                        | <b>21</b> |
| <b>3. Using Scanner from Graphic Shell</b> | <b>22</b> |
| <b>3.1. Main Options</b>                   | <b>22</b> |
| 3.1.1. General Tab                         | <b>24</b> |
| 3.1.2. Actions Tab                         | <b>26</b> |
| 3.1.3. Checking Tab                        | <b>28</b> |
| 3.1.4. Programs Tab                        | <b>31</b> |
| 3.1.5. Updating and Technical Support      | <b>32</b> |
| <b>3.2. Advanced Options</b>               | <b>34</b> |
| 3.2.1. Paths Tab                           | <b>36</b> |



|                                     |           |
|-------------------------------------|-----------|
| 3.2.2. File Types Tab               | 37        |
| 3.2.3. Log File Tab                 | 39        |
| 3.2.4. Archive Tab                  | 41        |
| 3.2.5. Other Tab                    | 42        |
| <b>3.3. Antivirus Scan</b>          | <b>43</b> |
| 3.3.1. Starting a Scan              | 44        |
| 3.3.2. Scan Results                 | 47        |
| <b>4. Using Console Scanner</b>     | <b>49</b> |
| <b>4.1. Starting a Scanning</b>     | <b>49</b> |
| <b>4.2. Command Line Parameters</b> | <b>51</b> |
| <b>5. Creating Boot Flash Drive</b> | <b>55</b> |
| <b>6. Reporting a bug</b>           | <b>57</b> |



# 1. Introduction

**Dr.Web® LiveCD** is a software product based on the standard **Dr. Web** anti-virus scanner. It allows to restore the system when loading a computer from a hard drive is impossible due to high virus activity. 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 Linux-based operating system 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 when it is impossible to load the system from a hard drive, and when there exists a need in a convenient customizable interface (for details about this variant of usage, see [Creating Boot Flash Drives](#) for **Dr.Web LiveCD**).

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 user-friendly interface and improved 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 operating systems and is used when the GUI fails to load. Working with the console shell is described in the last part of this manual.

## 1.1. 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 necessary to have constant reliable protection using 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, operation speed and reliability in detection of all types of malware.

**Doctor Web** company 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, visit the **Dr.Web [official web site](#)**.

## 1.2. 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 128 MB of free space



## 1.3. 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 options 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**.

Press TAB to edit each option manually.






## 2. Dr.Web LiveCD Graphic Shell

The **Dr.Web® LiveCD** software includes a graphic shell with a window-based interface similar to the Linux operating system GUI.

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
- Icons of currently used applications
- 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.

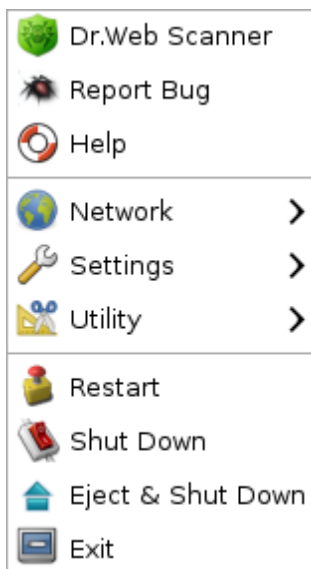


### Click an area for details

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.

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



### Click a command for info

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



### Click an area for info



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

After the graphic shell has been loaded, the main window of **Dr. Web Scanner for Linux** opens by default. **Dr.Web Scanner for**



**Linux** is designed to check all Windows root partitions for viruses.

### 2.1. 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
- [Xorg Configuration](#) which allows to configure the X Window System

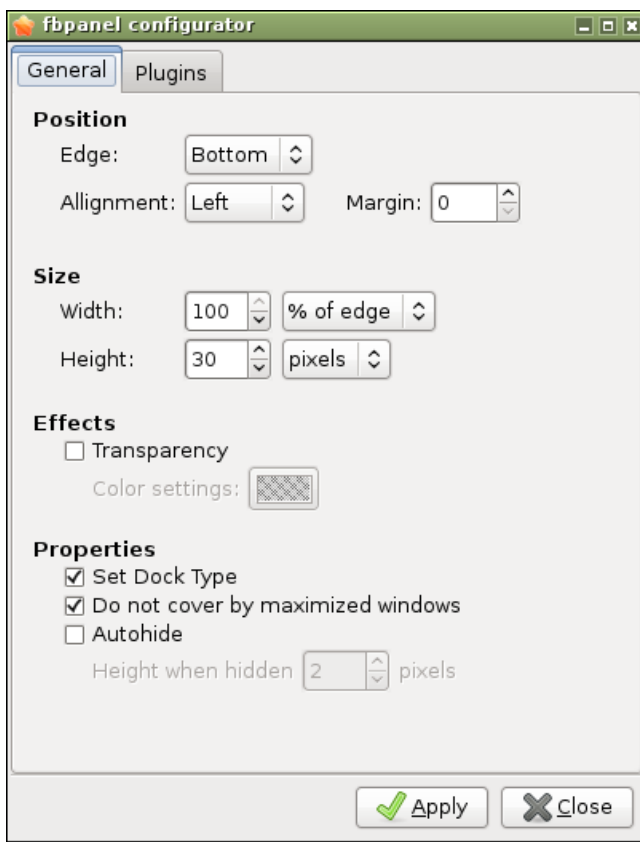
To configure settings, select a corresponding item in the menu. The settings window opens.



## 2.1.1. Taskbar 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 installed GUI plugins (on the **Plugins** tab). See [Figure 2](#).

**Figure 2.** Taskbar configuration





| Setting           | Description   |
|-------------------|---|
| <b>Position</b>   | Specify values for the following parameters: <ul style="list-style-type: none"><li>• the taskbar position on the screen (<b>Edge</b>)</li><li>• alignment of the taskbar elements (<b>Alignment</b>)</li><li>• the taskbar margine (<b>Margine</b>)</li></ul>     |
| <b>Size</b>       | Adjust the the taskbar width <b>Width</b> and <b>Height</b> .   |
| <b>Effects</b>    | Adjust the taskbar <b>Transparency</b> and <b>Color</b> settings.   |
| <b>Properties</b> | Specify values for other parameters: <ul style="list-style-type: none"><li>• <u>type</u> of the taskbar (<b>Set Dock Type</b>)</li><li>• taskbar covering options (<b>Do not cover by maximized windows</b>)</li><li>• hiding options (<b>Autohide</b>)</li></ul> |

### 2.1.2. NetWorks Configuration

This window allows you to configure IP protocol settings manually or receive them via DHCP. See [Figure 3](#).



