Dr.WEB®
LiveUSB

Defend what you create

User Manual

Dr.Web® LiveUSB
Version 6.0.2
User Manual
08.11.2012

Doctor Web 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

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

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

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards. State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

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

Table of Contents

1. Introduction

Dr.Web® LiveUSB is a software product based on the standard **Dr.Web** anti-virus scanner for GNU/Linux systems. It allows to restore the system when booting of a computer from a hard drive is impossible due to high virus activity. Using the emergency anti-virus assistance disk, you can clean your computer from infected and suspicious files, attempt to cure infected objects, and restore and edit the Windows registry.

Thus, **Dr.Web LiveUSB** provides access to computer resources both when it is impossible to boot the system from a hard drive and when there exists a need in a convenient customizable interface (settings are saved only if you use snapshots).

Dr.Web LiveUSB is a USB flash drive with a portable Linux-based operating system and built-in 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.

Dr.Web LiveUSB is distributed as the **drwebliveusb.exe** tool for creating a bootable USB drive. The tool must be launched in Windows OS. For more information on this tool, see section 1.5.

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

- standard mode;
- advanced mode that offers more options and provides access to a command-line interface or Graphics mode.

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.

During its operation **Dr.Web LiveUSB** uses a temporary RAM drive created when the system boots. Thus, all changes in program settings stored on the RAM drive will be lost when the computer reboots.

The **Quarantine** folder is also created on the RAM drive, so backup copies saved to **Quarantine** will be lost unless they are saved to one of the computer hard disk drives (physical disk drives) or a removable media.

To save the changes, use a snapshot (available in Advanced mode only).

1.1. Dr.Web Anti-Virus Protection

Dr.Web® LiveUSB 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, 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 Security Suite**)
- Protection of workstations (**Dr.Web Security Space 6.0**, **Dr.Web Anti-virus for Windows 6.0**, **Dr.Web Anti-virus for Linux**, **Dr.Web Console Scanners**);
- Protection of file servers (**Dr.Web for Windows servers**, **Dr.Web for Unix servers**, **Dr.Web for Novell NetWare servers**);
- 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 LiveUSB** anti-virus solution:

Specification	Requirement
CPU	i386 processor
RAM	Minimum 256 MB (512 MB if virtual memory on hard drive can not be used)
Hard disk space	Minimum 512 MB when Snapshots are used
Drives	USB flash drive with minimum 256 MB of free space. If a USB flash drive is also will be used to store Snapshots, minimum 512 MB of additional free space on it is required
Other	Video card, monitor, keyboard, and mouse are required

1.3. Dr.Web Anti-virus for Linux

Dr.Web Anti-virus for Linux is designed to protect computers of GNU/Linux users from viruses and other threats.

The main program components (anti-virus engine and virus databases) are considered extremely effective and have low system requirements. They are cross-platform, which enables **Dr.Web** specialists to create anti-virus solutions for different operating

systems (OS). The components of **Dr.Web Anti-virus for Linux** and virus databases are constantly updated to provide up-to-date protection. For additional protection against unknown viruses **Dr.Web Anti-virus for Linux** uses heuristic analyzer.

Dr.Web Anti-virus for Linux consists of the following components, each of them has its own set of functions:

Component	Functions
Dr.Web Control Desk for Linux	The module helps you to control **Dr.Web Anti-virus for Linux** in GUI mode. Allows to set scanning options, launch and stop scanning, initiate updates and work with **Quarantine**.
Scanner	The main component for virus detection, which provides you with the following features: • full or custom scanning at request; • neutralization of detected threats (curing, deleting or moving to **Quarantine**). User can manually select a necessary option to detected threats of a particular type on the Anti-virus settings page.
Quarantine	The special catalogue that serves for isolation of malicious files and other threats to protect the system from them.
Updater	This component is used to update virus databases and other Anti-virus components via the Internet.
License manager	This component helps to work with key files. It allows to receive a demo or license key file, review information about it and renew a license.

Flexible **Dr.Web Anti-virus for Linux** settings allow to set sound notifications on different events, the maximum **Quarantine** size and list files and folders which you want to exclude from scanning.

For details on how to use **Dr.Web Anti-virus for Linux**, see the program Help.

To ensure maximum scanning effectiveness, virus databases are to be updated. An Internet connection is required for an update. For details on how to set up a connection, see Network configuration.

1.4. What is New in Dr.Web® LiveUSB

Dr.Web® LiveUSB 6.0.2 features the following enhancements:

1. Editing of **Windows** registry. On startup, **Dr.Web® LiveUSB** automatically finds the **Windows** registry and exports it into a folder in the root directory. That enables to edit the registry keys as files and folders through the File manager;
2. Utility that allows to repair **Windows** registry problems that occurred due to malicious activity;
3. Updated antivirus **Scanner** provides the following new features:
   - Multithread scanning;
   - Faster processing of scanning request, as it is not required to update virus databases before each scanning session;
   - Scanning of disk boot sectors.
4. When the **Report Bug** item on the **Start Menu** is selected, **Dr.Web® LiveUSB** automatically generates a bug report including MBR dumps that are also copied to the system `/tmp` folder;
5. Option to select the interface language on the Start Boot menu. The following two languages are available at the current moment: Russian and English.
6. Other enhancements:
   - **Linux kernel** version is updated form 2.6.30 to 3.2.12;
   - New module that enables to work with the **exFat** file system;
   - Support for USB flash drives with the **NTFS** file system;
   - Support for **NTFS ADS**;

- Updated and expanded list of devices supported by **Dr.Web® LiveUSB**;
- Updated graphics card drivers. The enhancement enables the new version of **Dr.Web® LiveUSB** to support wide range of video adapters.

1.5. Creating Dr.Web LiveUSB Bootable Flash Drive

Introductory remarks

You can create an original copy of **Dr.Web LiveUSB** to boot it from a USB flash drive. To do this, use **drwebliveusb.exe** which is a special tool for Windows OS. If necessary, you can create a new bootable copy in the **Dr.Web LiveUSB** with the **CreateLiveUSB** utility.

USB flash requirements

To create a boot copy of **Dr.Web LiveUSB**, you can use any USB flash drive with enough free space (not less than 256 MB is required).

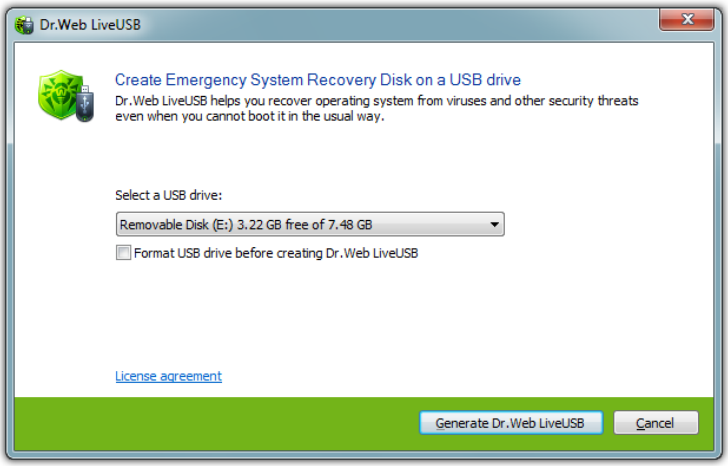
In spite of the fact that **drwebliveusb.exe** does not change or delete the content of drives, it is recommended to save the files of the flash drive you are going to use on another data carrier before launching the command.

All **Dr.Web LiveUSB** files are written to the `/boot` directory. The utility may change the configuration of the flash drive partitions, if necessary; the original configuration is saved to the `/boot/partition.backup` file. The **drwebliveusb.exe** utility copies the MBR on the flash drive; the original master boot record is saved to the `/boot/mbr.backup` file.

To create a boot flash drive

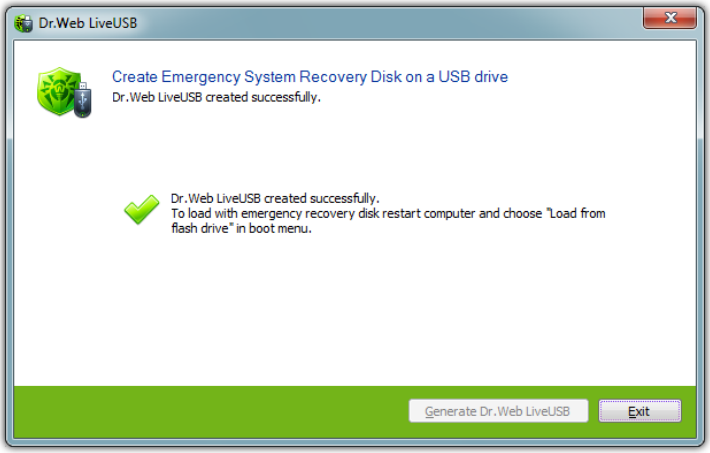
1. Connect the flash drive to the computer. It takes maximum ten seconds for a connection to be registered.

2. Launch the executable file of **drwebliveusb.exe**.
3. The program will find all flash drives available in the system. Select a required drive. You can also format it (before the process starts, the program displays a warning message that all data stored on the drive will be deleted).



To view the **License agreement**, click the corresponding link in the window (the default browser opens and displays the text of the **License agreement**).

4. To create a bootable flash drive, click **Generate Dr.Web LiveUSB**.
5. File copying will be started automatically.



6. To exit the program, click **Exit**.

To use the created copy of **Dr.Web LiveUSB**, reboot the computer without disconnecting the flash drive (to boot a computer from the USB flash drive, you may need to change the corresponding BIOS settings).

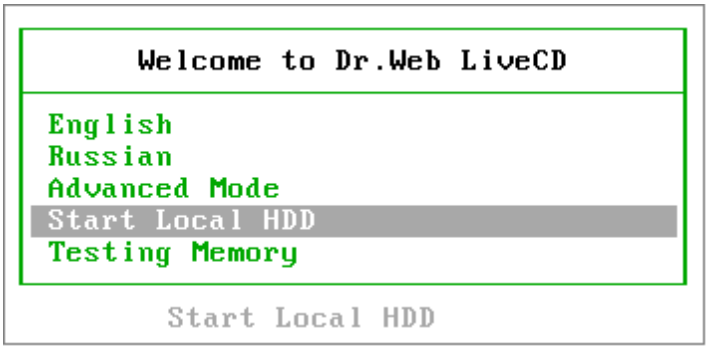
2. Launching Dr.Web LiveUSB

Before You Begin

Make sure that your computer is set up to boot from a USB flash drive on which **Dr.Web LiveUSB** is stored. Insert the data carrier and start or reboot the computer.

Start Boot Menu

At start the following menu appears where you can select the load mode:



Using the arrow keys on your keyboard (and), select one of the following options and press ENTER:

- To launch **Dr.Web LiveUSB** Graphic Shell, select one of the languages to use in the interface:
  - **English**,
  - **Russian**.
- To launch Advanced Mode of **Dr.Web LiveUSB**, select **Advanced Mode**.
- To boot your computer from the hard drive without launching **Dr.Web LiveUSB**, select **Start Local HDD** (an attempt to launch the system from the 0 partition of the 0 drive (hd0, 0)).

- To test memory (recommended when your computer is extremely unstable and restarts at random), select **Testing Memory**. After this item is selected, **Testing Memory program** starts. On completion of memory testing, the computer reboots.

In case the menu item is not chosen during 15 seconds, your computer will attempt to launch OS from the hard drive (menu item **Start Local HDD** selected by default).

Press `TAB` to edit each option manually.

During its operation **Dr.Web LiveUSB** uses a temporary RAM drive created when the system boots. Thus, all changes in program settings stored on the RAM drive will be lost when the computer reboots.

The **Quarantine** folder is also created on the RAM drive, so backup copies saved to **Quarantine** will be lost unless they are saved to one of the computer hard disk drives (physical disk drives) or a removable media.

To save the changes, use a snapshot (available in Advanced mode only).

3. Dr.Web LiveUSB Graphic Shell

The **Dr.Web® LiveUSB** software includes a graphic shell with a window-based interface similar to Linux GUI. After the **Dr.Web LiveUSB** Graphic Shell has been loaded, you see a standard desktop.

Desktop Elements

The following picture shows a **Dr.Web® LiveUSB** GUI desktop:

The default desktop with the **Dr.Web** trademark for the background contains icons of applications included in **Dr.Web LiveUSB**.

The taskbar (a horizontal bar at the bottom of the screen) contains:

	System menu button
	Quick Launch icons for inbuilt applications
	Desktop switching icons
	Icons of currently used applications
	Dr.Web Anti-virus for Linux icon and system clock

Dr.Web LiveUSB 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** and **nano** text editors;
- **ePDFViewer**;
- Utilities:
  - **CureRegistry**;
  - **NetWorks configuration**;
  - **Create LiveUSB**.

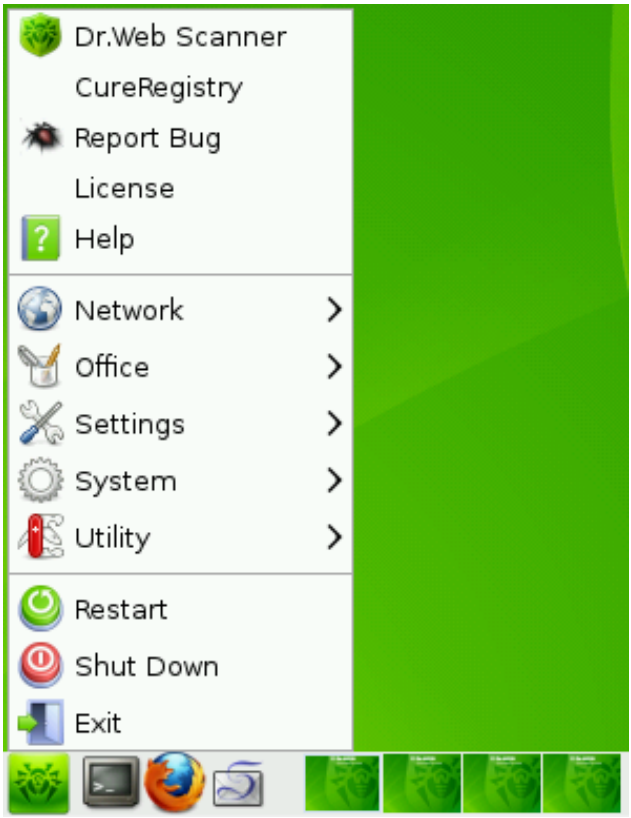
You can start the main components by

- double-clicking the icon of the corresponding component on the desktop (by default, basic components are represented on the desktop);
- clicking the icon of the corresponding component on the taskbar;

- selecting the corresponding component on the system menu.

System menu

To open the system menu, click the system menu button on the taskbar. The following picture shows the system menu:



System menu items:

Menu item	Description
Dr.Web Scanner	Opens the **Dr.Web Control Desk for Linux** window

Menu item	Description
CureRegistry	Starts the curing registry utility for **Windows**
Report Bug	Starts **Sylpheed** mail client and generates a bug report form (**Doctor Web** development team is automatically specified as a recipient)
Lisence	Starts **nano** text editor and opens an end-user license agreement
Help	Starts **Firefox** and opens **Dr.Web LiveUSB** Help
Network	Contains a submenu that provides access to: • **Firefox** Web browser; • **Sylpheed** mail client.
Office	Contains a submenu that provides access to: • PDF viewer.
Settings	Contains a submenu that provides access to the following utilities: • **Adobe flash player** settings; • **Openbox Configuration Manager**, which allows you to configure the **Openbox GUI**; • System menu configuration; • Network configuration.
System	Contains a submenu that provides access to the following applications: • **Dr.Web Anti-virus for Linux**; • Terminal - opens the **command-line terminal**
Utility	Contains a submenu that provides access to the following utilities: • **Leafpad** text editor; • **Midnight Commander** file manager; • **Create LiveUSB** that allows to create a boot flash drive
Restart	Reboots the computer
Shut Down	Shuts down the computer
Exit	Exits the graphic shell and opens the Start menu of Advanced mode

Launching Dr.Web Antivirus

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

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

3.1. Basic Functions

In Graphics mode you can:

1. Scan the system for viruses

Dr.Web Anti-virus for Linux allows to scan the system for viruses or malware. Working with **Dr.Web Anti-virus for Linux** is described in the following sections:

- in the graphic shell – section 3.2;
- in the command-line interface – section 5.

2. Restore the Windows registry

The special **CureRegistry** utility that is included into **Dr.Web® LiveUSB** allows to restore the Windows registry.

Working with the utility is described in the section 6.2.

3. View, edit, create and delete files

Midnight Commander is a file manager that allows to work with files and folders: view, edit, create, and delete them.

Working with the file manager is described in the section 3.4.3.

4. Create, view and edit text files

Leafpad and **nano** text editors allow to work with text files, including viewing and editing text files.

Working with the **Leafpad** text editor is described in the section 3.4.5.

Working with the **nano** console text editor is described in the section 3.4.6.

5. Edit the Windows registry

Midnight Commander allows to view and edit the Windows registry. When launching **Dr.Web LiveUSB**, the registry branches are exported into the file system (into the **/reg** folder). That enables to work with registry keys as with ordinary text files: view their contents and edit them when necessary.

Working with the **Midnight Commander** file manager is described in the section 3.4.3.

Despite the fact that working with Windows registry is similar to working with files and folders, registry branches are not folders, and you must not copy ordinary files and folders into them.

It is also not recommended to delete, remove, or rename registry branches and registry keys as that can lead to total or partial malfunction of the operating system (or some of its components) because of a damaged registry.

6. Create Boot Flash Drive

Dr.Web LiveUSB includes a special **Create LiveUSB** utility that enables to create a boot flash drive. The boot flash drive can be used as an emergency boot device, like **Dr.Web LiveUSB**.

Working with **Create LiveUSB** is described in the section 6.1.

7. Configure network settings

Network configuration is necessary to download updates to virus databases from the Internet. You can configure network by the special utility that operates in the console. It is recommended to adjust network settings only when configuration created automatically on **Dr.Web LiveUSB** booting does not work.

Working with the **NetWork Configuration** utility is described in the section 6.3.

8. Configure the graphic shell

A special utility of the graphic shell allows to configure the appearance of the GUI and system menu.

Working with the utility is described in the section 3.3.

9. View Web pages

With the inbuilt **Firefox** browser, you can view Web pages and **Dr. Web LiveUSB** Help.

Working with the **Firefox** browser is described in the section 3.4.1.

10. Send e-mail messages

The inbuilt **Sylpheed** mail client allows you to carry on e-mail correspondence in full volume (create, view, receive, and send e-mail messages). This component also enables you to contact **Doctor Web** Technical Support by e-mail.

Working with the **Sylpheed** mail client is described in the section 3.4.2

11. Work in the Linux command-line terminal

Terminal provides access to the Linux command-line Terminal to work directly from under the graphic shell.

Working with **Terminal** is described in the section 3.4.4.

12. Shut down or reboot the computer

Dr.Web LiveUSB shut down commands are on the system menu of the graphic shell. To open the system menu, click  on the taskbar.

You can choose one of the following items to shut down the computer:

Item	Description
Restart	Reboots the computer
Shut Down	Shuts down the computer

Item	Description
Exit	Exits the GUI and opens the start boot menu

3.2. Dr.Web Antivirus

This section describes how to use **Dr.Web Anti-virus for Linux** from **Dr.Web LiveUSB** Graphic Shell. **Dr.Web Control Desk for Linux** with graphical interface helps you to control **Dr.Web Anti-virus for Linux** in the GUI mode.

Launching Dr.Web Antivirus

When you boot **Dr.Web LiveUSB** in the default (GUI) mode, **Dr.Web Control Desk for Linux** will be started automatically.

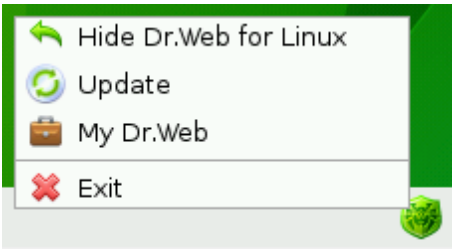
Dr.Web Control Desk for Linux can be launched manually (for example, if its operation was terminated) in one of the following ways:

1. With the left mouse button, double-click the **Dr.Web for Linux** icon  on the desktop;

2. Select **Dr.Web for Linux**  or select **System** and then **Dr.Web for Linux** on the main system menu.

If **Dr.Web Control Desk for Linux** is already launched, the icon of the application displays in the lower-right corner of the desktop (in the notification area next to the clock):

By right-clicking the icon in the notification area, you can open the context menu:

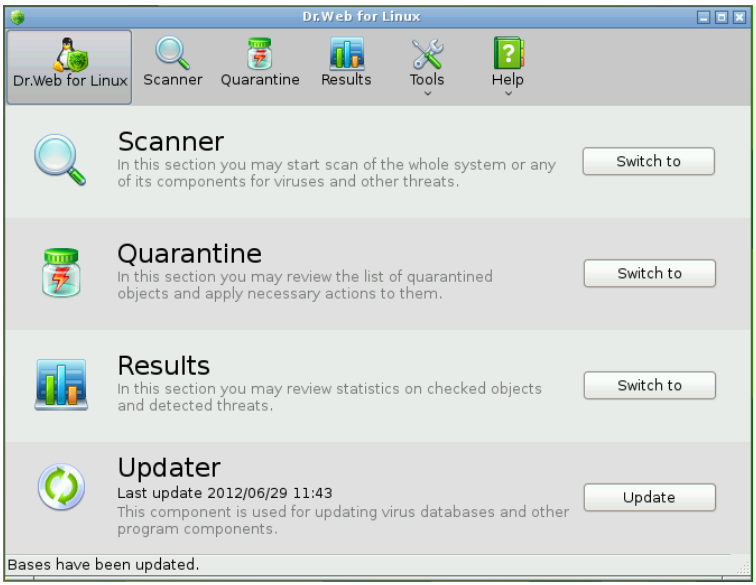


On the context menu the following items are available:

Item	Description
Show/Hide Dr.Web for Linux	Shows or hides **Dr.Web Control Desk for Linux** window. You can also open **Dr.Web Control Desk for Linux** window by clicking the corresponding icon in the notification area.
Update	Updates virus databases at request
My Dr.Web	Opens your personal page of the official **Doctor Web** Web site in a window of the **Firefox** browser
Exit	Exits **Dr.Web Control Desk for Linux**

Dr.Web Control Desk for Linux main window

The following picture shows the **Dr.Web Control Desk for Linux** main window



The toolbar at the top of the window provides access to the main functions of **Dr.Web Anti-virus for Linux**:

Button	Description
Dr.Web for Linux	Opens the **Dr.Web Control Desk for Linux** page (shown in the picture above)
Scanner	Opens the **Scanner** managing page
Quarantine	Opens the **Quarantine** page
Results	Opens the Results page with statistics about **Scanner** operation results

Button	Description
Tools	Opens the context menu of additional **Dr.Web Anti-virus for Linux** tools • **Settings** - adjusting **Dr.Web Anti-virus for Linux** settings; • **Journal -** review a log file of **Dr.Web Anti-virus for Linux** operations; • **License Manager** – review your license and work with key files; • **Send suspicious file** – send a suspicious file to **Doctor Web** specialists.
Help	Opens the context menu of the product help: • **Help** – opens **Dr.Web Anti-virus for Linux** help in a window of the Internet browser; • **Forum** – opens **Doctor Web** forum in a window of the Internet browser; • **What is new** – opens a page with information about new **Doctor Web** anti-virus products in a window of the Internet browser; • **About** – opens a page with brief information about the product name and its version.

Dr.Web Control Desk for Linux Tasks

With **Dr.Web Control Desk** you can:

- scan you system with Dr.Web Scanner;
- view objects in Quarantine;
- view reports on Scanner operations;
- update virus databases;
- configure Dr.Web Anti-virus for Linux;
- view information about your license;
- send a suspicious file for checking;
- View Help and contact Technical support.

3.2.1. Anti-Virus Scanning

This section describes how to scan your system by **Dr.Web Anti-virus for Linux** from **Dr.Web LiveUSB** Graphic Shell.

To start Antivirus scanning

1. Launch **Dr.Web Control Desk for Linux** if it is not already opened;

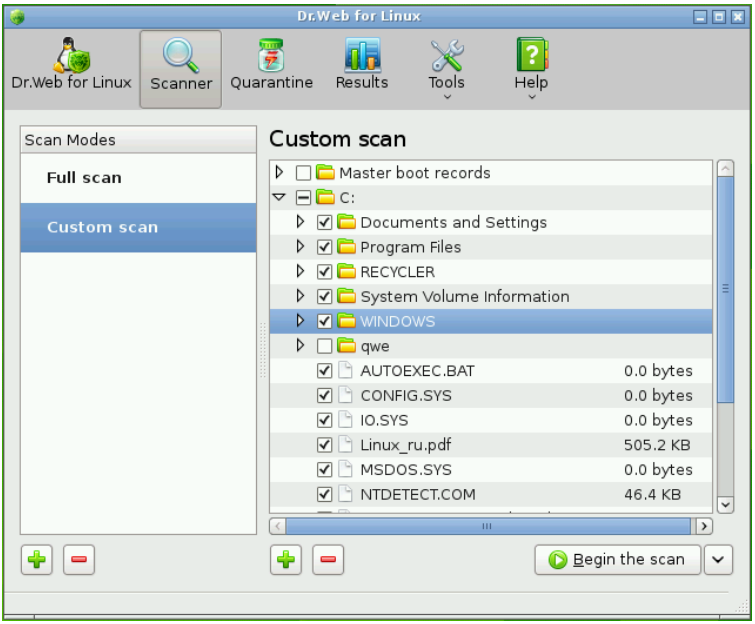
2. Open the Scanner page by clicking the button 

on the toolbar or by clicking **Switch to** on the **Dr.Web Control Desk for Linux** main page

It is strongly recommended to update Dr.Web virus databases before scanning.

Starting Scanning

The following picture shows the **Scanner** page of **Dr.Web Anti-virus for Linux**:



To select a scanning mode

The left pane of the **Scanner** Settings page contains a list of the main scanning modes and the right pane displays a directory tree. **Scanner** supports the following modes:

Scanning mode	Description
Full scan	All files and all master boot records (MBR) are scanned on all drives, except the **Dr.Web LiveUSB** disk. In this mode a user can not add or exclude boot records, files and folders from scanning

Scanning mode	Description
Custom scan	This mode allows to select master boot records, drives, folders, and files for scanning

It is strongly recommended to start scanning in **Full scan** mode if the computer is infected.

Creating new scanning modes

The buttons  and  allow to edit the list by adding or removing created modes of scanning user-selected objects. To add a new mode to the list, click the button  , specify the name in the opened window, and click **OK**. By default, a new mode contains no object for scanning. You can select files and folders in the directory tree to be added to scanning in this mode.

To remove a selected scanning mode from the list, click the button  .

To rename a mode, double-click it (after the name is changed, click `ENTER` to save changes).

Removing standard scanning modes **Full scan**, **Custom scan** from the list is not available.

Selecting files and folders to scan

You can select files and folders to scan in the directory tree in the right pane of the window. The selection is available only in **Custom Scan** mode or any mode created by you.

Master boot records (MBR) of all drives connected to the computer are in the root directory. Boot records contain a program code that launches Windows operating system and can be compromised by viruses. It is recommended to include boot records into constant scans.

In addition to Master Boot Records branch, the root directory contains all drives found by **Dr.Web LiveUSB**. Consider that **Dr.**

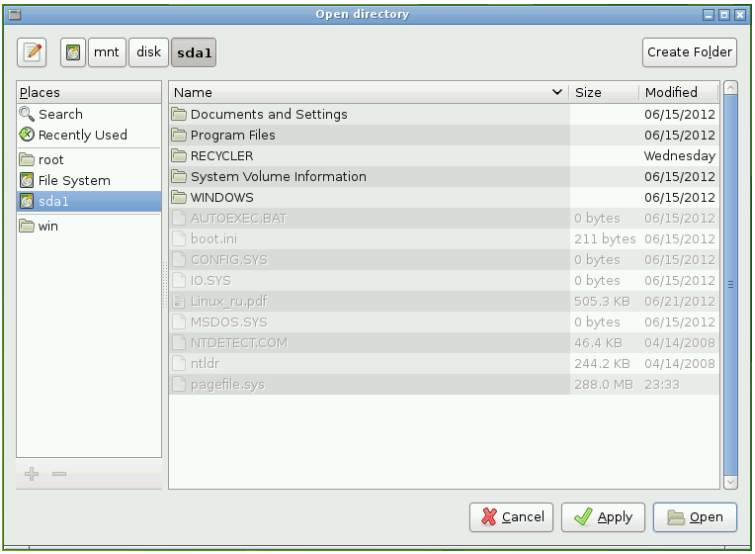
Web LiveUSB automatically finds all disks and partitions formatted in FAT or NTFS systems and assigns drive letters to them (`C:`, `D:`, and so on), as common in **Windows** or **DOS** systems.

To view folder contents, click a triangle symbol ▷ left of a disk or folder name. All subfolders and files are to be displayed below the opened folder. If the folder is opened, a triangle symbol is the following: ▽. To close the opened folder and hide its subfolders and files, click the upside down triangle symbol ▽.

To add an element to scanning, select its name in the directory tree. Clear the checkbox to remove the element from the list of objects for scanning. Select a folder to add all its subfolders and files to the list of objects for scanning. If the symbol left of the folder name is the following: ☐, not all subfolders and files are selected for scanning.

The buttons  and  below the directory tree allow to add paths into the root directory for scanning.

To add a new path to the list, click the button  . The window, where you can select a folder, appears:



The left pane **Places** enables to open the following folders:

- **Search** – searches for a file or a folder in all file directories;
- **Recently Used** – opens the list of recently used documents and files;
- **root** – opens a login directory of a superuser (**Dr.Web LiveUSB** programming environment has Linux superuser privileges);
- **File system** – opens a root folder of the Linux file system;
- **hdX*** or **sdX*** (where **X** is a Latin letter and * is a number) – opens contents of a drive mounted on the Linux file system as a mount point (`/mnt/disk/hdX*` or `/mnt/disk/sdX*` respectively);
- **win** – opens the list of found NTFS or FAT drives with their drive letters (`C:` , `D:` , and so on), as common in **Windows** or **DOS** systems (each drive corresponds to its logical mount point `/mnt/disk/hdX*` or `/mnt/disk/sdX*`).

The contents of the selected folder is listed in the right pane of the window. Double-click a folder name to display its contents.

The path to the current folder displays in the top part of the window as a set of buttons corresponding to the passed folders ('bread crumbs'). Click the button to open the corresponding folder.

The buttons  and below the **Places** pane enable to add or remove the current folder to this quick access list.

To add a folder to the list, select its name in the file system and click the button  .

To remove a folder from the quick access list, select its name and click the button  .

To add the selected folder to scanning, click **Apply**. To cancel adding the folder, click **Cancel**.

The selected folder is always added to the root directory.

Click  below the directory tree to remove the selected path. The physical folder is not to be deleted. Scanning of this folder is canceled unless it is checked in the tree (as one of the folders for scanning in the disk).

Files and folders added to the list of exclusions on the Scanner settings page are not scanned

Starting scanning

After selecting drives, files, and folders to scan, click **Begin the scan**.

It is recommended to specify actions of **Scanner** for suspicious and infected files before scanning. To set actions, click the button  on the right of the **Begin the scan** button.

The menu with the following items appears:

Item	Description
Actions are applied automatically	Scanner applies specified actions to detected threats of different types automatically.
Actions are selected manually	Scanner displays a notification and suggests selecting an action upon the detected dangerous object.

To select a **Scanner** reaction, click the corresponding item. By default, actions are applied manually.

Scan Results

While scanning, the following information displays on the **Scanner** page:

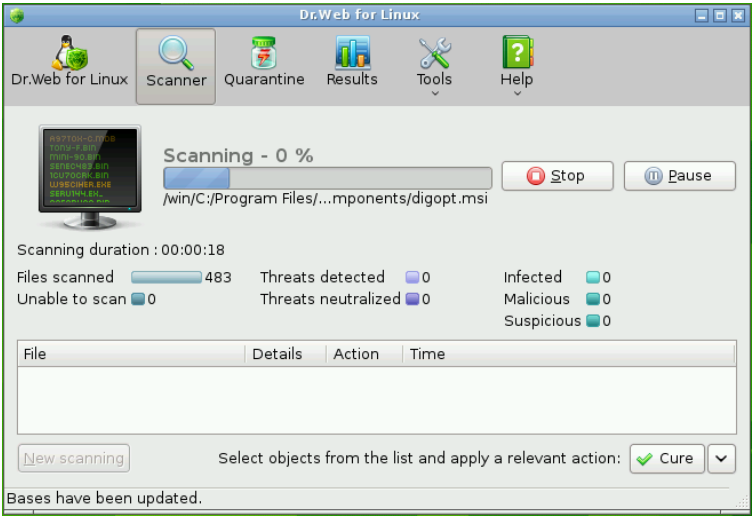
- Scanning progress;
- Name of the file being scanned;
- Statistics.