Figure 3. Networks configuration

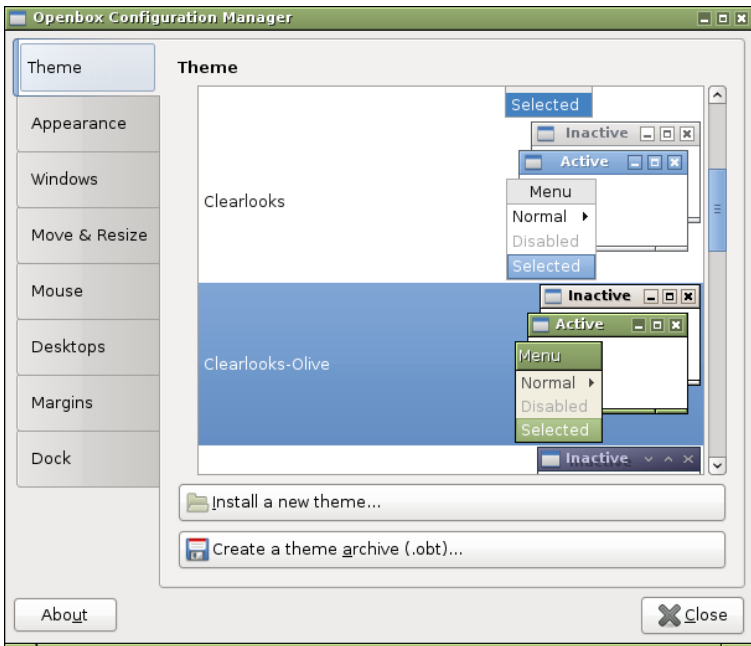




### 2.1.3. Openbox Configuration Manager

This window allows you to configure the [Openbox](#) GUI including colour schemes, desktop parameters etc. See [Figure 4](#).

**Figure 4. Openbox configuration**







### 2.1.4. X Window Configuration

This window allows you to configure the [X Window](#) system (screen resolution, type of the video driver and the mouse, keys for shifting the keyboard layout). See [Figure 5](#).

**Figure 5. X Window configuration**





## 2.2. Inbuilt Applications

This section describes applications available within the **Dr.Web LiveCD** anti-virus solution. Access to these applications can be gained via **Network** and **Utility** options of the [system menu](#).

The **Utility** option on the system menu opens the drop-down list:

- [Create Live USB](#) - create boot flash drive;
- **Leafpad** - open the inbuilt text editor (notepad);
- [Midnight Commander](#) - open the file manager;
- **Terminal** - open the command-line terminal.

The **Network** option on the system menu opens the drop-down list:

- [Firefox](#) - open the inbuilt browser;
- [Sylpheed](#) - open the inbuilt mail client.

### 2.2.1. Browser

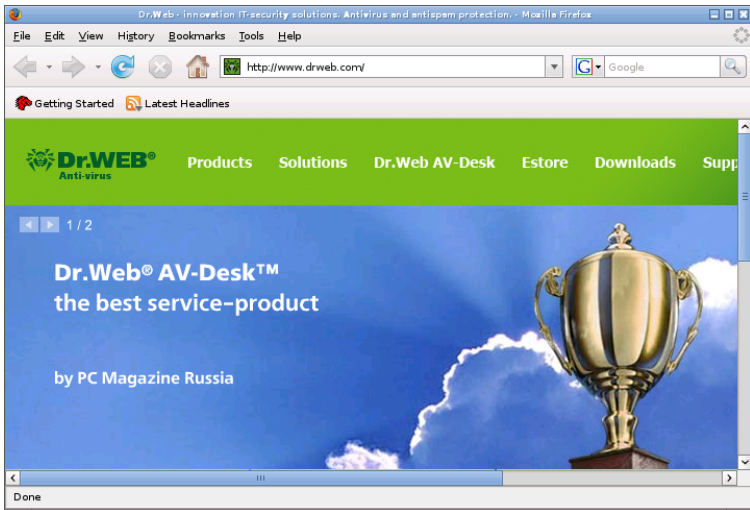
Even though your computer cannot be loaded from the hard drive, the Mozilla Firefox web browser included in **Dr.Web LiveCD** will allow you to view web sites and save the pages. See [Figure 6](#). You will be able to view the saved pages after the OS is fully restored and loaded.



An Internet connection via the Local Area Network is required to access the web pages with the inbuilt browser.

The browser default start page is the **Doctor Web** official web site.

**Figure 6. Inbuilt Browser**



### 2.2.2. Mail Client

The inbuilt **Sylpheed** mail client will enable you to carry on e-mail correspondence in full volume. See [Figure 7](#).

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

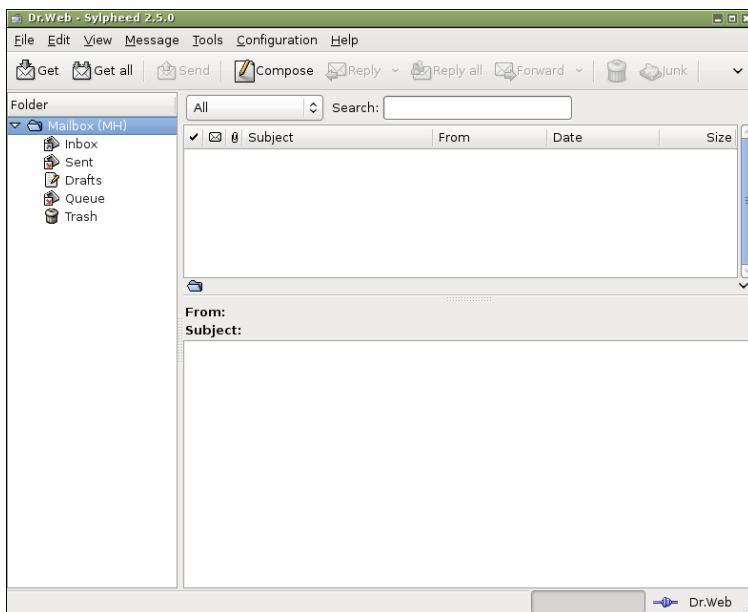
To create a new account, select **Configuration** menu -> **Create new account**. Enter all information necessary to enable mail transfer, such as sender's e-mail address, mail sending and receiving parameters (SMTP and POP3 protocols respectively), and



accompanying information.

To work with several accounts, you can create separate 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.

**Figure 7. Mail client**



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

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

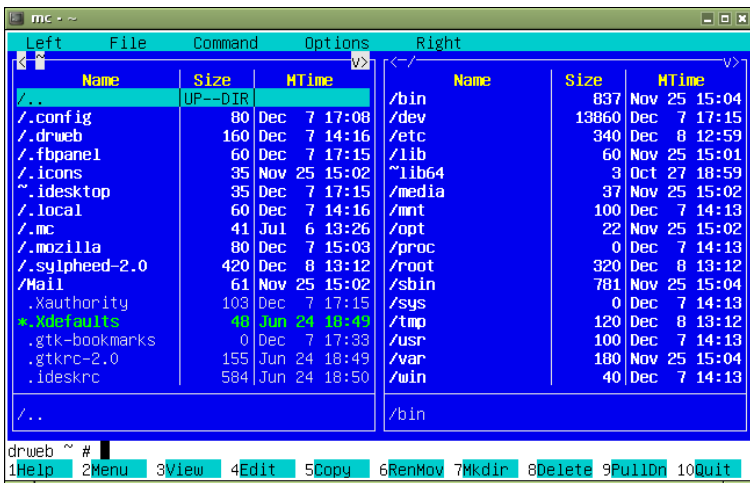


### 2.2.3. File Manager

The inbuilt **Midnight Commander** file manager is similar to the Norton Commander file manager. See [Figure 8](#). By using full screen display mode it provides an intuitive user interface to the operating system and serves as a useful tool for operations with files, suitable for users with any level of experience, from a newbie to a guru.

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

Figure 8. File manager






# 3. Using Scanner from Graphic Shell

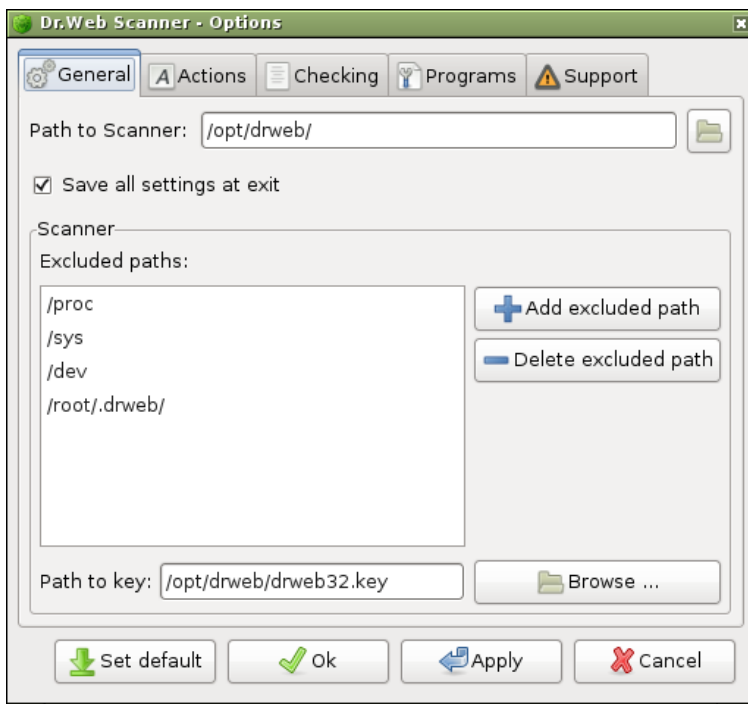
This section describes Scanner parameters and settings, and how to use it from a Graphic Shell.

## 3.1. 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, specify actions taken upon detection of infected or suspicious objects and set up Scanner interaction with the OS and various modules of the anti-virus complex. See [Figure 9](#).



**Figure 9. Scanner main options**



Main settings are divided between several tabs:

- [General](#) - general Scanner settings;
- [Actions](#) - adjustment of program's reactions upon detection of virus threats or malware;
- [Checking](#) - adjustment of scan modes for files, possibility to save current settings and restore the defaults;
- [Programs](#) - adjustment of interaction with other anti-virus components and inbuilt programs;
- [Support](#) - updates and technical support.


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



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

### 3.1.1. General Tab

By default, the main options window opens on the **General** tab. See [Figure 10](#).

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



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

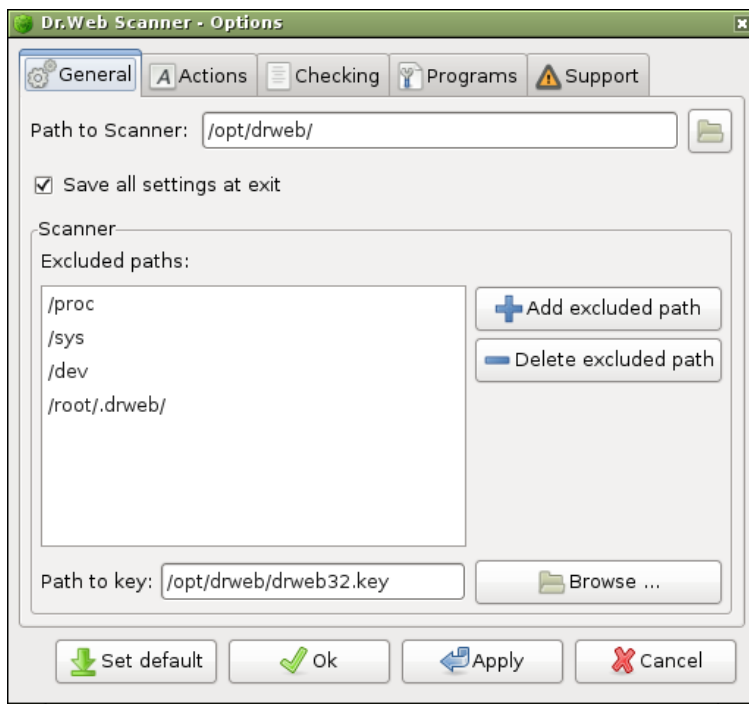
---

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 (refer to [Checking](#) tab). By default, this checkbox is selected and the settings are saved every time the Scanner is closed.







**Figure 10. General options**



You can specify the list of paths which you do not want to scan. To add a certain directory to the list of exclusions, 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** - opens the file name entry field to add a path to file (to close the field, click the button again).
-  **File System** - opens the list of **Dr.Web LiveCD** file system partitions.

As you view file system objects, the buttons for the directories



passed («bread crumbs») appear on the path selection pane (at top of the window). 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** button. To remove a shortcut, select the shortcut in the **Places** list and click **Delete** button. You can use the shortcuts for navigation through the file system.

When done with selections, click **OK** to add the selected directory to the list of objects to be excluded from scan and close the window, or click **Cancel** to close the window without saving the changes.

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.

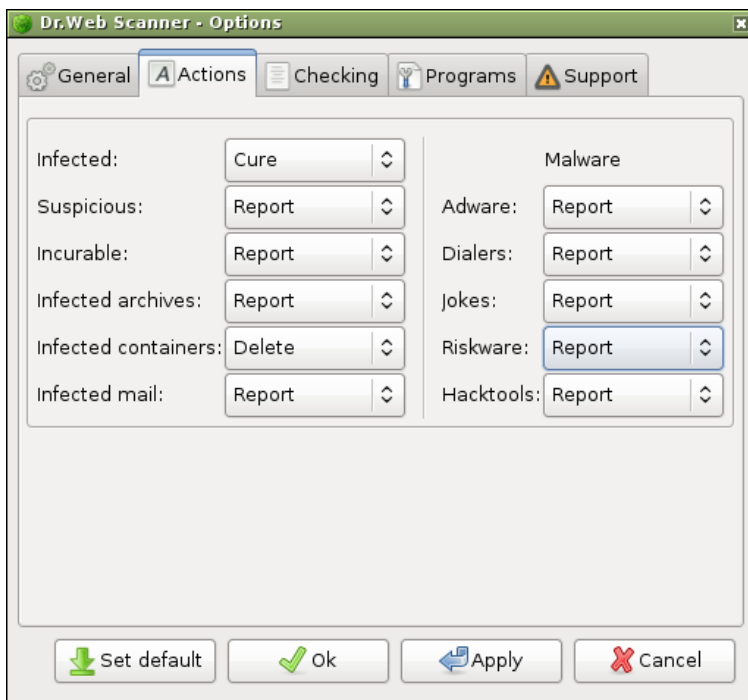
#### 3.1.2. Actions Tab

On the **Actions** tab, you can adjust reactions of the program on detected virus threats or some other malware. See [Figure 11](#).