Scanning can be stopped or paused at any time by clicking a corresponding button to the right of the scanning progress in dicator. After clicking the **Stop** button, scanning is interrupted. To start a new scanning process, click the **New scanning** button. Clicking the **Pause** button allows to suspend scanning and resume it later. Results and settings of a scanning process will not be reset and scanning can be continued from the point it was paused at.

Scan results are displayed as a table in the bottom of the **Scanner** page. There you can find information on infected and suspicious objects detected during the scanning: the path, reason of including it into the list, and actions performed by the program over this object.

The list of detected objects is displayed in a hierarchical order. For example, if a virus is found inside an archive, then the infected archive is displayed in the report field as a node whose contents you can minimize or expand.

The following picture shows the Scanner window when scanning is in progress:



The button that enables to apply actions for selected objects is below the list of dangerous objects. To select an object in the list, click its name (hold down `SHIFT` to select multiple adjacent objects or `CTRL` to select multiple nonadjacent objects).

After objects are selected, click the button  to display the menu with available actions. To apply an action, select the corresponding item and click the button (button caption and its icon always correspond to the action selected on the menu).

List of the available actions:

Scan mode	Description
Cure	Available only for files infected by a virus. Curing is an attempt to neutralize virus and restore the original state of the object before infection
Move to quarantine	Moving the selected file from its original path to the specific **Quarantine** folder (action is not available for read-only files)

Scan mode	Description
Remove	Deleting the selected files completely (action is not available for read-only files)

There are the following limitations:

- For suspicious objects curing is impossible;
- For objects which are not files (boot sectors) moving, renaming, and deletion is impossible;
- For individual files inside archives, installation packages, or attachments, no action is possible. Actions are applied to the whole object.

If another action is set to this type of detected threats on the Actions Tab in the **Scanner** settings window, the **Status** column will display the result of performed actions.

In case an attempt to cure a file failed, the action set to incurable objects on the **Actions** tab in the **Scanner** settings window is performed.

It is recommended to send suspicious files moved to the specific **Quarantine** folder to **Dr.Web** Virus Laboratory. Use the special form on the Web site at http://vms.drweb.com/sendvirus/

To open the start scanning window, click the **New Scanning** button (the button is not available when scanning is in progress; you should wait for completion of scanning or interrupt the process by clicking **Stop**).

3.2.2. Quarantine Page

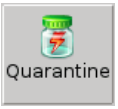
This section describes how to manage **Quarantine**, where infected, malicious or suspicious objects detected by **Dr.Web Anti-virus for Linux** during scanning are stored.

Quarantine is a special folder in the file system, where **Scanner** moves infected, suspicious, or malicious objects that were not cured, deleted, or skipped during scanning. The **Quarantine** component enables the user to view **Quarantine** content and

apply the selected action to quarantined objects.

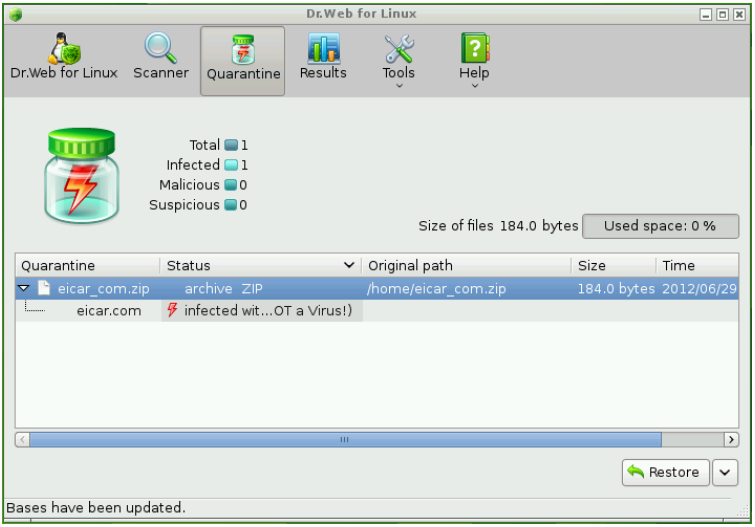
To open Quarantine:

1. Launch **Dr.Web Control Desk for Linux** if it is not already opened;

2. Open the **Quarantine** page by clicking 

on the toolbar or clicking **Switch to** in the **Quarantine** section on the **Dr.Web Control Desk for Linux** main page.

The following picture shows the **Quarantine** page:



Quarantined objects are to be listed in the table in the bottom pane. The table displays the following information on infected, malicious, or suspicious objects:

- **Quarantine** - name of the quarantined object;
- **Status** - malware class of the object;

- **Original Path** - path of the object before it was quarantined;
- **Size** - size of the object;
- **Time** - time of moving the object to **Quarantine**.

The objects are listed in a hierarchical order. For example, a quarantined archive is displayed as a node, whose contents you can expand and collapse.

Quarantine stores the following objects:

1. Temporary files, indicated by the icon  . These files are backup copies of infected, malicious, or suspicious files, for which the **Cure** action was assigned. Temporary files can also be backup copies of deleted files (for which the **Delete** action was assigned), that enables to restore a deleted file if necessary.
2. Permanent files, indicated by the icon  . These are infected, malicious, or suspicious files, moved to **Quarantine** according the specified settings (**Move to quarantine** action). As anti-virus algorithms are constantly being improved, these files might be cured later.

Temporary files are stored in **Quarantine** during a time period specified in Settings. When the time period is expired, files are to be deleted completely. They are also deleted after **Quarantine** has reached the maximum of disk space set for the **Quarantine** folder (to give space to new objects). Permanent files can be deleted only by the user (**Delete** action).

By default, **Quarantine** is located in the subfolder `.drweb` of the user's login directory.

Working with quarantined objects

The button that enables to apply an action upon the selected objects is below the list of quarantined objects. To select an object in the list, click its name (hold down SHIFT to select multiple adjacent objects or CTRL to select multiple nonadjacent objects).

After selecting objects, click the button  and specify one of the actions. To apply the selected action, click the button with corresponding caption and icon.

You can specify one of the following actions:

Action	Description
Restore	The selected file is to be moved to its original folder
Restore to...	The file is to be moved to the specified folder
Remove	The file is to be deleted from **Quarantine** completely

It is recommended to send suspicious files moved to the specific **Quarantine** folder to **Dr.Web** Virus Laboratory. Use the special form on the Web site at http://vms.drweb.com/sendvirus

The **Quarantine** folder is created on the RAM drive, so backup copies saved to **Quarantine** will be lost unless they are saved to one of the computer hard disk drives (physical disk drives) or a removable media.

To save quarantined files, you can use snapshots (available in Advanced mode only)

3.2.3. Results Page

This section describes how to work with a report on scan results. The **Results** page contains information about malicious objects and other threats, detected by **Scanner** on your computer. The **Results** component allows to view statistics on detected threats and delete outdated data.

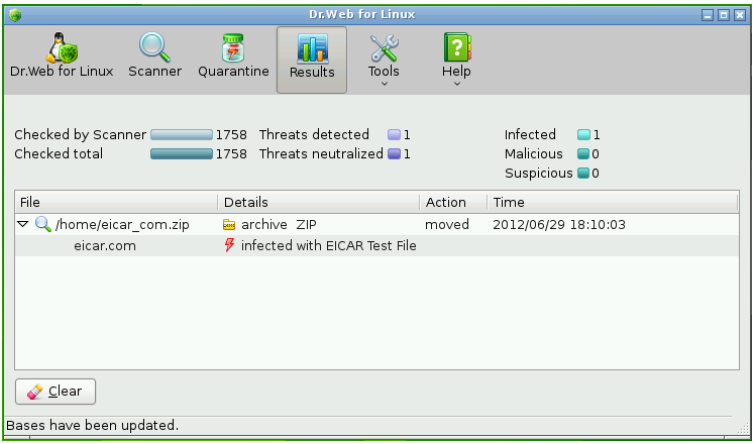
To view Results page:

1. Launch **Dr.Web Control Desk for Linux** if it is not already opened;

2. Open **Results** page by clicking 

on the toolbar or by clicking **Switch to** in the **Results** section on the **Dr.Web Control Desk for Linux** main page.

The following picture shows the **Results** page:



The top pane of the window displays statistics on detected threats. To delete Statistics, click **Clear** button in the bottom pane.

The middle pane displays the table of detected threats:

Column	Description
File	Path to the file that poses a threat and the file name
Details	Information about the threat (for example, its name or its type)
Action	Information about the action applied to neutralize the threat (the field is empty if no action was applied to the object)
Time	Time of the threat detection

3.2.4. Updating Virus Databases

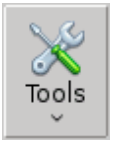
New types of computer threats with more perfect masking techniques are constantly appearing worldwide. Updating virus databases and other **Dr.Web for Linux** components guarantee an up-to-date protection for your computer. Updates are downloaded and installed by a special component **Updater**.

Running Updater

1. Launch **Dr.Web Control Desk for Linux** if it is not already opened;
2. Open **Updater** page by clicking **Update** button on the main page of **Dr.Web Control Desk for Linux** or by right-clicking the Anti-Virus icon  in the taskbar notification area and select **Update**.

3.2.5. Dr.Web Anti-virus for Linux Configuration

To open **Dr.Web Settings** page:

1. Launch **Dr.Web Control Desk for Linux** if it is not already opened;
2. Open **Dr.Web Settings** page by clicking 

on the toolbar of **Dr.Web Control Desk for Linux** and selecting **Settings** on the opened menu.

Dr.Web Settings page contains the following tabs:

- **Scanner** tab - where you can configure **Scanner** operations;

- **Quarantine** tab - where you can configure **Quarantine** operations;
- **Updates** tab - where you can configure **Updater** operations;
- **Notification** tab - where you can configure displaying of notifications.

The bottom pane of the **Dr.Web Settings** page displays the following buttons:

- **Set default -** click to restore settings to their default values;
- **OK -** click to save changes and opens the **Dr.Web Control Desk for Linux** main page;
- **Apply** - click to save changes without closing the **Dr.Web Settings** page;
- **Cancel** - click to open the **Dr.Web Control Desk for Linux** main page without saving the changes.

During its operation **Dr.Web LiveUSB** uses a temporary RAM drive created when the system boots. Thus, all changes in program settings stored on the RAM drive will be lost when the computer reboots.

To save the changes, use a snapshot (available in Advanced mode only).

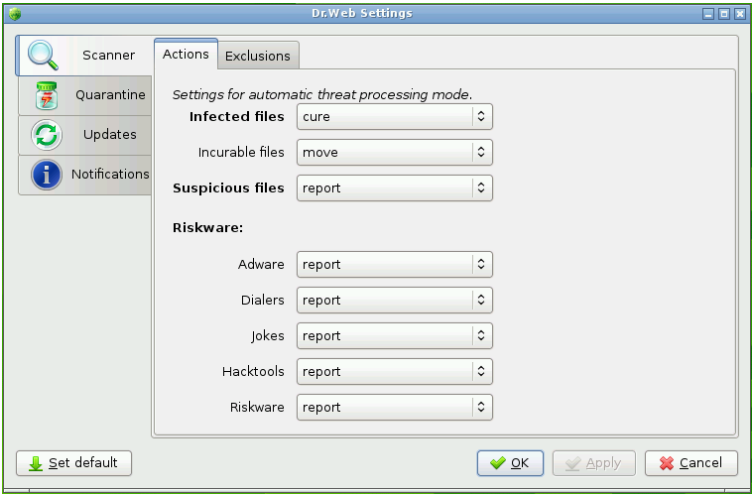
Scanner Settings

Scanner Settings page contains two tabs:

- **Actions** - where you can configure automatic reaction of **Dr.Web Scanner** on detection of suspicious or malicious objects;
- **Exclusions** - where you can specify files or directories to be excluded from scanning.

Actions tab

The following picture shows the **Actions** tab:



On this tab, you can set automatic actions upon different types of computer threats if a necessary action is not to be selected manually.

You can select one of the following actions for different types of threats:

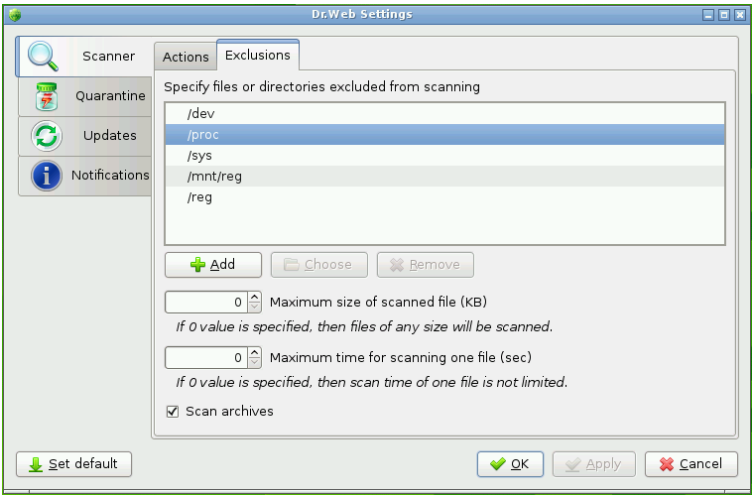
- **Cure** (available only for infected files) - instructs to try to cure the object infected by a known virus. If the attempt fails (for example, the object is incurable), the action set for incurable files is to be applied. By default, this action is set for all infected files;
- **Delete** - instructs to delete the infected or suspicious file;
- **Move** - instructs to move the infected or suspicious file to the Quarantine folder. By default, this action is set for incurable files;
- **Report** - instructs to inform the user about detected threats on the Results page. In this case actions upon detected files are to be applied manually. By default, this action is set for suspicious and supposedly infected files, for example, hacker or joke programs;

- **Ignore** (available for suspicious files and all supposedly infected files) - instructs to skip the file (information about this file is to be registered in the log file).

Default settings specified on the **Actions** tab are optimal for efficient protection of your computer. It is recommended to keep these settings unless it is necessary to change them.

Exclusions tab

The following picture shows the **Exclusions** tab:



On this tab, you can list files and directories to be excluded from scanning. As the **Quarantine** folder is used to isolate dangerous objects and the access to this folder is blocked, the **Quarantine** folder is automatically excluded from scanning and you do not need to add this directory to the list.

To configure the list of exclusions:

1. To add a file or directory to the list of exceptions
   - Click **Add**;
   - In the opened window specify the object and click **Apply**;

2. To change a folder or/and a file, select it in the list and click **Choose**;
3. To remove a folder or a file from the list, select it and click **Remove**;
4. You can limit the maximum size of scanned files (files whose size is more than the specified size are to be skipped). You can also specify the maximum time for scanning one file to prevent Anti-Virus not responding during scanning large or damaged files. To enable this option, specify the limit values in the respective fields. "0" value disables the respective limit;
5. To exclude all types of archives from scanning, clear the check box **Scan archives**.

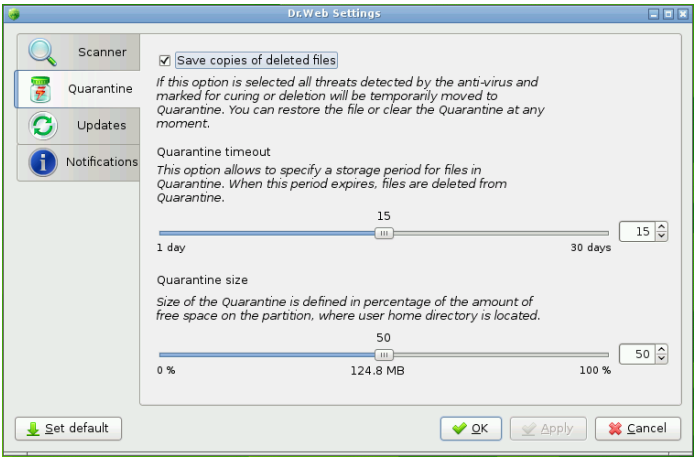
Default settings are optimal for most cases. It is recommended to keep these settings unless it is necessary to change them. Some folders on the list of exclusions cannot be removed from the list.

Listed files are to be excluded from scanning even if they were selected for scanning on **Scanner** startup.