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 select actions to be applied to the certain types of objects manually using the **Cure** and **Delete** buttons under the report field.



**Figure 11. Actions settings**



You can change the program's reaction on detected 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. Depending of the threat type these lists contain different sets of available actions:

- **Report** - report about the detected threat in the report field of the Scanner main window.
- **Cure** - try 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 can detect the following types of malware:

- **Adware** - used to display advertisements;
- **Dialers** - used to create an unauthorized connection to paid Internet sites over the dial-up modem;
- **Jokes** - may scare or distract the user;
- **Riskware** - potentially harmful programs which may be used by the intruder;
- **Hacktools** - programs intended to facilitate unauthorized access to computers.

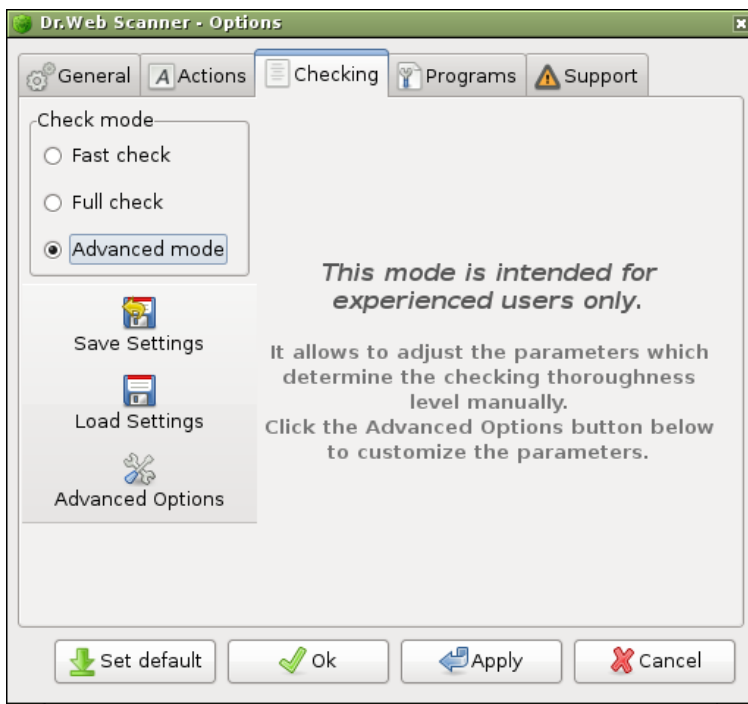
When you are done, click **Apply** to save the changes and leave the dialog box open.

### 3.1.3. Checking Tab

All main Scanner settings are located on the **Checking** tab of the Scanner main window. See [Figure 12](#). Here you can save necessary settings, load the settings from the user configuration file `drweb.ini` and access **Advance options** section with advanced Scanner settings.



**Figure 12. Checking settings**



The **Checking** tab includes

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

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



- **Fast check** - only the files which internal structure allows them to contain virus code are scanned; archives and symlink objects are not scanned; the heuristic analyzer is disabled. The scanning process in this mode 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 provides a much higher level of protection.
- **Advanced mode** - in this mode you can manually adjust the parameters which determine the check severity level. It is intended primarily for experienced users. When this mode is selected, the **Advanced Options** button becomes available in the bottom-left of the tab. Click the button to adjust 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**. The new settings will now be used each time program starts or settings are loaded from the user configuration file.



---

If you restart your system without saving the new settings, any changes made to the configuration file will be lost and all the parameters will be reset to the default, as when **Dr.Web LiveCD** was written to the disk or another medium. Please note, 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**.



When the program starts settings from the configuration file are loaded automatically. Use the **Load Settings** button only to discard the new 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 information about the configuration file refer to the **Dr.Web Anti-virus for Linux** documentation.


#### 3.1.4. Programs Tab

On the **Programs** tab, you can adjust Scanner interaction with the other components of **Dr.Web LiveCD**. See [Figure 13](#).

The **Programs** tab includes three panes:

- **Updater** - contains information necessary for Updater adjustment;
- **Mail** - used for adjustment of call options for the mail client;
- **Browser** - used for adjustment of call options 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 to start the mail client in the batch mode and edit it, if necessary. Under the entry field, you can find possible parameters to be used with this command and their descriptions.

On the **Browser** pane, you can type a command to start the



browser and edit it, if necessary. Under the entry field, you can find possible parameters to be used with this command and their descriptions.

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

### 3.1.5. 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 **Dr.Web**, and view program info. See [Figure 14](#).

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

- Start the Updater. Click **Update**.
- Open the **Dr.Web** official [Web site](#). Click **www.drweb.com**.
- Open the [Dr.Web forum](#) in the web browser window. Click **Forum**. The inbuilt browser will open at the page of the **Dr.Web** forum.
- Send a request to the technical support. Click **Request to support**. The inbuilt browser will open at the page of the **Dr.Web** 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 **Dr.Web** laboratory. Click **Send file for check**. A file manager window 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 update.





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

In case you receive a notification that the browser or the mail client is not found at the attempt to follow any of the links above, adjust properly paths to the executable files of the browser and mail client. To do this, on the **Settings** menu select **Options -> Programs** and enter necessary data.

**Figure 14. Support tab**





## 3.2. Advanced Options

Experienced users may adjust scanning parameters by themselves in the [Advanced options](#) section.