Quarantine Settings

On this page, you can specify the size of the **Quarantine** folder and the period for storing quarantined files.

The following picture shows the **Quarantine Settings** page:



You can select one of the actions for different types of threats:

- Option **Save copies of deleted files** instructs **Scanner** to move backup copies of deleted files to **Quarantine**. If this option is disabled, the objects are to be deleted completely;
- Slider **Quarantine timeout** enables to specify the time for storing the backup copies of deleted files (files moved to **Quarantine** are to store there permanently until they are either restored or completely deleted by the user);
- Slider **Quarantine size** enables you to specify the maximum disk space (as percentage of total disk space) for the **Quarantine** folder. After **Quarantine** has reached the specified maximum of disk space, backup copies of files are to be deleted.

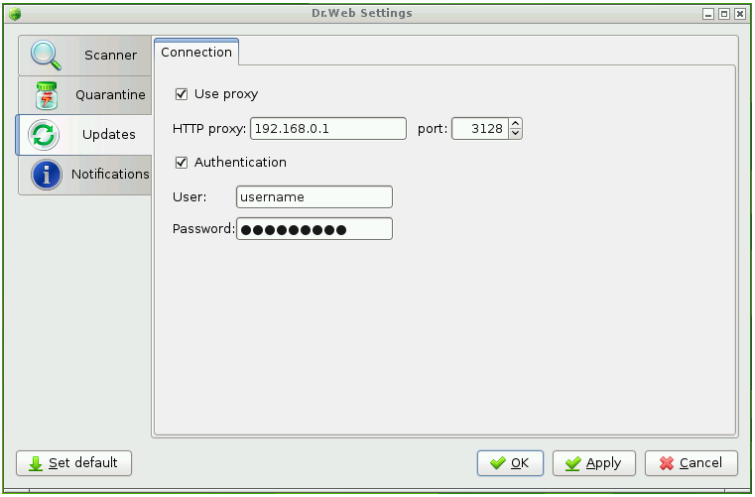
Updater Settings

This page contains one tab:

- **Connection** - where you can set parameters of connection to **Doctor Web** update servers.

Connection Tab

The following picture shows the **Connection** tab:



On this tab, you can specify a proxy server for updating and configure proxy connection settings.

To specify a proxy server, check **Use proxy**. You need to configure the following settings:

- **HTTP proxy** – specify the name or IP address of the proxy server;
- **port** - specify the port number that the proxy server uses;
- **Authentication -** check this option and specify user (login) and password in the respective fields if the proxy server requires authentication.

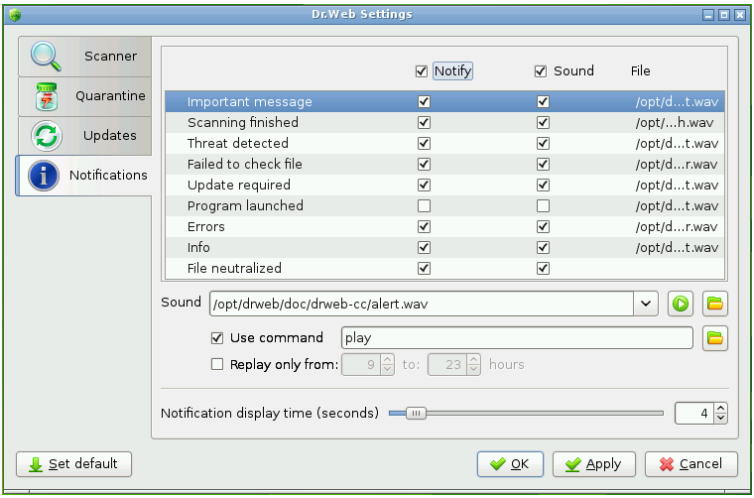
Using a proxy server is required only if the local network policy forbids access to external servers or only to **Doctor Web** servers.

Notification Settings

On this tab, you can configure notification settings by which **Dr.**

Web Anti-virus for Linux notifies the user on different events in the operation of Anti-virus.

The following picture shows the **Notification Tab**:



Notifications of the following types are available:

- **Pop-up notifications** – notifications that appear on the screen when an event occurs;
- **Sound notifications** – sound alerts on events.

Notification setting

1. You can change sound alert settings if necessary:
   - To enable (or disable) all sound alerts, select (or clear) the **Sound** check box in the top pane of the tab;
   - To enable (or disable) sound alerts on particular events, select (or clear) the corresponding check box in the **Sound** column;
   - To select a special sound for a particular event, select this event in the list, then select one of the sounds in the drop-down **Sound** list. To add a new sound to the list, click **Select**. If necessary, you can set a command and time

period for sound notifications. To play the selected file, click **Play Sound**

2. You can change pop-up notification settings if necessary:
   - To specify notification display time, use the slider;
   - Pop-up notifications are enabled by default. To disable (or enable) all pop-up notifications, select (or clear) the **Notify** check box in the top pane of the tab;
   - To enable (or disable) pop-up notifications on particular events, select (or clear) the corresponding check box in the **Notify** column.

3.2.6. Journal Tab

This section describes how to work with **Journal**. **Journal** contains all messages that occur while **Dr.Web Anti-virus for Linux** operation: information about skipped malicious objects, errors, and notifications. On the Journal tab you can view Journal contents and, if necessary, export records from **Journal,** or delete them.

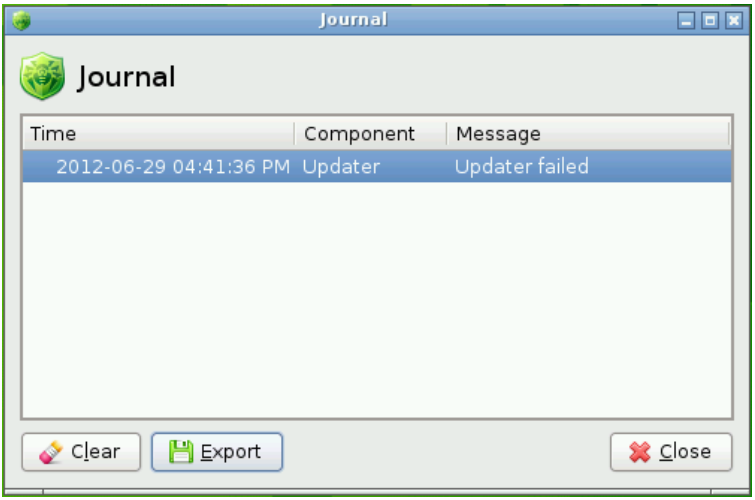
To open the Journal Tab:

1. Launch **Dr.Web Control Desk for Linux** if it is not already opened;

2. Open the Journal Tab by clicking the button 

and selecting the **Journal** item on the opened menu.

The following picture shows the **Journal Tab**:



The bottom pane of the window displays:

- **Clear** - allows to delete all records from the Journal;
- **Export** - allows to save all records to a text file (specify the file name and directory in the opened window).

The middle pane of the Journal Tab displays the table with Journal messages. Specify the following parameters for each message:

Parameter	Description
Time	Time when the record was created
Component	Name of an Anti-virus component that created the message
Message	Text of the message created by an Anti-virus component, or description of the occurred event

Click **Close** to close the **Journal** Tab.

3.2.7. License Manager

Dr.Web Anti-virus for Linux operation modes and the list of the

available functions are set in accordance with the active license. The license key file is included into the **Dr.Web LiveUSB** software and allows to use **Dr.Web Anti-virus for Linux** basic configuration which is enough for scanning the computer.

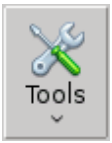
You can view the license usage period in the special window of **Dr.Web Control Desk for Linux**.

Due to emergence of new threats, **Dr.Web Anti-virus for Linux** can become obsolete. Therefore, the license period for **Dr.Web Anti-virus for Linux**, included into **Dr.Web LiveUSB**, is restricted.

After the license is expired, download a new version of the product from **Doctor Web** Web site at http://www.freedrweb.com/liveusb/

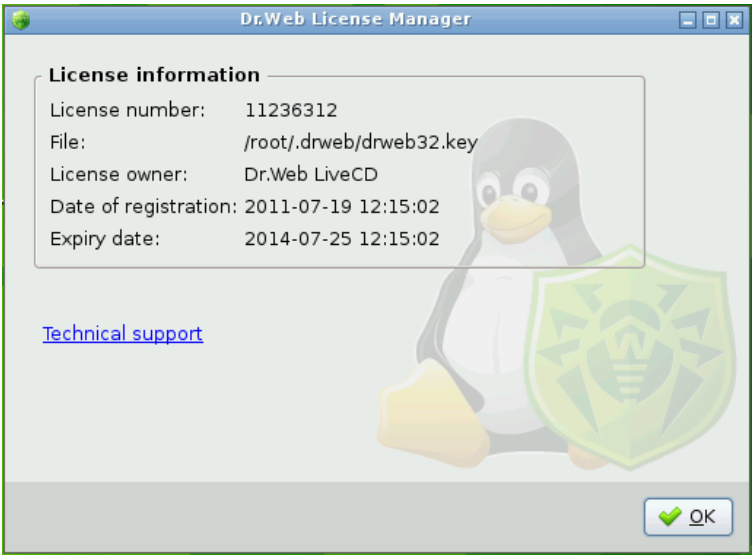
To view information on the license:

1. Launch **Dr.Web Control Desk for Linux** if it is not already opened;

2. Open the License Manager window by clicking 

on the toolbar and select **License manager** on the opened menu.

The following picture shows the **License manager** tab:



Click **OK** to close the window.

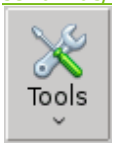
Click **Technical support** to open the **Doctor Web Technical support** Web page in the **Firefox** Web browser.

3.2.8. Sending Files for Checking

It is recommended to send files marked by **Dr.Web Anti-virus for Linux** to be suspicious or probably infected by unknown viruses for analysis to the **Doctor Web** laboratory.

Such files are moved to the **Quarantine** folder during scanning. **Scanner** can delete such files and move their copies to the **Quarantine** folder (see Scanner and Quarantine settings). If **Scanner** is allowed to skip the file during scanning, you need to remember its directory or view it on the Results page.

To send the suspicious file for checking:

1. Open the Web page for sending files at http://vms.drweb.com/sendvirus/ in the browser. You can open the page by clicking 

on the toolbox of **Dr.Web for Linux** main window and selecting **Send suspicious file** on the opened menu.
2. Follow the instructions on the opened Web page for sending virus.

Files stored in the **Quarantine** folder are located in `/root/.drweb/quarantine` or `~/.drweb/quarantine` (as operation runs in the superuser (root) mode)

3.2.9. Getting Help

If you need help with the product, open the **Help** menu on the **Dr.Web Control Desk for Linux** tab.

To open Help, click 

on the toolbar and select one of the following items:

- **Help** – opens **Dr.Web Anti-virus for Linux** Help in the inbuilt browser;
- **Forum** - opens the page of the **Doctor Web** forum in the inbuilt browser;
- **What is new?** - opens the news page with information about **Doctor Web** anti-virus products in the inbuilt browser;
- **About** - opens the window with information about the name

and your version of the product.

To contact **Technical support**, **visit Doctor Web Technical Support** Web site at support.drweb.com.

3.3. Graphic Shell Configuration

To configure **Dr.Web LiveUSB** Graphic Shell, click **Settings** on the System Menu. The following options are available:

- Adobe Flash Player – allows to configure Adobe Flash Player;
- Openbox Configuration Manager – allows to configure the GUI;
- Menu Configuration – allows to configure Taskbar parameters;
- Network Configuration – allows to configure the network connection.

To adjust settings, open the System menu by clicking the button  in the corner of the taskbar and select a required item in the **Settings** submenu. The window displaying required settings will appear.

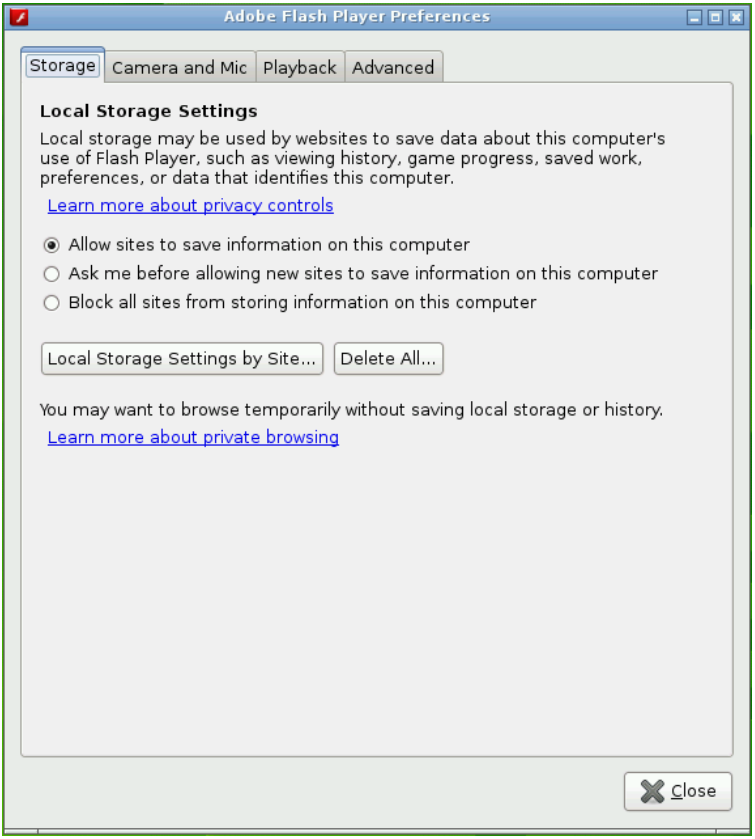
During its operation **Dr.Web LiveUSB** uses a temporary RAM drive created when the system boots. Thus, all changes in program settings stored on the RAM drive will be lost when the computer reboots.

To save the changes, use a snapshot (available in Advanced mode only).

3.3.1. Adobe Flash Player Configuration

Adobe Flash Player is software for playing multimedia (video and audio) injected into Web pages. This player is also used by some Web applications. In the **Adobe Flash Player Preferences** window you can configure storage settings for data used by flash applications as well as camera and microphone access settings.

The following picture shows the **Adobe Flash Player Preferences** window:



In this window you can configure the following **Adobe Flash Player** parameters:

- **Storage**. On this tab, you can allow or deny Web sites that you open in the browser to store Adobe Flash information on the computer. You can allow Web sites to save data without asking you or only after your permission (in this case each time a Web site wants to save information on your computer, you will receive a request which you can approve or deny). To specify the storage option, click the corresponding item. You can also specify different storage options for different Web sites by clicking **Local Storage Settings by Site**. Click **Delete All** to remove all information from the storage.
- **Camera and Mic**. On this tab, you can allow or deny Web sites to access your camera and microphone connected to this computer (without asking you or only after your permission). You can specify different settings for different Web sites by clicking **Camera and Microphone Settings by site**.
- **Playback**. On this tab, you can allow Web sites to use a peer-to-peer network while playing video (without asking you or only after your permission). In addition, you can specify different playback options for different Web sites;
- **Advanced**. On this tab, you can specify the following advanced settings for **Adobe Flash Player**:
  - Delete all local storage settings, clear all permissions for Web sites;
  - Check for **Adobe Flash Player** updates;
  - Deauthorize the computer and delete all personal information used by **Adobe Flash Player**;
  - Specify trusted locations for developer testing (not recommended).

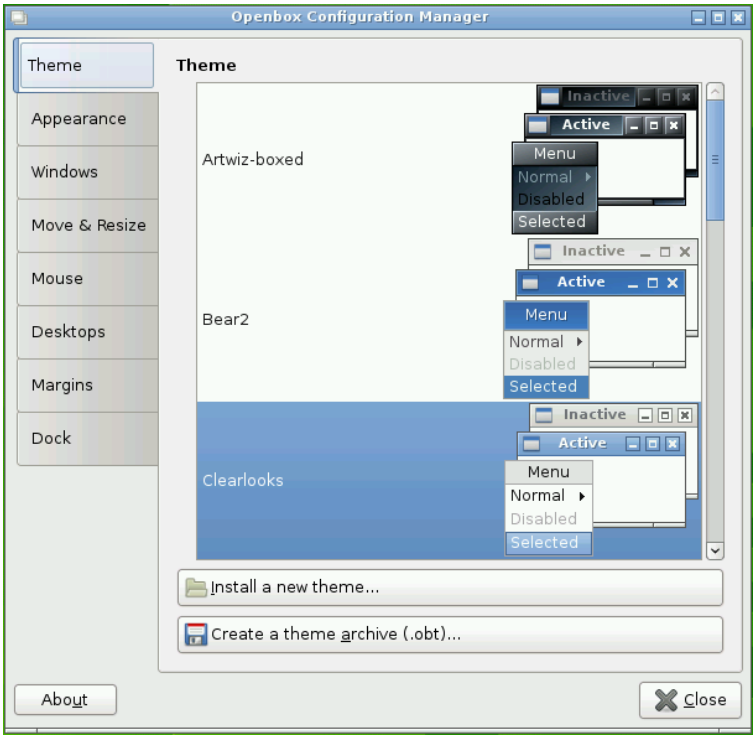
You can open Web pages with additional information on configuring **Adobe Flash Player** in the browser. To do this, click **Learn more about...** links on the tabs in **Adobe Flash Player Preferences** window.

Any change in **Adobe Flash Player** settings that you make in this window is applied at once. Click **Close** to close the **Adobe Flash Player Preferences** window.

3.3.2. Openbox Configuration Manager

Dr.Web LiveUSB graphic shell is based on Openbox GUI - a window manager for Linux systems.

The following picture shows the window of Openbox Configuration Manager:



This window allows to configure the following parameters of the graphic shell:

- **Theme** - on this tab, you can choose the common style for all windows (for example, background color, color of headers);
- **Appearance** - on this tab, you can adjust window settings (for example, format of headers, fonts);

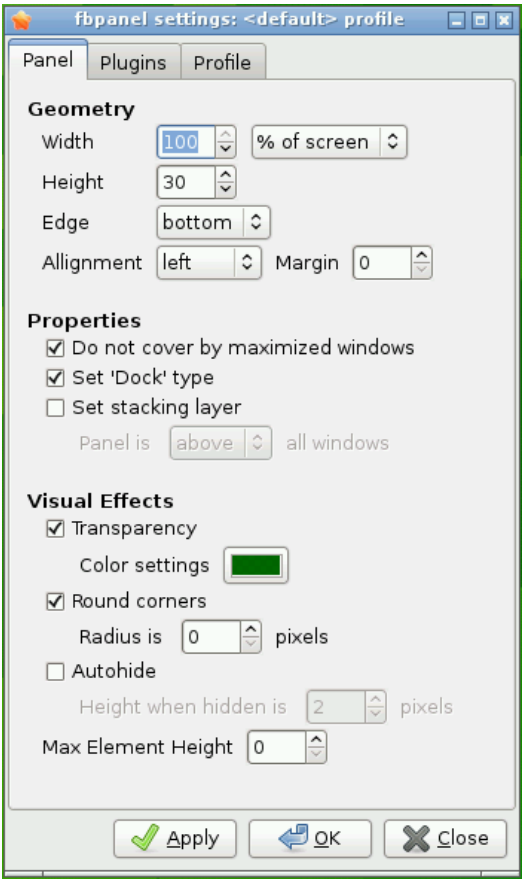
- **Windows** - on this tab, you can set a window opening behavior (for example, gaining focus, alignment in the center of the screen);
- **Move & Resize** - on this tab, you can adjust parameters of moving windows and changing window size;
- **Mouse** - on this tab, you can adjust window reaction on pointer movements (for example, gaining focus);
- **Desktops** - on this tab, you can set the number of desktops (by default, four desktops are set) and parameters of switching them;
- **Margins** - on this tab, you can set the desktop size (width);
- **Dock** - on this tab, you can adjust dock parameters - the special area at the edge of the screen used to launch and switch between graphical modules of dock applications (for example, the clock, the calendar).

Any changes in the graphic shell parameters made in this window are applied at once. Click **Close** to close the Settings window.

3.3.3. Menu Configuration

Menu configuration window allows to choose the position, size, and special effects of the taskbar display (**Panel** tab) and also adjust plugins for the graphic shell (Plugins tab).

The following picture shows the Menu configuration window:



You can adjust the following parameters in this window:

- Geometry of the Taskbar (**Geometry** section):
  - **Width**: Width in pixels or percentage of the screen width;
  - **Height**: Height in pixels;
  - **Edge**: position on the screen (left, right, top, bottom);
  - **Alignment**: alignment of elements on the taskbar (left alignment, right alignment, center alignment);
  - **Margin**: desktop margins in pixels.
- Taskbar properties (**Properties** section):
  - **Do not cover by maximized windows** – on top of all windows;
  - **Set 'Dock' Type** – enable using Dock panel;
  - **Set stacking layer** – set the position of the taskbar (above or below all windows);
- **Visual Effects**:
  - **Transparency** – select the taskbar transparency and color settings;
  - **Round corners** – enable using rounded corners and set their radius (**Radius is**);
  - **Autohide** – automatically hide the Taskbar when moving the pointer away (you can specify the Taskbar height when it is hidden);
  - **Max Element Height** – the maximum height of elements on the Taskbar.

On the **Plugins** Tab, you can view the set of plugins (components) to be displayed on the Taskbar and configure it if necessary (change the order of plugins, add, or remove components).

On the **Profile** Tab, you can view information on all profile settings to be displayed in the Menu Configuration window (this file is named `default` and is in the `/root/.config/fbpanel` directory).

Click **Apply** to save the changes without closing the window.

Click **OK** to save changes and close the window.

Click **Close** to close the window without saving the changes.

3.4. Inbuilt Applications

This section describes applications within **Dr.Web LiveUSB** anti-virus solution. You can launch them by clicking the respective icons on the desktop, items on the system menu in the graphic shell or items on the Start menu in Advanced mode.

3.4.1. Browser

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

An Internet connection via the local LAN (Local Area Network connection) is required to access the Web pages with the inbuilt browser.

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

Launching the browser in the graphic shell

You can launch the inbuilt browser in one of the following ways:

- Double-click the **Firefox** icon  on the desktop;
- Click the icon  on the Taskbar;
- Select **Network** and then select **Mozilla Firefox** on the main menu of the graphic shell.

Launching the browser in the console

Launching the browser is not available in the console. You can only launch the browser in the graphic shell.

During its operation **Dr.Web LiveUSB** uses a temporary RAM drive created when the system boots. Thus, all saved Web pages and the browser history will be lost when the computer reboots. To save Web pages, use the hard drive.

To save the changes, create a boot flash drive or use a snapshot (available in Advanced mode only).

For more information about working with the **Mozilla Firefox** browser, visit the Web site of the developer at http://support.mozilla.org/.

3.4.2. Mail Client

The inbuilt **Sylpheed** mail client will provide you with all options to maintain e-mail correspondence.

Launching the mail client in the graphic shell

You can launch the mail client in one of the following ways:

- Double-click the **Sylpheed** icon  on the desktop;
- Click the icon  on the Taskbar;
- Select **Network** and then select **Sylpheed** on the system window of the graphic shell.

Launching the mail client in the console

Launching **Sylpheed** is not available in the console. You can only launch the mail client in the graphic shell. If you need to send a message in the console, use the **ssmtp** utility.

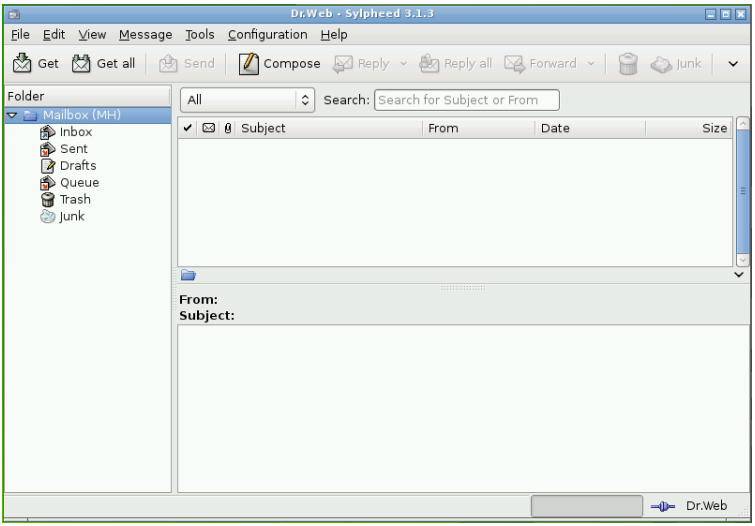
Working with the mail client

An account at the `mail.drweb.com` server is preinstalled in **Sylpheed** to enable user to send messages only to e-mail addresses with drweb.com domain name (`<mailbox>@drweb.com`). To send messages to e-mail addresses with another domain name (for example, `gmail.com` or `yandex.ru` domain names), create additional accounts. You can use any of your accounts if mail servers for the domain can be accessed.

To create a new account, select **Configuration** and then select **Create new account**. Enter all required information to enable mail transfer:

- sender's e-mail address;
- mail sending parameters (SMTP protocol: server, port, authentication);
- mail receiving parameters (POP3 protocol: server, port, authentication);
- accompanying information.

To work with several accounts, you can create separate mailboxes. To do this, select **File**, and then select **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.

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

During its operation **Dr.Web LiveUSB** uses a temporary RAM drive created when the system boots. Thus, all saved messages will be lost when the computer reboots. To save e-mail messages, use the hard drive or a removable media.

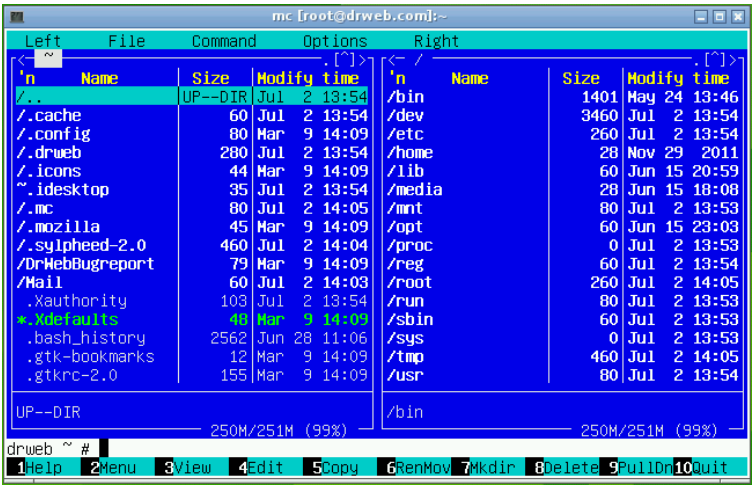
To save the changes, use a snapshot (available in Advanced mode only).

For more information about working with **Sylpheed** visit the Web site of the developer at http://sylpheed.sraoss.jp/en/.

3.4.3. File Manager

The inbuilt **Midnight Commander** file manager is similar to the **Norton Commander**, **FAR** and **Total Commander** file managers used in OS MS-DOS and Windows operating systems. The **Midnight Commander** file manager works in the console, so you can launch the file manager not only in the graphic shell, but also from the command line.

The following picture shows the screen of the File manager (in window mode):



Launching the file manager in the graphic shell:

You can launch the file manager in the graphic shell in one of the following ways:

- Double-click the icon  on the desktop;

- Select **Utility** and then select **File Manager** on the main system menu of the graphic shell.

Launching the file manager in the console:

To launch the file manager in the console shell, enter the following command:

```
mc
```

Working with files

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

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

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

For more information visit Web site at https://www.midnight-commander.org/.

Viewing and editing the Windows registry branch

Windows registry branches are exported to the file system (into the **/reg** folder) when launching **Dr.Web LiveUSB**. This enables to work with registry keys as with ordinary text files: view their contents and edit them when necessary.

Despite the fact that working with the Windows registry is similar to working with files and folders, registry branches are not folders, and you must not copy ordinary files and folders into them.

It is also not recommended to delete, remove, or rename registry branches and registry keys as that can lead to total or partial malfunction of the operating system (or some of its components) because of the damaged registry.

Closing the file manager

To finish working with the file manager and close it, press `F10`.

3.4.4. Terminal

Terminal enables you to access the Linux command line console to enter commands in the console.

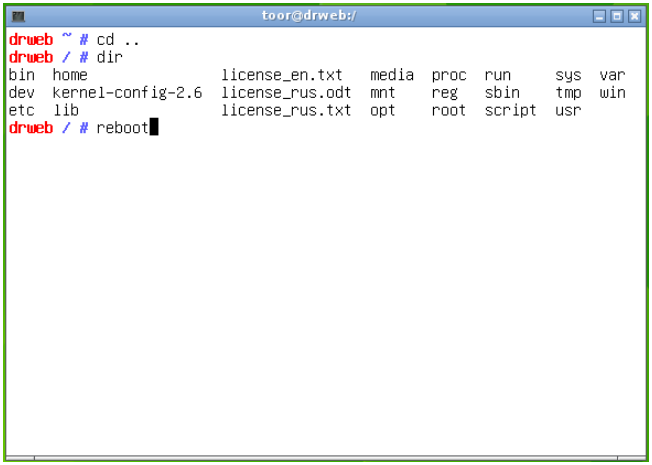
Launching Terminal in the graphic shell

You can launch Terminal in one of the following ways:

- double-click the Terminal icon  on the desktop;
- Click the icon  on the Taskbar;
- Select **System** and then select **Terminal** in the main system window of the graphic shell.

Working with Terminal

The following picture shows the Terminal window in the graphic shell:



The user types commands into the active line after the prompt character #. Before the prompt character, the line shows the user's name and the current working directory.

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

Closing the Terminal

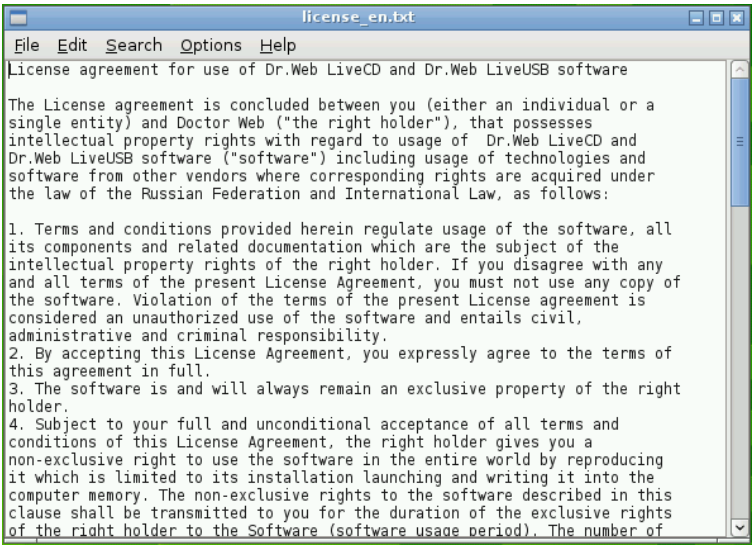
To finish working in **Terminal**, close the Terminal window or type the **exit** command.

3.4.5. Leafpad Text Editor

Leafpad is a windowing text editor available in the graphic shell and similar to the **Notepad** text editor used in Windows operating system.

Leafpad is created to be a simple, lightweight, and fast text editor for Unix-based systems. One of its advantages is short launch time on most computers which are up-to-date. Recent versions support printing when a printer is installed in the system. **Leafpad** works with text files without providing formatting features (for example, using different fonts, changing alignment).

The following picture shows the **Leafpad** text editor window:



Launching the text editor in the graphic shell:

To launch the text editor in the graphic shell, select **Utility** on the main system menu and then select **Leafpad**.

Launching the text editor in the console

The text editor is not available in the console. To view text files, switch to the graphic shell or use the nano text editor.

Working with text files

Working with text files in the **Leafpad** text editor is similar to working in other standard text editors:

- Items of the **File** menu allows to create a new file, open existing text files and specify the name to save the file;
- The **Edit** menu contains items for working with clipboard (copy, cut, paste, select all);
- The **Search** menu enables to search and substitute the selected fragment and move to the text line with the specified number.
- The **Options** menu allows to configure the following editor options:
  - Font;
  - Word wrap;
  - Line numbers.

For more information about the program visit Web site at http://tarot.freeshell.org/leafpad/.