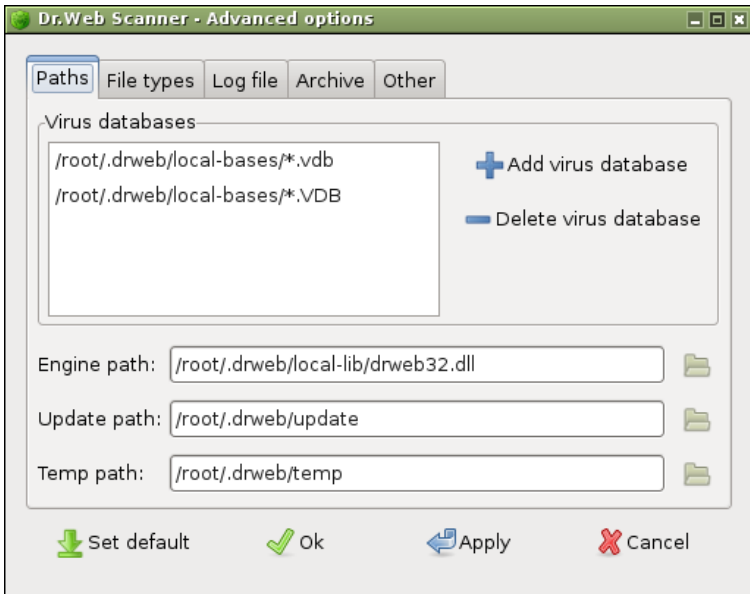
### To set individual scanning parameters

1. On the Scanner **Settings** menu, select **Options** and then select the **Checking** tab.
2. On the **Check mode** pane, select **Advanced mode**.
3. The **Advanced Options** button in the bottom-left of the window becomes available. Click the button to access the settings.
4. Or directly from the Scanner **Settings** menu select the **Advanced mode** option button.
5. **Advanced options** item in **Settings** menu becomes available. Select it to access the settings.

The advanced options menu allows to adjust manually paths to directories used by the various Scanner components, specify types of files for scan, set up logging procedure, etc. See [Figure 15](#).



**Figure 15. Scanner advanced options**



The advanced options are divided between several tabs:

- [Paths](#) - specify the paths to main Scanner modules.
- [File Types](#) - set the file types to be checked.
- [Log File](#) - set logging parameters.
- [Archive](#) - set limitations to actions to be applied to archives for safety reasons.
- [Other](#) - adjust parameters managing computer workload, select Updater's timeout and enable the heuristic analyzer.

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

- **Set default** - discard the user settings and set the default ones;
- **Ok** - save the changes and return to the main window of the Scanner;

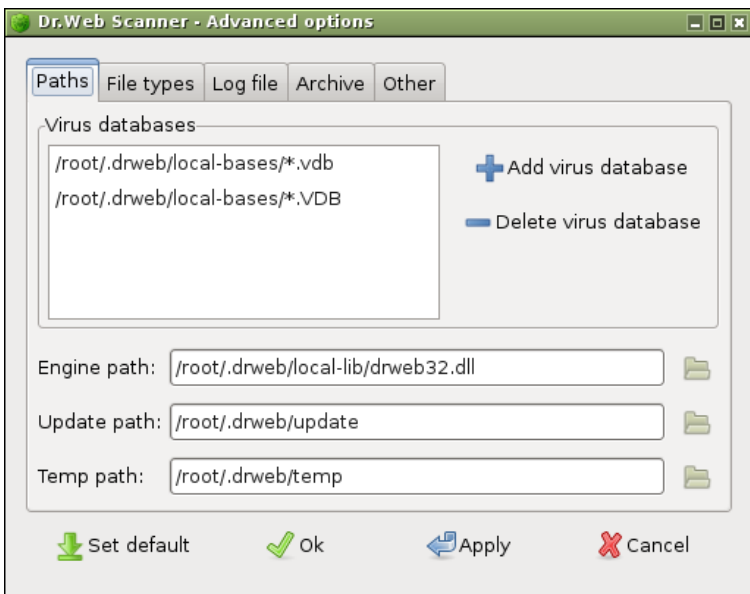


- **Apply** - save the changes and stay in the settings window;
- **Cancel** - return to the main window of the Scanner and discard the changes.

#### 3.2.1. Paths Tab

By default, the advanced options window opens on the **Paths** tab. See [Figure 16](#).

**Figure 16. Paths tab**




In the **Virus databases** list the location of databases with [virus records](#) is specified. By default, the databases are located in the directory specified during the program installation. The Updater module automatically puts updated databases to this directory. However, if you wish to connect some 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 also specify only one \* symbol to point to 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 paths to the engine, the update directory and the temporary files directory in the corresponding input fields, or select these paths via the file system explorer by clicking the button  next to the relevant field.

## 3.2.2. File Types Tab

On the **File Types** tab you can set up restrictions on the types of files to be checked by the Scanner. See [Figure 17](#).

On the **Scan mode** pane set the selection method for files to scan using the group of option buttons:

- **All** - all files are scanned regardless of their types and internal structure. This mode is set by default when you select **Full check** on the [Checking](#) tab of the Scanner settings section.
- **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 necessary extension in the opened window and then click **Apply**. 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 which internal structure allows them to contain 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 section.

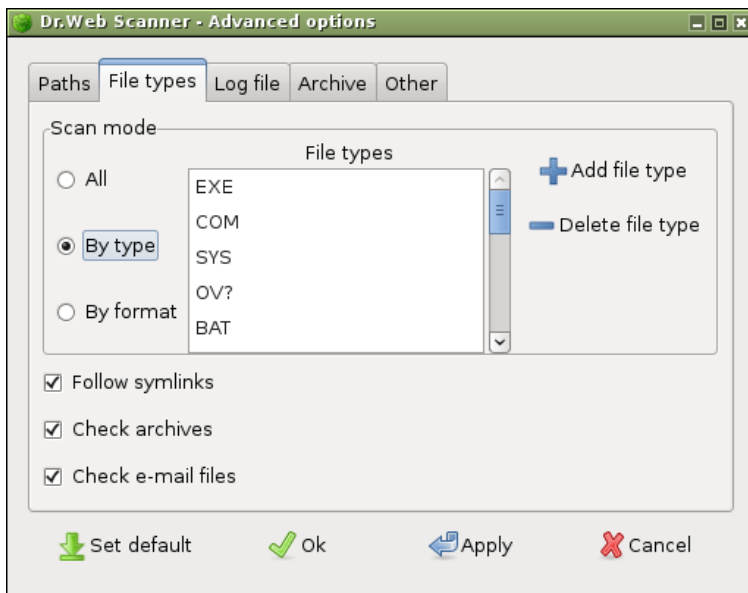
Below the pane you can select the following options to set up additional restrictions for the scanning process:

- Select the **Follow symlinks** checkbox if you want the Scanner to check the files, symbolic links to which are included into the scan.
- Select the **Check archives** checkbox if you want the Scanner to unpack archives and check the files inside (in the **By format** mode archives should have a suitable format; in the **By type** mode, the extension of both the archive and the scanned file should be in 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 (these modes are available on the [Checking](#) tab of the settings section).




Figure 17. File types tab



### 3.2.3. Log File Tab

On the **Log file** tab you can adjust logging parameters. See [Figure 18](#).

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 system 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 between the following priority levels for logging: **Info | Notice | Alert | Warning.**

A selected **Limit log file size** checkbox instructs that the log file must not exceed the size specified in the entry field to the right. 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.