Closing the text editor

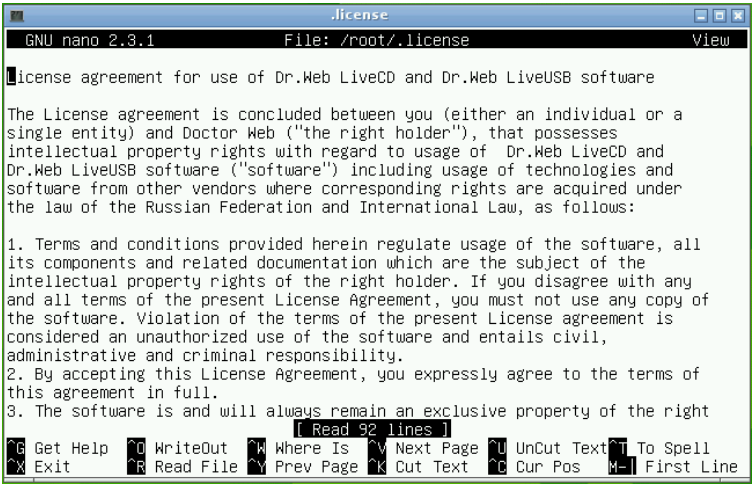
To finish working with the Text editor, close the window or select **File** and then select **Exit**.

3.4.6. Nano Text Editor

Nano is a console text editor available in both the graphic shell and console.

Nano is created for Unix-based systems and works with text files without providing formatting features (for example, using different fonts, changing alignment).

The following picture shows the **nano** text editor window displaying the text of the license agreement:



Launching the text editor in the graphic shell

Launching the **nano** text editor is not available by clicking a menu item or icon. However, if you select **License** on the main system menu, the text of the license agreement will open in the **nano** text editor.

Launching the text editor in the console

To launch the text editor in the console, type the following command:

```
nano
```

To open a text file in the **nano** text editor, type the following command:

```
nano <filename>
```

where `<filename>` - is the file directory including the filename. For example, to view the text of the license agreement, type the following command:

```
nano /license_rus.txt
```

To access the console from the graphic shell, use Terminal.

Working with text files

When the nano text editor is launched, the screen area displays three sections:

- **Title bar**, which contains the name and version of the text editor, the name of the opened file, and the editor operating mode. The **Title bar** displays on the top screen line;
- **View and edit area**, which occupies the full screen except the title bar and notification area.
- **Notification area and prompts of available commands**, which occupy the last three screen lines.

Working with **nano** is similar to working with other standard text editors:

- Text is entered at the position of the pointer;
- To move the pointer, use the arrow keys or `PgUP` and `PgDn` keys;
- Available key combinations and the corresponding actions are listed in the notification area.

For more information about the program, open Help (by the key combination `Ctrl` + `G`).

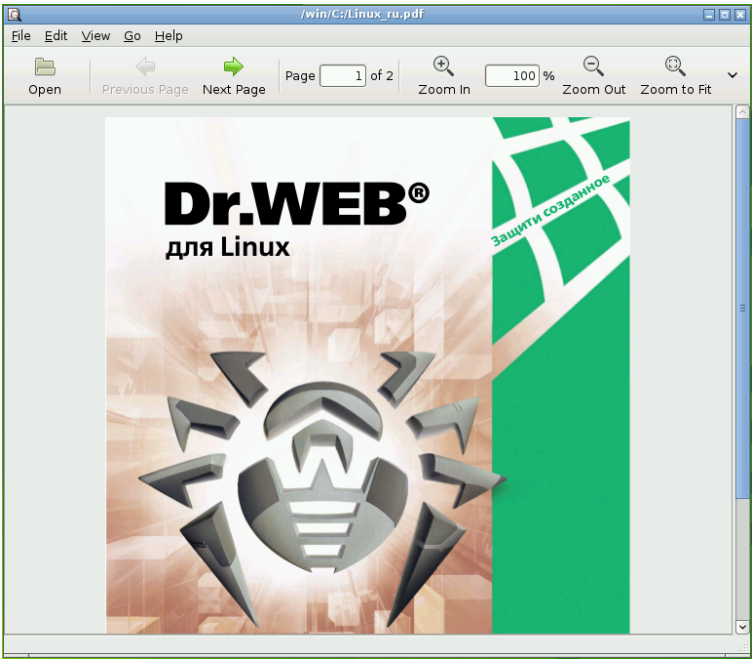
Closing the nano text editor

To finish working with the text editor, use the key combination `Ctrl` + `X`.

3.4.7. PDF Viewer

The **ePDFViewer** PDF viewer is a program that allows to open PDF-files in the view mode (read only mode) when working in the graphic shell.

The following picture shows the **ePDFViewer** PDF viewer window with an opened PDF file:



Launching PDF viewer in the graphic shell

To launch the PDF-viewer in the graphic shell, select **Office** on the main system menu and then select **ePDFViewer**.

Launching the PDF viewer in the console

Launching the PDF-viewer is not available in the console. To view PDF-files, switch to the graphic shell.

Viewing PDF-files:

- The items of the **File** menu allow to select and open the document, reload the opened document, save its copy and exit the application. You can also open the file for viewing by clicking **Open** on the toolbar.
- Selecting the **Find** item on the **Edit** menu enables the search panel. You can also choose the view mode (scrolling or selecting the text) on the **Edit** menu.
- The items of the **View** menu allow to control display of the additional panels (**Toolbar**, **Statusbar** and **Index** panels). This menu also allows to set the parameters of viewing the document (zoom and rotation).
- The items of the **Go** menu allow to navigate the pdf document (go to the previous, next, first or last page of the document).
- Buttons on the toolbar allow to navigate the pdf document (page through the pdf file) and adjust its scale.

Closing the PDF-viewer

To finish working with the PDF-viewer, close the window or select the **File** menu and then select **Close**.

4. Advanced Mode

To start **Dr.Web LiveUSB** in Advanced mode, click the **Advanced Mode** item on the Start boot menu.

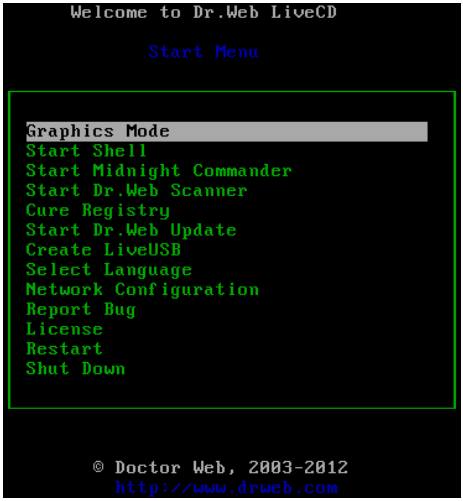
When starting the system in Advanced mode, the following actions are performed:

1. Linux operating system engine, used by **Dr.Web LiveUSB**, boots;
2. **Snapshot utility** (where you can choose one of the snapshots, create a new one, or disable using snapshots) boots;
3. Start menu appears.

You can also switch to the Advanced mode Start menu from the graphic shell by clicking **Exit** on the system menu.

4.1. Start Menu

The following picture shows the advanced mode menu of **Dr.Web LiveUSB** when choosing English language.



Use arrow keys ⇧ and ⇩ and ENTER key to select one of the following modes:

- **Graphics mode** allows to launch **Dr.Web LiveUSB** in the graphic shell (to switch back to the Advanced mode, click **Exit** on the main desktop menu, and the Start menu will appear again). In **Graphics mode** the current language of Advanced mode will be used. To change the language, select the item **Select Language** in the main window before switching to Graphics mode;
- **Start Shell** allows to bring up the command line of the Linux operating system (to exit the command line and open the Start menu in Advanced mode, use the **exit** command);
- **Start Midnight Commander** allows to launch the Midnight Commander inbuilt file manager. After closing the file manager, the Start menu appears;

- **Start Dr.Web Scanner** allows to launch the command-line version of the **Dr.Web** anti-virus scanner (**Dr.Web Console Scanner**) with default settings. After scanning, the Start menu appears. If you want to start scanning with changed settings, use the command line or file manager.
- **CureRegistry** allows to start the **CureRegistry** utility. After finishing work with the utility, the Start menu appears;
- **Start Dr.Web Update** allows to start updating the databases of **Dr.Web** anti-virus scanner. After finishing an update, the Start menu appears;
- **Create LiveUSB** allows to start the utility for creating a boot flash drive with **Dr.Web LiveUSB**. After the utility finishes working, the Start menu appears;
- **Select Language** allows to select the language, used in Advanced mode, including the language of the Start menu. English and Russian languages are available. English language is used by default. After the language is selected, the Start menu appears;
- **Network Configuration** allows to start the **Network configuration utility**. It is necessary to have right network configuration to update virus databases. After the utility finishes working, the Start menu appears;
- **Report Bug** allows to open the nano text editor to write the message about the **Dr.Web LiveUSB** error for sending it by e-mail to the **Doctor Web** development team. After the text editor finishes working, the Start menu appears;
- **License** allows to open the nano text editor displaying the text of the license agreement with the end user. The text of the license is always displayed in the selected language. After the text editor finishes working, the Start menu appears;
- **Restart** allows to reboot the computer.
- **Shut Down** allows to finish working with **Dr.Web LiveUSB** and shut down the computer.

During its operation **Dr.Web LiveUSB** uses a temporary RAM drive created when the system boots. Thus, all changes in program settings stored on the RAM drive will be lost when the computer reboots.

The **Quarantine** folder is also created on the RAM drive, so backup copies saved to **Quarantine** will be lost unless they are saved to one of the computer hard disk drives (physical disk drives) or a removable media.

To save the changes, use a snapshot (available in Advanced mode only).

4.2. Snapshots

Introductory remarks

Snapshots enable you to save all changes in **Dr.Web LiveUSB** settings as well as log files and files moved to **Quarantine** during scanning the system. You can save them on the local drives and flash storages. Using snapshots reduces memory footprint and helps to avoid program failures when scanning large archives.

Snapshots are saved as files into. `DrWebLive` folder in the root directory of the drive. You can delete the folder manually if you do not need saved snapshots. You can also move the folder to a flash drive and use it to boot **Dr.Web LiveUSB** configured according to your preferences on other computers (this option is particularly useful for those who boot **Dr.Web LiveUSB** from a USB flash drive).

Using snapshots requires minimum 512 MB of free space on the drive selected for storing snapshots.

Launching utility

The utility for using snapshots is launched automatically, when booting **Dr.Web LiveUSB** in Advanced mode.

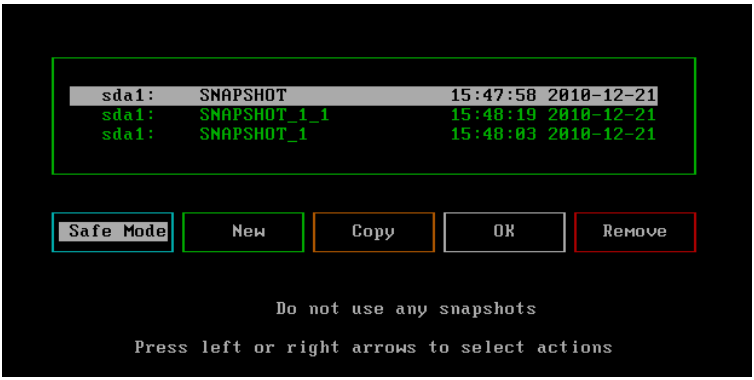
The utility launches only once per session, if Advanced mode is selected. If you selected another mode or refused using snapshots on Advanced mode startup, you cannot launch the utility during this session. In this case, reboot your computer to use snapshots.

When booting **Dr.Web LiveUSB** in Advanced mode, all available drives will be automatically scanned for existing snapshots and you will be offered to select a snapshot or create a new one. If no available disk partitions or flash drives are found on **Dr.Web LiveUSB** startup, snapshot list will not be displayed and the utility will automatically finish its work.

Working with snapshots

If the utility finds snapshots, they will be listed on the screen. If snapshots were not found on disk partitions and flash drives, the screen displays "**Snapshots not found**".

The following picture shows the screen on the utility startup with the list of existing snapshots:



For each snapshot, the following information is displayed:

- Disk (the device), where the snapshot is stored;
- Name of the snapshot;
- Date and time of the snapshot creation.

Use ⇧ and ⇩ arrow keys to select a snapshot. The selected snapshot is highlighted light gray line.

Below the list of snapshots the following items are displayed:

- **Safe Mode** - boot **Dr.Web LiveUSB** without snapshot support;
- **New** - create a new snapshot;
- **Copy** - copy selected snapshot to a different partition;
- **OK** - boot **Dr.Web LiveUSB** using selected snapshot;
- **Remove** - remove selected snapshot.

Remember that removing a snapshot is irreversible.

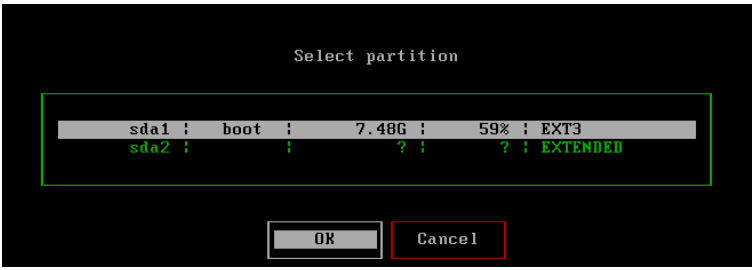
Use ⇦ and ⇨ arrow keys to select a required action. Press ENTER to activate the selected command. The selected command is highlighted light gray line.

To create a new snapshot

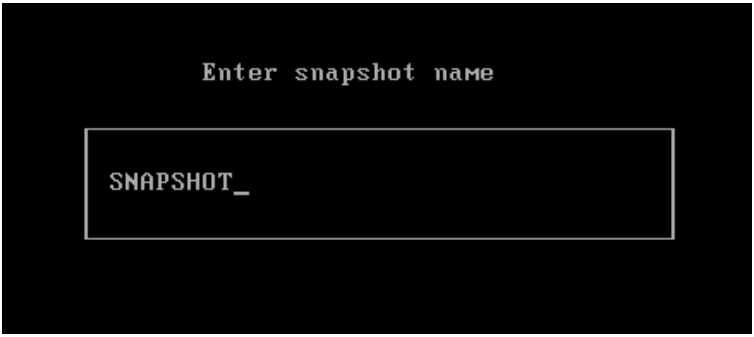
- Boot **Dr.Web LiveUSB** in Advanced mode;
- Select **New** below the list of snapshots and press ENTER;
- Select a disk partition in the appeared list where the new snapshot is to be stored. Use ⇧ and ⇩ arrow keys to select the required partition.
- To create a snapshot, select **OK**. If you decided to cancel snapshot creation, select **Cancel**.

Use ⇦ and ⇨ arrow keys to select the required command (as for selecting snapshots). Press ENTER to activate the selected command. The selected command is highlighted light background.

The following picture shows the screen of selecting partition:



- After the partition was selected, specify the name for the new snapshot. You can specify any name. After you typed the name, press ENTER. The following picture shows the screen of specifying the snapshot name:



Booting the system without using snapshots

- Boot **Dr.Web LiveUSB** in Graphics mode, or
- Boot **Dr.Web LiveUSB** in Advanced mode, select **Safe Mode** under the list of snapshots and press ENTER.

Booting the system using existing snapshot

- Boot **Dr.Web LiveUSB** in Advanced mode.
- Select the snapshot in the list.
- Select **OK** under the list of snapshots and press ENTER.

Copying snapshots

- Boot **Dr.Web LiveUSB** in Advanced mode.
- Select a snapshot in the list.
- Select **Copy** under the list of snapshots and press `ENTER`.
- Select in the appeared list a partition where the snapshot is to be copied and press `ENTER`.
- Specify the name of the copy and press `ENTER`.

After creating the copy, the main utility screen with the list of existing snapshots will display.

Deleting snapshots

- Boot **Dr.Web LiveUSB** in Advanced mode.
- Select a snapshot in the list.
- Select **Remove** under the list of snapshots and press `ENTER`.

After deleting the snapshot, the main utility screen with the list of existing snapshots will display.

5. Command Line Version of Dr.Web Anti-Virus

You can also work with **Dr.Web Console Scanner** in the console mode (with the command-line interface). To start **Console Scanner**, type the following command:

```
drweb <path> [command line options]
```

where `<path>` is the path to the folder or the filename mask which needs to be scanned.

Console Scanner launched without any option except a specified path uses the default options. The following example shows the command for scanning the C: drive with default settings:

```
drweb /mnt/disk/sda1
```

Report files, logged by **Console Scanner**, are stored in folder `/var/drweb/log`.

- To open the command-line in Advanced mode, click **Start Shell** on the menu;
- To open the command-line in the graphic shell, use **Terminal**.

For the list of options that you can specify for this command, see the section 5.1.