---

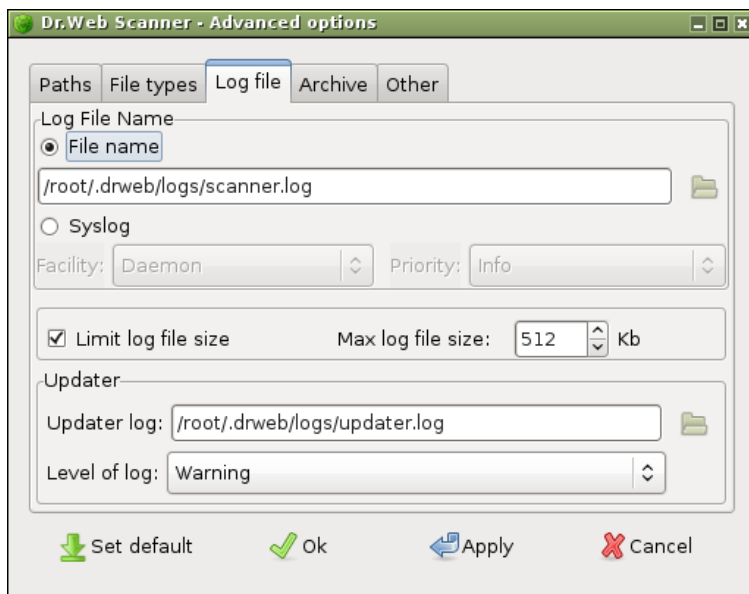
In the **Updater** section you can edit the path to the log file of the updating utility. Specify it in the **Log file** entry field or click the button  and choose the path via the file system explorer.

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





Figure 18. Log file tab



### 3.2.4. Archive Tab

On the **Archive** tab you can set limitations to actions which will be applied to archives for safety reasons. See [Figure 19](#).

The parameters on the **Archive** tab are designed to protect the Scanner from «mailbomb» attacks. They specify limiting 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:

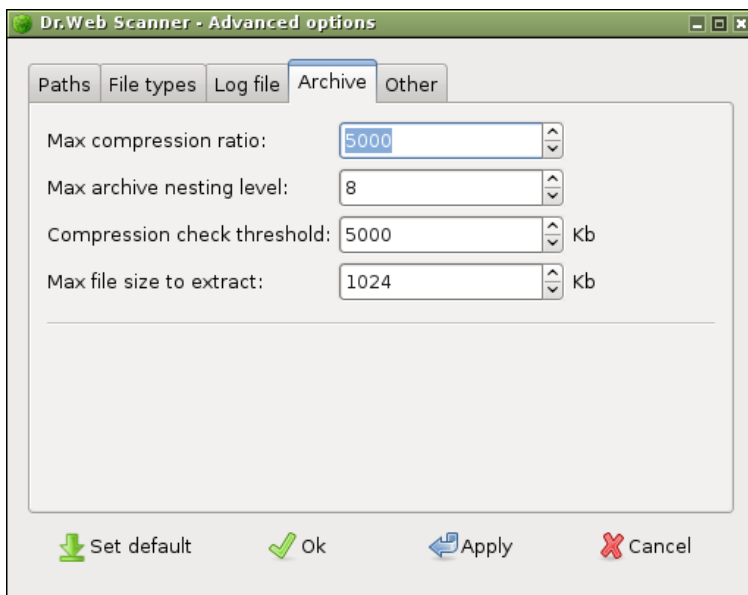
- **Max compression ratio** - by default is set to 5000;
- **Max archive nesting level** - by default is set to 8;
- **Compression check threshold** - by default is set to 5000



Kbytes. Smaller archives are scanned regardless of the compression ratio;

- **Max file size to extract** - by default is set to 1024 Kbytes. Larger archives will not be unpacked.

**Figure 19. Archive tab**



### 3.2.5. 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 20](#).

In the **Scan priority** group of option 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



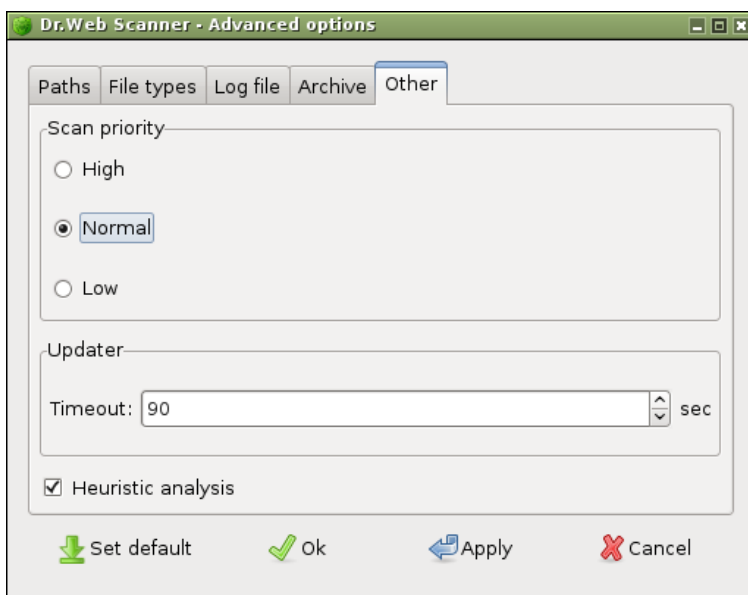
server.

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 20. Other tab**



Click an area for details

## 3.3. Antivirus Scan

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



### 3.3.1. Starting a Scan

**Dr.Web Scanner for Linux** can 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 launch the Scanner main window opens. See [Figure 21](#).

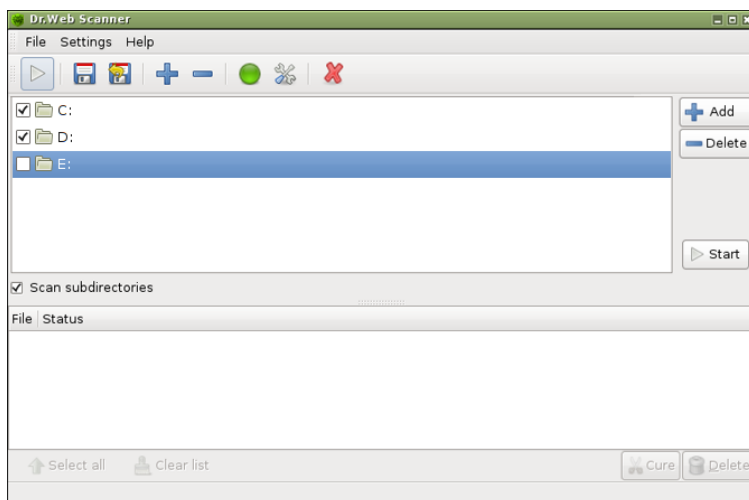
The Scanner allows to check all types of Windows partitions (FAT, FAT32, NTFS) for viruses. By default, all available partitions of the hard drive are selected for scanning.



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

By default, all the subdirectories in selected directories are scanned. If you want to scan only files in certain selected directories and partitions, excluding the content of the enclosed directories (in spite of the possible infection), clear the **Scan subdirectories** checkbox.