5.1. Command Line Options

Using options to start Console Scanner

You can use numerous options of the command line to configure **Dr.Web Console Scanner**. They are separated by blanks and begin with the '`-`' character (hyphen). The full list of options can be viewed by calling the command `drweb` with the `-?`, `-h` or `-help` options.

The most commonly used options can be grouped as follows:

- scanning area option;
- diagnosing options;
- actions options;
- interface options.

Scanning area options

Scanning area options define what objects are to be scanned for viruses. **Dr.Web Console Scanner** provides the following scanning area options:

- path – specifying the path to the objects which are to be scanned. You can specify several paths;
- @[+]<file> – scanning of objects listed in the specified file; the character '+' means that the file should not be deleted after the scanning; this file can contain paths to periodically scanned files and folders or the list of objects that are to be regularly scanned;
- `sd` – recursive search and scanning of files in subfolders, beginning from the current one;
- `fl` – follow the symbolic links for files and folders; links which lead to 'looping' are ignored;
- `mask` - ignoring filename masks.

Diagnosing options

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

- `al` – scanning of all files on the specified drive or folder;
- `ar[ d/m/r][ n]` – scanning of files in archives (ARJ, CAB, GZIP, RAR, TAR, ZIP, etc.)
  - `d` – deletion;
  - `m` – moving;
  - `r` – renaming of archives which contain infected objects;
  - `n` – disable output of the archive name.

Not only proper archives (for example, *.tar) are understood as archives here, but also their compressed formats (for example, compressed TAR archives `*.tar.bz2` and *.tbz);

- `cn[d/m/r][n]` – scanning of files in containers (HTML, RTF, PowerPoint);
  - `d` – deletion,
  - `m` – moving,
  - `r` – renaming of containers which contain infected objects;
  - `n` – disable output of the the container type.
- `ml[d/m/r][n]` - scanning of mail client files
  - `d` – deletion;
  - `m` – moving;
  - `r` – renaming of mail client files which contain infected objects;
  - `n` – disable output of the mail client files type.
- `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);
- `ha` – heuristic analysis of files, detection of unknown viruses.

Action options

The action options define the actions to be carried out by **Console Scanner** over infected and suspicious files. **Dr.Web Console Scanner** provides the following action options:

- `cu[d/m/r]` - curing of infected files
  - `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;
  - `i` – ignoring.
- `dls[d/m/r/i]` – actions for files containing dialers:
  - `d` – deletion;
  - `m` – moving;
  - `r` – renaming;
  - `i` – ignoring.
- `jok[d/m/r/i]` – actions for files containing jokes:
  - `d` – deletion;
  - `m` – moving;
  - `r` – renaming;
  - `i` – ignoring.
- `rsk[d/m/r/i]` – actions for files containing riskware:
  - `d` – deletion;
  - `m` – moving;
  - `r` – renaming;
  - `i` – ignoring.
- `hck[d/m/r/i]` – actions for files containing hacktools:
  - `d` – deletion;
  - `m` – moving;
  - `r` – renaming;
  - `i` – ignoring.

Interface options

The interface options determine the manner of scan results display. **Dr.Web Console Scanner** provides the following interface options:

- `v, version` – output of information about product version and anti-virus engine version;
- `ki` - output of information about key and its owner (only in UTF8 Transformation Format);
- `foreground[yes|no]` – launching **Console Scanner** in the foreground mode or background mode;
- `ot` – output of information on stdout (a standard output on the screen);
- `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.

Special options

Some options act as the opposite parameter if they end with the character '-'. Such options are:

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

For example, when launch scanning by the following command

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

The heuristic analysis, which is enabled by default, will be disabled.

Options enabled by default

The following options are enabled by default if **Console Scanner** is launched without any additional parameters and the configuration file was not changed:

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

These default options (including archive and packaged files, mail client files, recursive search, heuristics analysis and so on) are considered the

most rational for everyday scanning purposes and can be used in most typical cases. If one of the parameters set by default is not required, you can disable it by specifying «–» symbol after it, as it was shown in the example with the `-ha` option above (heuristic analysis).

Notes on using options

Disabling scanning of archived and packaged files dramatically decreases the security level as viruses are often spread as archives (often self-extracting) in the attachments. Documents of application programs (for example, Word, Excel) are potentially vulnerable to macro viruses and are attached to e-mail messages as archived or packaged files.

When launch **Console Scanner** with default parameters, infected files are not to be scanned. No action is performed on incurable or suspected files. To instruct **Console Scanner** to take actions on this objects, specify the conform options (actions options) in the command-line.

You can specify different actions for each specific case, but the following options are considered the most rational:

- `cu` - attempt to cure infected files and system areas without deletion, moving, or renaming;
- `icd` - deletion of incurable files;
- `spm` - moving of suspicious files;
- `spr` - renaming of suspicious files.

Launching **Console Scanner** with `cu-` option means that the program is to attempt to restore the original state of the infected object. It is possible only if detected virus is a known virus and the databases contain necessary instructions on curing. If the infected file is seriously damaged, attempt of curing may fail.

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 folder and instruct **Console Scanner** to check it by specifying this folder as the command option at the restart.

When **Console Scanner** is started with `icd` option specified, it will

remove all infected files from the disk. This option is suitable for incurable (irreversibly damaged by a virus) files.

`spr` option makes **Console Scanner** replace file extension with another specified extension (for example, *.#?? by default, that is, first extension character is replaced with "#" character). Enable this parameter for files of other operating systems (for example, DOS/ Windows) detected heuristically as suspicious. Renaming helps to avoid accidental execution of such files or downloading Word and Excel documents without further scanning in these operating systems and therefore prevents infection.

Moving option `spm` makes **Console Scanner** move infected or suspicious files to the **Quarantine** folder.

6. Utilites

Dr.Web LiveUSB features apart from **Scanner** a useful set of utilities:

- **Create LiveUSB**. It is used for creating the copy of **Dr.Web LiveUSB** to start the computer from the USB drive.
- **CureRegistry**. This utility is used for automatic scanning of the Windows registry and neutralize the consequences of malicious activity.
- **NetWorks configuration**. This utility is used to configure network connection necessary for virus databases update.
- **Reporing a bug**. This utility is used for sending e-mail messages about occured errors to the **Dr.Web LiveUSB** developers.

All the utilities can be launched in both console and graphic shell.

6.1. Create LiveUSB

Introductory remarks

Dr.Web LiveUSB enables to create a full copy of it. You can use the copy similar to **Dr.Web LiveUSB** CD drive on any computer that supports USB drive boot. In this case **Dr.Web LiveUSB** may be used as a portable operating system customized according to the certain user needs. It enables access to data on any computer regardless of the OS and software installed.

If you use a USB flash drive instead of a CD to boot **Dr.Web LiveUSB**, all changes made in the system are also stored on a temporary RAM drive. Thus, you need to use a snapshot to save the changes. The advantage of booting **Dr.Web LiveUSB** from a USB flash drive is that snapshots are stored on the same drive as the system.

USB flash requirements

To create a boot copy of **Dr.Web LiveUSB**, you can use any USB flash drive with enough free space (not less than 256 MB is required).

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

All **Dr.Web LiveUSB** 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.

To create a boot flash drive

1. Connect the flash drive to the computer. It takes maximum ten seconds for a connection to be registered.
2. Start **CreateLiveUSB** in one of the following ways:
   a) In the graphic shell:
      - Double-click the **CreateLiveUSB** icon  on the desktop;
      - Select the **Utility** item on the system menu and then select **Create Live USB**.

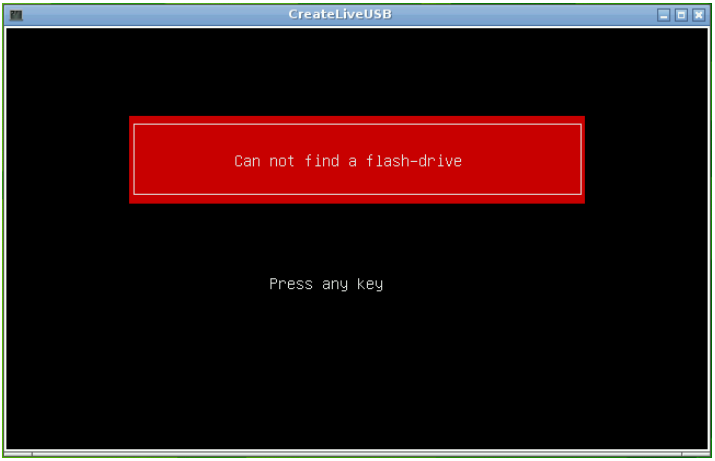
   b) In Advanced mode
      - Select the **Create LiveUSB** item on the menu.

   c) In the command-line:
      - Type the command

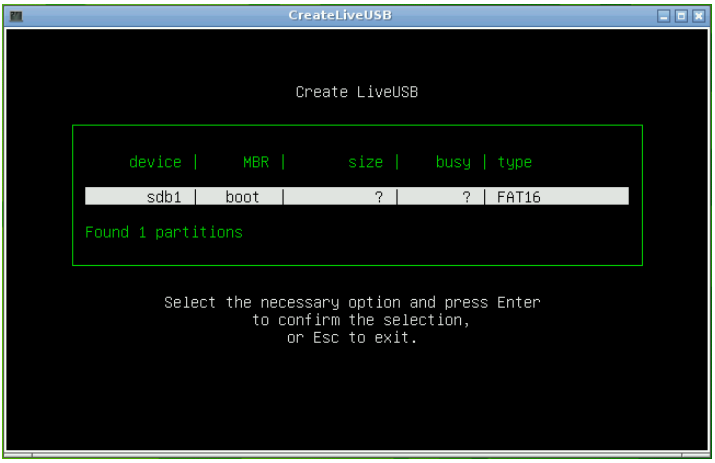
```
CreateLiveUSB
```

- To access the command-line in Advanced mode, select the **Start Shell** item;
- To access the command-line in Graphics mode, open **Terminal**.

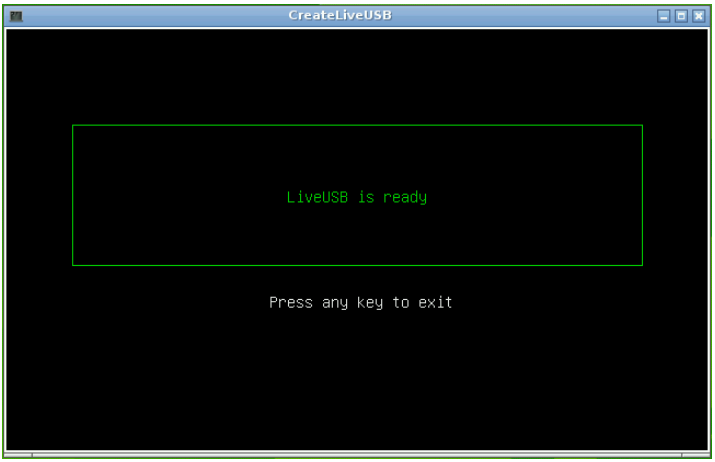
3. The **CreateLiveUSB** utility is to find all flash drives available in the system. If no flash drive is found, the utility will display the following message:



4. Select the required partition and press ENTER. The following picture shows the window when selecting the required device:



5. After selecting the device, file copying is to start automatically. After the utility finishes copying, the following message will display:



6. To exit the utility, press any key.

6.2. Cure Registry

Introductory remarks

The CureRegistry utility allows to automatically scan Windows registry (if the registry was found on the computer). During scanning the utility automatically neutralize all detected errors and damage caused by a virus.

When booting, **Dr.Web LiveUSB** automatically finds the Windows registry and mount it to its file system as a `/reg` folder. If you want to make some changes in the registry manually (for example, change registry keys, add, or delete keys), use the file manager.

CureRegistry provides standard scanning of the registry (the list of provided actions is presented below). This utility does not restore registry branches and keys deleted or changed by a user.

This utility restore the scanned keys to the default state using the registry backup copy. Thus, all changes in the registry branches that are under utility control will be lost.

Registry curing

1. Launch CureRegistry by one of the following ways:

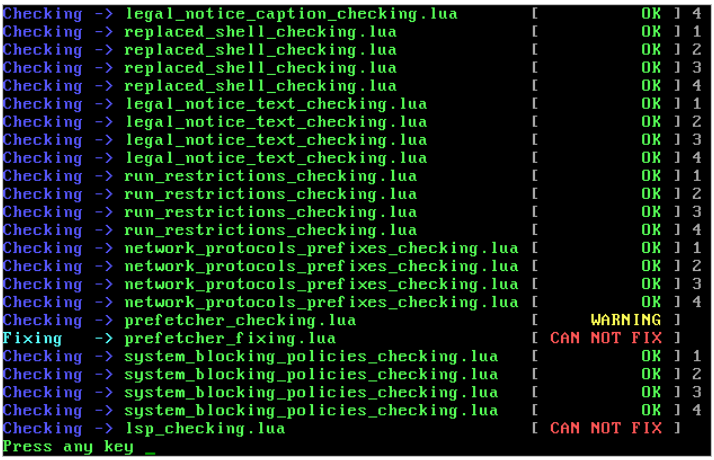
a) In the graphic shell:

- Select the **CureRegistry** item on the system menu.

b) In Advanced mode:

- Select the **CureRegistry** item on the Start menu.

2. When launched, the utility finds the Windows registry. If the registry is not found, the utility will display an appropriate message. Otherwise, the utility will start scanning the registry branches. The report about scanning with its results is to be displayed on the screen. The following picture shows an example of the report made during scanning:



3. To exit the utility after the registry is checked, press any key.

Scans provided by CureRegistry

The utility restores keys either to the original state set by default in Windows operating system or from the back up copy of the registry (`System.sav`).

The utility provides the following scans of the registry:

1. Scanning and restoring file associations of the operating system (`exe`, `com`, `bat`, `cmd`, `pif`, `scr`, `lnk`, `reg`).
2. Scanning and restoring Windows boot options in the safe mode.
3. Detecting and removing records about process debugger.
4. Detecting and eliminating changes in **Internet Explorer** settings:
   1) Adjustment of the home page is blocked;

2) The standard title of the **Internet Explorer** window is changed;
3) Closing of the browser window is blocked;
4) Navigation buttons are blocked;
5) The context menu is blocked;
6) Access to browser settings is blocked;
7) Selecting a folder to save files is blocked;
8) Viewing Web page HTML code is blocked;
9) Display of address bar is disabled;
10) Different settings are blocked.

5. Detecting and removing policies that block system work:
   1) Blocking of the control panel;
   2) Hiding of all elements on the desktop;
   3) Changing of screen settings is blocked;
   4) **Desktop** tab in the Screen properties window is blocked;
   5) **Screen saver** tab in the Screen properties window is blocked;
   6) **Settings** tab in the Screen properties window is blocked;
   7) **Appearance** tab is the Screen properties window is blocked;
   8) **Windows Update** settings are blocked;
   9) **System Restore** settings are blocked;
   10) Access to Network configuration is blocked;
   11) Configuration of automatic updates is blocked;
   12) Command-line interface (`cmd. exe`) is blocked;
   13) Display of the **My computer** icon is blocked;
   14) Registry is restricted from running applications;
   15) Control of installed applications is disabled;
   16) **Wallpaper** tab in the Screen properties window is blocked.
6. Detection and elimination of changes in user session startup options:
   1) Options of launching user shell (**Windows Explorer**) are changed;
   2) Message displayed on system startup is set;

3) Options of session initiation are changed (`userinit.exe`).

7. Restoring **Windows Explorer** settings:
   1) Display of drives in **Windows Explorer** is limited;
   2) Closing of **Windows Explorer** windows is blocked;
   3) Access to **Network neighborhood** is blocked;
   4) Session shutdown is blocked;
   5) Management item on **My computer** menu is blocked;
   6) The Context menu of the **Windows Control panel** is disabled;
   7) The Context menu of the **Start** button is disabled;
   8) The **Search** command on the **Start** menu is blocked;
   9) The **Run** command on the **Start** menu is blocked;
   10) Display of tray icons is disabled;
   11) Mounting of net drives is blocked;
   12) Display of subfolders on the **Start** menu is blocked;
   13) Access to printer settings is blocked;
   14) Items of the **Start** menu are blocked;
   15) Access to folder properties is blocked;
   16) Access to Taskbar properties and the **Start** menu is blocked;
   17) The item of the **Help** and **Support** menu is blocked.
8. Detection and elimination of Task manager blocking.
9. Detection and elimination of the registry editor blocking.
10. Detection and elimination of `hosts` file modifications.
11. Detection of LSP failures and repairing the LSP chain.
12. Detection and elimination of known Web sites blocking in the list of static routes.
13. Detection and elimination of the Task manager spoofing.
14. Detection and elimination of restrictions to running applications.
15. Detection and elimination of network prefixes changes.
16. Detection and elimination of **Prefetcher** disabling or **Prefetcher** nonoptimal configuration.