**Figure 21. Main Scanner window**



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

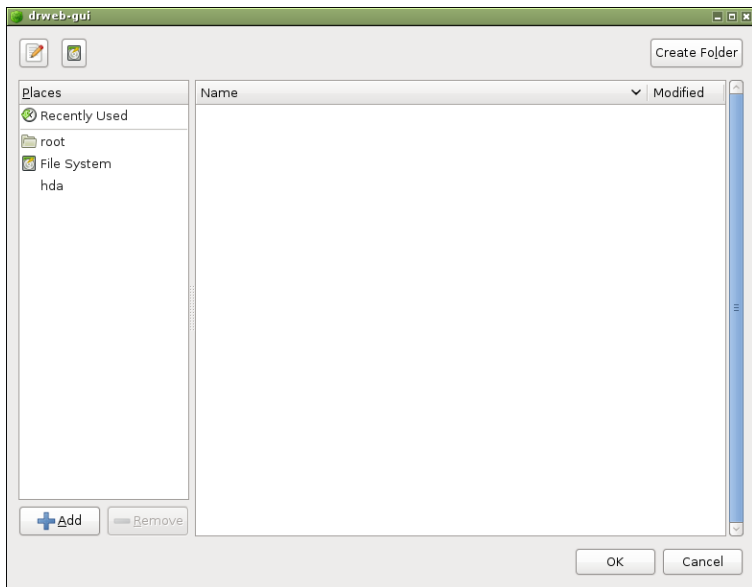


The **Delete** button becomes available once you select an object.

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

When you click **Add**, a window opens, where you can select objects to scan. See [Figure 22](#).

**Figure 22. File Manager window**



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.



As you view file system objects, the buttons for the directories passed («bread crumbs») appear on the path selection pane (at top of the window). 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** button. To remove a shortcut, select the shortcut in the **Places** list and click **Delete** button. You can use the shortcuts for navigation through the file system.

When done with selections, click **OK** to add the selected directory to the list of objects for scan and close the window, or click **Cancel** to close the window without saving the changes.

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

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

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

You can set additional parameters before scan, such as: scan mode (check severity level), actions over detected objects, etc. For more information on the **Scanner** settings, please refer to the [Main Options](#) section.

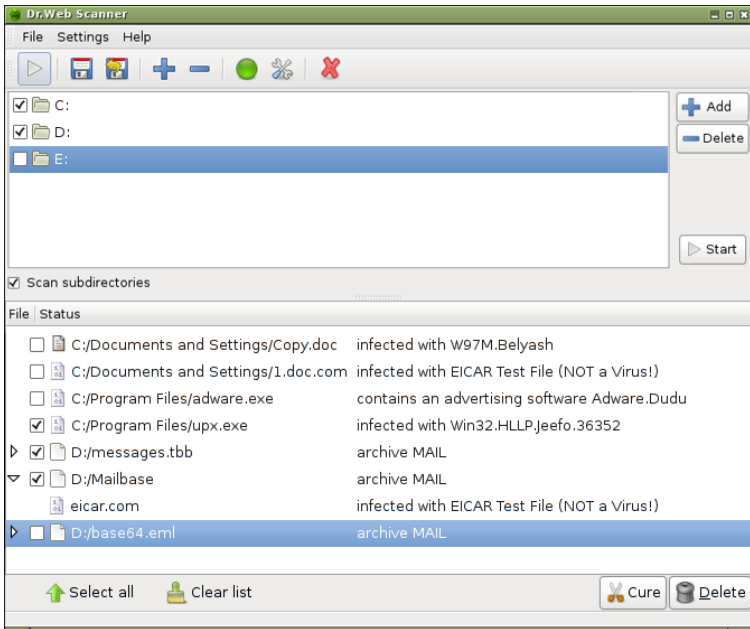
### 3.3.2. Scan Results

Scan results are shown as a table in the bottom of the Scanner main window. See [Figure 23](#). There you can find information on infected and suspicious objects found during the scan: their location, their reasons to be included into the current selection and actions performed by the program over these objects.

Items in the list of detected objects are displayed in a hierarchical order: if a virus is found inside an archive, then the archive is displayed as a node, which contents you can expand and collapse.



**Figure 23. Scan results**



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 there some other action, different from **Report**, was specified for a certain type of detected objects on the [Actions tab](#) of Scanner settings section, then the result of this action will be shown in the **Status** column.

When the **Cure** action is assigned for an object, and this object appears 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**.





## 4. Using Console Scanner

This section helps you get started using the Console Scanner.

### 4.1. Starting a Scanning

After launching **Dr.Web LiveCD** in the safe mode, the **Start Menu** appears. See [Figure 24](#).

Figure 24. Start Menu



Using the arrow keys, select one of the following items from 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;
- **Choose Language** - to change the interface language;
- **Xorg Configuration** - to adjust parameters of the X Window system, if it was not configured automatically;
- **Network Configuration** - to adjust network parameters, if the network was not configured automatically;
- **Report Bug** - to [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. To run console Scanner you can use the following command:

```
$ /opt/drweb/drweb -  
path <path> [command line parameters]
```

where <path> - is the path to scanned directory or the mask for checked files.

When **Scanner** is started only with <path> argument without any parameters specified, it scans the specified directory using the default set of parameters. In the following example drive **C:** is being checked:

```
$ /opt/drweb/drweb -path /win/C:
```



## 4.2. Command Line Parameters

**Dr.Web Scanner** supports numerous command line parameters. They are separated from specified path by white space and are prefixed by hyphen «-». To get complete list of parameters, start `drweb` component with `-?`, `-h` or `-help` parameters.

Main program parameters can be classified in the following way:

- scan area parameters;
- diagnostics parameters;
- actions parameters;
- interface parameters.

Scan area parameters determine where the virus check must be performed. They include:

- `path` — specify path for scan. Several paths can be specified in one parameter;
- `@[+] <file>` — check objects listed in the specified file. Plus «+» instructs Scanner not to delete files from the list of objects after scan is completed. List file may contain paths to directories that must be scanned regularly, or list of files to be checked only once;
- `sd` — recursive search and scan of files in subdirectories starting from the current directory;
- `fl` — follow links, both to files and directories. Links causing loops are ignored;
- `mask` — ignore masks for file names.

Diagnostics parameters determining what types of objects must be scanned for viruses:

- `al` — scan all files on specified drive or in specified directory;
- `ar[d|m|r][n]` — scan files in archives (ARJ, CAB, GZIP, RAR, TAR, ZIP, etc.).  
`d` - delete, `m` - move, `r` - rename archives containing infected objects, `n` - archiver name output disabled.  
Archives can be in simple (`*.tar`) or compressed forms (`*`).