6.3. Network Configuration

Introductory remarks

Dr.Web LiveUSB uses a network connection on your computer to connect to the Internet. An Internet connection is used to update virus databases. You can also carry on e-mail correspondence and view Web sites by the mail client and the inbuilt browser (available only in the graphic shell).

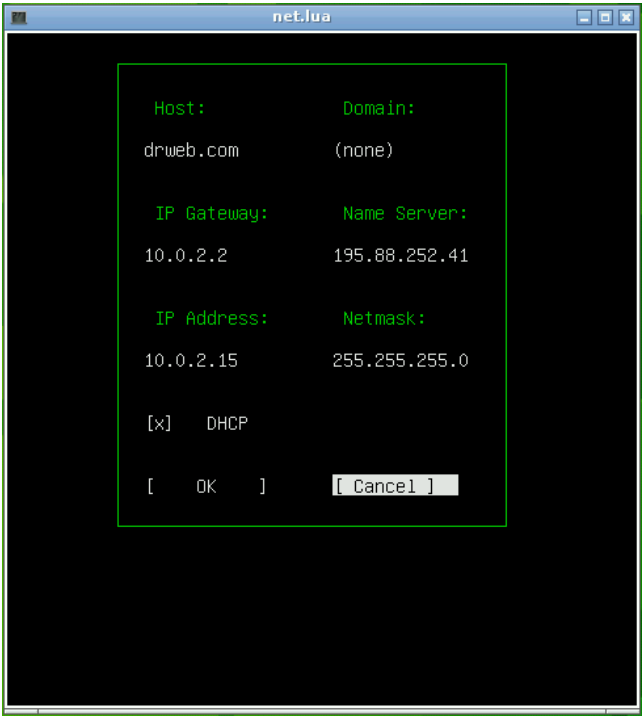
Dr.Web LiveUSB automatically identifies connection settings while launching. In most cases the settings are identified correctly and do not require manual adjustment. However, if a network connection is not found or there is no network access, you can try to adjust settings manually by the Network configuration utility.

Configuring network connection

1. Check that the computer is connected to network (network cable is plugged in).
2. Start **NetWork Configuration** in one of the following ways:
   a) In the graphic shell:
      - Select **Settings** on the system menu and then select **NetWorks Configuration**.

   b) In Advanced mode:
      - Select **Network Configuration** on the menu.

3. The following picture shows the screen when the **Network Configuration** utility is launched:



4. This utility allows to configure the following parameters of a network connection:
   - **Host name** (computer netname). By default the host name is `drweb.com`;
   - **Domain**. This parameter is not used. Do not specify the domain name;
   - IP address or host name of the **Gateway** (a computer that allows your computer to access the Internet);
   - IP address or host name of the **Name Server** (a computer that is used to support the Domain Name System);
   - **IP address** and **netmask**, used by this computer;

- **DHCP** check box (provides automatic receiving of an IP address and connection parameters from the gateway). **DHCP** is checked by default. When **DHCP** is checked, all the parameters except the host name are not available for configuring.

5. To move the pointer between the entry fields, press `TAB`. The active field is highlighted white. You can select or clear the check box (when it is in focus) by pressing `ENTER`.
6. To close the utility window and save the changes, click **OK** (switch to **OK** using `TAB` and then press `ENTER`). To close the utility window without saving the changes, click **Cancel**.

6.4. Reporting a Bug

If you use Graphic Shell, then to send a report about some bug in program operation, do the following actions:

- Select **Report Bug** item on the system menu;
- 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 arrow keys, select the **Report Bug** item on 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. Press the corresponding key (`Y` - to send a report, `N` - to discard it).

Appendix A. Types of Computer Threats

Herein, the term "threat" is defined as any kind of software potentially or directly capable of inflicting damage to a computer or network and compromising the user's information or rights (that is, malicious and other unwanted software). In a wider sense, the term "threat" may be used to indicate any type of potential danger to the security of the computer or network (that is, vulnerabilities that can result in hacker attacks).

All of the program types stated below have the ability to endanger the user's data or confidentiality. Programs that do not conceal their presence (e.g. spam distribution software and various traffic analyzers) are usually not considered as computer threats, although they can become threats under certain circumstances.

In **Dr.Web** classification, all threats are divided according to the level of severity into two types:

- **Major threats** – classic computer threats that may perform destructive and illegal actions in the system on their own (erase or steal important data, crash networks, etc.). This type of computer threats consists of software that is traditionally referred to as malware (malicious software), that is, viruses, worms and Trojans.

- **Minor threats** – computer threats that are less dangerous than major threats, but may be used by a third person to perform malicious activity. Also, mere presence of minor threats in the system indicates its low protection level. Among IT security specialists this type of computer threats is sometimes referred to as grayware or PUP (potentially unwanted programs) and consists of the following program types: adware, dialers, jokes, riskware, hacktools.

Major threats

Computer Viruses

This type of computer threats is characterized by the ability to implement its code into other objects. Such implementation is called infection. In most cases, the infected file becomes a virus carrier itself and the implemented code does not necessarily match the original. Most viruses are intended to damage or destroy data in the system.

In **Dr.Web** classification, viruses are divided by the type of objects which they infect:

- File viruses infect files of the operating system (usually executable files and dynamic libraries) and activate upon launching of the infected file.

- Macro-viruses are viruses that infect documents used by Microsoft® Office and some other applications supporting macro commands (usually, written in Visual Basic). Macro commands are a type of implemented programs (macros) written in a fully functional programming language. For instance, in Microsoft® Word macros can automatically initiate upon opening (closing, saving, etc.) a document.

- Script viruses are created using script languages and usually infect other scripts (e.g. service files of an operating system). They are also able to infect other file formats that allow execution of scripts and thus take advantage of scripting vulnerabilities in Web applications.

- Boot viruses infect boot records of diskettes and partitions or master boot records of fixed disks. They require very little memory and remain ready to continue performing their tasks until a system roll-out, restart or shut-down occurs.

Most viruses have some kind of protection against detection. Protection methods are being constantly improved and ways to overcome them are constantly being developed. All viruses may also be classified according to the type of protection that they use:

- **Encrypted viruses** cipher their code upon every infection to hamper their detection in a file, boot sector or memory. All copies of such viruses contain only a small common code fragment (the decryption procedure) that can be used as a virus signature.

- **Polymorphic viruses** also encrypt there code, but besides that they also generate a special decryption procedure that is different in every copy of the virus. This means that such viruses do not have byte signatures.

- **Stealth viruses** perform certain actions to disguise their activity and thus conceal their presence in an infected object. Such viruses gather the characteristics of an object before infecting it and then plant these "dummy" characteristics that mislead the scanner searching for modified files.

Viruses can also be classified according to the programming language in which they are written (in most cases, it is Assembler, high-level programming languages, script languages, etc.) or according to affected operating systems.

Computer Worms

Worms have become a lot more widespread than viruses and other types of computer threats recently. Like viruses, they are able to reproduce themselves and spread their copies, but they do not infect other programs and files (that is, they do not need host files to spread). A worm infiltrates a computer from a worldwide or local network (usually via an attachment to an e-mail message) and distributes its functional copies to other computers in the network. It can begin distributing itself either upon a user's action or in an automatic mode choosing which computers to attack.

Worms do not necessarily consist of only one file (the worm's body). Many of them have an infectious part (the shellcode) that loads into the main memory (RAM) and then downloads the worm's body as an executable file via the network. If only the shellcode is present in the system, the worm can be deleted by simply restarting the system (at which the RAM is erased and reset). However, if the worm's body infiltrates the computer, then only an anti-virus program can cope with it.

Worms have the ability to cripple entire networks even if they do not bear any payload (i.e. do not cause any direct damage) due to their intensive distribution.

In **Dr.Web** classification, worms are divided by the method of distribution:

- **Net worms** distribute their copies via various network and file-sharing protocols.
- **Mail worms** spread themselves using e-mail protocols (POP3, SMTP, etc.).
- **Chat worms** use protocols of popular messengers and chat programs (ICQ, IM, IRC, etc.).

Trojan Programs (Trojans)

This type of computer threats cannot reproduce itself or infect other programs. A Trojan substitutes a program that is used a lot and performs its functions (or imitates its operation). At the same time, it performs some malicious actions in the system (damages or deletes data, sends confidential information, etc.) or makes it possible for hacker to access the computer without permission, for example, to harm the computer of a third party.

A Trojan's masking and malicious facilities are similar to those of a virus. A Trojan may even be a component of a virus. However, most Trojans are distributed as separate executable files (through file-exchange servers, removable data carriers or e-mail attachments) that are launched by users or system tasks.

It is very hard to classify Trojans due to the fact that they are often distributed by viruses or worms and also because many malicious actions that can be performed by other types of threats are ascribed to Trojans only. Here are some Trojan types which are distinguished as separate classes in **Dr.Web**:

- **Backdoors** are Trojans that make it possible for an intruder to log on into the system or obtain privileged functions bypassing any existing access and security measures. Backdoors do not infect files, but they write themselves into the registry modifying the registry keys.

- **Rootkits** are used to intercept system functions of an operating system in order to conceal themselves. Besides, a rootkit can conceal processes of other programs (e.g. other threats), registry keys, folders and files. It can be distributed either as an independent program or as a component of another malicious program. There are two kinds of rootkits according to the mode of operation: User Mode Rootkits (UMR) that operate in user mode (intercept functions of the user mode libraries) and Kernel Mode Rootkits (KMR) that operate in kernel mode (intercept functions on the level of the system kernel, which makes it harder to detect).

- **Keyloggers** are used to log data that users enter by means of a keyboard. The aim of this is to steal personal information (i. e. network passwords, logins, credit card data, etc.).

- **Clickers** redirect hyperlinks to certain addresses in order to increase traffic of Web sites or perform DDoS attacks.

- **Proxy Trojans** provide anonymous Internet access through a victim's computer.

Trojans may also perform other malicious actions besides those stated above, for example, change the start page in a Web browser or delete certain files. However, other actions can also be performed by other types of threats (viruses and worms).

Minor Threats

Hacktools

Hacktools are programs designed to assist the intruder with hacking. The most common among them are port scanners that detect vulnerabilities in firewalls and other components of computer protection system. Besides hackers, such tools are used by

administrators to check security of their networks. Occasionally, common software that can be used for hacking and various programs that use social engineering techniques are designated as among hacktools as well.

Adware

Usually, this term refers to a program code implemented into freeware programs that force display of advertisements to users. However, sometimes such codes can be distributed via other malicious programs and show advertisements in Web browsers. Many adware programs operate with data collected by spyware.

Jokes

Like adware, this type of minor threats can not be used to inflict any direct damage to the system. Joke programs usually just generate messages about errors that never occurred and threaten to perform actions that will lead to data loss. Their purpose is to frighten or annoy users.

Dialers

These are special programs that are designed to scan a range of telephone numbers and find those where a modem answers. These numbers are then used to mark up the price of telephoning facilities or to connect the user to expensive telephone services.

Riskware

These programs were not intended as computer threats, but can potentially cripple or be used to cripple system security due to certain features and, therefore, are classified as minor threats. Riskware programs are not only those that can accidentally damage or delete data, but also ones that can be used by crackers or some malicious programs to do harm to the system. Among such programs are various remote chat and administrative tools, FTP-servers, etc.

Suspicious Objects

These are possible computer threats detected by the heuristic analyzer. Such objects can potentially be any type of threat (even unknown to IT security specialists) or turn out safe in case of a false detection.

Suspicious objects should be sent for analysis to the **Dr.Web Virus Laboratory**.

Appendix B. Fighting Computer Threats

There are many methods of detecting and neutralizing computer threats. All Dr.Web products combine these methods for the most reliable protection of computers and networks using flexible user-friendly settings and comprehensive approach towards security assurance.

Detection methods

Signature checksum scanning

This method is a type of signature analysis. A signature is a continuous finite byte sequence unique to a certain computer threat. If a signature from the virus database is found in a program's code which is being scanned, then a detection occurs.

Signature checksum scanning implies comparison of signature checksums rather then signatures themselves. This helps to reduce the size of the virus databases considerably and maintain reliability of traditional signature analysis.

Execution emulation

The program code execution emulation method is used to detect polymorphic and encrypted viruses in cases when implementation of signature checksum analysis is impracticable or extremely difficult (due to impossibility of extracting a reliable signature from a sample). This is how the method is performed: an emulator, which is a software model of the CPU, simulates execution of an analyzed code sample; instructions are executed in protected memory space (called emulation buffer) and are not passed on to the CPU for actual execution; when an infected file is processed by the emulator, the result is a decrypted virus body, which can be easily defined via signature checksum analysis.

Heuristic analysis

Heuristic analysis is used to detect newly created unknown computer threats, whose byte signatures have not yet been added to virus databases. Operation of the heuristic analyzer is based on defining and calculating the summary weight of certain features which are either typical for computer threats or, on the contrary, very rarely found in them. These features are characterized by their weight (a figure which defines the importance of a feature) and sign (positive sign means that the feature is typical for computer threats; negative means that the feature is not relevant for them). If the sum of these features for an object exceeds a certain operation threshold, the heuristic analyzer concludes that the object may be a threat and defines it as suspicious.

As with other hypothesis checking systems, heuristic analysis assumes the possibility of false positives (that is, type I errors when a threat is overlooked) and false negatives (that is, type II errors of a false detection).

Origins Tracing™

Origins Tracing™ is a unique non-signature threat detection algorithm developed by **Dr.Web** and used only in **Dr.Web products**. Combined with traditional signature-based scanning and heuristic analysis, it significantly improves detection of unknown threats. The .Origin extension is added to names of objects detected using the **Origins Tracing** algorithm.

Actions

To neutralize computer threats, **Dr.Web** products use a number of actions that can be applied to malicious objects. A user can leave the default settings, configure which actions to apply automatically, or choose actions manually upon every detection. Below is a list of possible actions:

- **Cure** is an action that can only be applied to major threats (viruses, worms and Trojans). It implies deletion of malicious code from infected objects as well as recovery of their structure and operability to the state in which it was before the infection if possible. Sometimes malicious objects are made of malicious code only (for example, Trojans or functional copies of computer worms) and for such objects to cure the system means to remove the whole object completely. Not all files infected by viruses can be cured, but curing algorithms evolve all the time.
- **Quarantine** (Move to Quarantine) is an action when the detected threat is moved to a special folder and isolated from the rest of the system. This action is preferable in cases when curing is impossible and for all suspicious objects. It is recommended to send copies of such files to the **Dr.Web Virus Laboratory** for analysis.
- **Delete** is the most effective action for neutralizing computer threats. It can be applied to any type of computer threat. Note that deletion will sometimes be applied to certain objects for which the **Cure** action was selected. This will happen in cases if the object consists of only malicious code and have no useful information (for example, curing a computer worm implies deletion of all its functional copies).
- **Rename** is an action when the extension of an infected file is changed according to a specified mask (by default, the fist character of the extension is replaced with #). This action may be appropriate for files of other operating systems (such as MS-DOS® or Microsoft® Windows®) detected heuristically as suspicious. Renaming helps to avoid accidental startup of executable files in these operating systems and therefore prevents infection by a possible virus and its further expansion.

- **Ignore** is an action applicable to minor treats only (that is, adware, dialers, jokes, hacktools and riskware) that instructs to skip the threat without performing any action or displaying information in report.
- **Report** means that no action is applied to the object and the treat is only listed in results report.

Appendix C. Contacting Support

Visit **Dr.Web Technical Support** Web site at http://support.drweb.com/.

If you encounter any issues installing or using company products, take advantage of the following Doctor Web support options:

- Download and review the latest manuals and guides at http://download.drweb.com/
- Read the frequently asked questions at http://support.drweb.com/
- Look for the answer in **Dr.Web knowledge database** at http://wiki.drweb.com/
- Browse **Dr.Web official forum** at http://forum.drweb.com/

If you have not found solution for the problem, you can request direct assistance from **Doctor Web Technical Support** by filling in the web-from in the corresponding section of the support site at http://support.drweb.com/.

For regional office information, visit the **official Doctor Web Web site** at http://company.drweb.com/contacts/moscow.