`tar.bz2, *.tbz);`

- `cn[d|m|r][n]` — scan files in containers (HTML, RTF, PowerPoint,..).  
`d` - delete, `m` - move, `r` - rename containers containing infected objects, `n` - container type output disabled;
- `ml[d|m|r][n]` — scan files in mailboxes.  
`d` - delete, `m` - move, `r` - rename mailboxes, containing infected objects; `n` - mailbox type output disabled;
- `up[n]` — scan executable files packed with LZEXE, DIET, PKLITE, EXEPACK;  
`n` - packer type output disabled;
- `ex` — diagnostics using file masks (see `FilesTypes` parameter in configuration file);
- `ha` — heuristic analysis (search for unknown viruses).

Actions parameters determine what actions must be performed if infected or suspicious files are detected. They include:

- `cu[d|m|r]` — cure infected files: `d` - delete, `m` - move, `r` - rename infected files;
- `ic[d|m|r]` — actions for incurable files: `d` - delete, `m` - move, `r` - rename incurable files;
- `sp[d|m|r]` — actions for suspicious files: `d` - delete, `m` - move, `r` - rename suspicious files;
- `adw[d|m|r|i]` — actions for files containing adware: `d` - delete, `m` - move, `r` - rename, `i` - ignore;
- `dls[d|m|r|i]` — actions for dialers: `d` - delete, `m` - move, `r` - rename, `i` - ignore;
- `jok[d|m|r|i]` — actions for joke programs: `d` - delete, `m` - move, `r` - rename, `i` - ignore;
- `rsk[d|m|r|i]` — actions for potentially dangerous programs: `d` - delete, `m` - move, `r` - rename, `i` - ignore;
- `hck[d|m|r|i]` — actions for hacktools: `d` - delete, `m` - move, `r` - rename, `i` - ignore;

Interface parameters configure **Scanner** report output:

- `v, version` — output information about product and



**Engine** versions;

- `ki` – output information about key file and its owner (in UTF8 encoding only);
- `foreground[ yes| no]` – enable **Scanner** to run in foreground or in background;
- `ot` – output information to standard output (`stdout`);
- `oq` – disable information output;
- `ok` – display «Ok» for not infected files;
- `log=<path to file>` – logging to specified file;
- `ini=<path to file>` – path to alternative configuration file;
- `lng=<path to file>` – path to alternative language file.

You can use hyphen «-» postfix to disable the following parameters:

```
-ar -cu -ha -ic -fl -ml -ok -sd -sp
```

For example, if you start **Scanner** with the following command:

```
$ drweb -path <path> -ha-
```

heuristic analysis (enabled by default) will be disabled.

By default (if **Scanner** configuration was not customized and no parameters were specified) **Scanner** starts with the following parameters:

```
-ar -ha -fl- -ml -sd
```

Default **Scanner** parameters (including scan of archives, packed files and mailboxes, recursive search, heuristic analysis, etc.) is sufficient for everyday diagnostics and can be used in typical cases. You can also use hyphen «-» postfix to disable some parameters, as it was explained above.

Disabling scan of archives and packed files will significantly decrease antivirus protection level, because in archives (especially, self-extracting) enclosed in e-mail attachments viruses are distributed. Office documents potentially susceptible to infection with macro viruses (Word, Excel) are also dispatched via e-mail in archives and containers.



When you run **Scanner** with default parameters, no **cure** actions and no actions for incurable and suspicious files are taken. For these actions to be performed, you must specify corresponding command line parameters explicitly.

Set of actions parameters may vary in particular cases. We recommend the following:

- `cu` — cure infected files and system areas without deletion, moving or renaming infected files;
- `icd` — delete incurable files;
- `spm` — move suspicious files;
- `spr` — rename suspicious files.

When **Scanner** is started with **Cure** action specified, it will try to restore the previous state of infected object. It is possible only if detected virus is known virus, and cure instructions for it are available in virus database, though even in this case cure attempt may fail if infected file is seriously damaged by virus.

If infected files are found inside archives they will not be cured, deleted, moved or renamed. To cure such files you must manually unpack archives to the separate directory and instruct **Scanner** to check it.

When **Scanner** is started with action **Delete** specified, it will delete all infected files from disk. This option is suitable for incurable (irreversibly damaged by virus) files.

Action **Rename** makes **Scanner** replace file extension with a certain specified extension («\*. #?? » by default, i.e. first extension symbol is replaced with «# » symbol). Enable this parameter for files of other OS (e.g., DOS/Windows) detected heuristically as suspicious. Renaming helps to avoid accidental startup of executable files in these OS and therefore prevents infection by possible virus and its further expansion.

With action **Move** enabled **Scanner** will move infected or suspicious files to the quarantine directory.



## 5. Creating Boot Flash Drive

**Dr.Web LiveCD** may be used as a portable operating system customized according to the certain user needs to enable access to 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 purpose the `CreateLiveUSB` command is used.



---

In spite of the fact that `CreateLiveUSB` does not change or delete the content of devices, it is recommended to save the files from the flash drive you are going to use to another data carrier, before running the command.

---

To enable load of **Dr.Web LiveCD** it is not required to 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` directory. `CreateLiveUSB` may change the configuration of the partitions of the flash drive, if necessary; the original configuration is saved to the `/boot/partition.backup` file. `CreateLiveUSB` copies the MBR on the flash drive; the original master boot record is saved to the `/boot/mbr.backup` file. See [Figure 25](#).



Figure 25. Create LiveUSB


```
Create LiveUSB

device | MBR | size | busy | type
-----|----|-----|-----|-----
sdf1 | boot | 238.06M | 35% | FAT16
sdf2 | | 238.06M | 1% | W95 FAT32 LBA
sdf3 | | 238.06M | 1% | VFAT
sdf4 | | 476.34M | 0% | W95 FAT16 LBA

Found 4 partitions

Select partition, press Esc to exit
```

### To create a boot flash automatically


1. Connect the flash drive. It takes maximum ten seconds for a connection to be registered.
2. In the graphic shell, double-click the **Create Live USB**  icon on the desktop, or run `create_usb` command in the console.
3. **CreateLiveUSB** will detect all available partitions automatically.
4. Select the suitable partition and press ENTER.
5. Files will start to copy automatically.





## 6. Reporting a bug

If you use graphic shell, then to send a report about some bug in program operation you must do the following:

- pass to the main options section of the **Scanner** using the **Options** button  on the toolbar or using the menu in the **Scanner** main window: **Settings -> Options**;
- in the main options section select **Support** tab;
- press the **Bug report** button on this tab;
- after that an inbuilt mail client will be started with the message template already opened;
- in the **Subject** field give a brief description of the problem encountered, and in the message body describe the problem in every detail, including the steps to be made to reproduce it;
- send the message using the default e-mail account.

If you use console, then to send a report about a bug use the following algorithm:

- using the arrow keys, select the **Report Bug** items from the **Start Menu** and press **ENTER**;
- a console text editor ([nano](#)) will open, where you can describe the encountered problem;
- after finishing the description, press **CTRL+X** to exit the text editor;
- before exit you will be prompted to make a decision whether you want to send the bug report or not, and press the corresponding key (**Y** - to send a report, **N** - to discard it).

