Dr.WEB®

Anti-virus for Novell NetWare

Administrator Manual

Defend what you create

TRADEMARKS

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

DISCLAIMER

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

Dr.Web Anti-virus for Novell® NetWare®
Version 5.01.2
Administrator Manual
30.07.2012

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

Chapter 1. Introduction

This program is a representative of the 32-bit family of the **Dr.Web** anti-virus programs. This family includes programs for Microsoft® Windows® and Unix® (Linux®, FreeBSD® etc.) operating systems, as well as anti-viruses for MS-DOS® 386, Novell® NetWare®, and IBM® Operating System/2®.

Dr.Web Anti-virus for Novell® NetWare® (hereafter, **Dr.Web Anti-virus**) is a NetWare Loadable Module® (NLM®) that runs on a server under Novell NetWare 4.11, 4.2, 5.1, 6.0, 6.5. The program can be administered from the server console or a remote console on a workstation.

Dr.Web Anti-virus supports the following features:

- Scheduled scanning of network server volumes
- On-demand scanning of network server volumes upon the administrator's request
- On-access scanning of files that are written to and read from the server
- Selection of objects to scan, such as files, directories and volumes
- Flexible manipulation of infected or suspicious files
- Multiple simultaneous scan processes
- Adjustable priorities and control over scan processes
- Scan logging with configurable verbosity

Conventions

The following conventions are used in the Manual:

Symbol	Description
⚠ Warning	Warns about possible errors.
Dr.Web Agent	Names of **Dr.Web** products and components.
Anti-virus network	A term in the position of a definition or a link to a definition.
<IP-address>	Placeholders.
Cancel	Names of buttons, windows, menu items and other user interface elements.
CTRL	Keyboard keys names.
`C:\Windows\`	Code examples, input to the command line and application output.
Configuration	Cross-references or Internal Hyperlinks to web pages.

The following abbreviations are used in this manual:

- CPU - Central Processing Unit;
- GUI - Graphical User Interface;
- OS - Operating System.

Contacting Support

Support is available to customers who have purchased a commercial version of **Dr.Web** products. Visit **Doctor Web Technical Support** website 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 website** at http://company.drweb.com/contacts/moscow.

Chapter 2. Licensing

The *key file* regulates the use rights for the product.

Key File

A key file has the .key extension and contains, among other, the following information:

- Licensed period for the **Dr.Web Anti-virus**
- List of components licensed to the user
- Period of versions updating (the subscription period, it may be different from the license period)
- Licensed versions of the anti-virus
- Other restrictions (the number of protected computers, etc.)

There are two types of key files:

- *License key file* is purchased with the Dr.Web software and allows purchasers to use the software and receive technical support. Parameters of the license key file are set in accordance with the software's license agreement. The file also contains information about the purchaser and seller.
- *Demo key file* is used for evaluation of **Dr.Web** products. It is distributed free of change and provides full functionality of the software. However demo key files have limited validity period and cannot be renewed.

A *valid* license key file satisfies the following criteria:

- License is not expired.
- The license applies to all components of the product.
- Integrity of the license key file is not violated.

If any of the conditions are violated, the license key file becomes invalid, **Dr.Web Anti-virus** stops detecting and neutralizing malicious programs.

Acquiring Key Files

Commercial users who have purchased **Dr.Web Anti-virus** from certified partners receive a license key file. The parameters of this key file governing the user rights are set in accordance with the user agreement. Such file also includes information about the customer and the selling company.

You can receive a license key file in one of the following ways:

- By email in an archived attachment
- With the Dr.Web plugin distribution kit
- On separate media

To acquire a license key file by email

1. Launch an Internet browser and go to the site which is specified on the product registration card supplied with your copy of the product.
2. Fill in the registration form.
3. Enter the serial number which is typed on the registration card.
4. The license key file is archived and sent to the email address you specified in the registration form. Extract the license key file and copy it to the **Dr.Web Anti-virus** installation directory.

For demonstrative purposes Doctor Web may provide you with a *trial license key file*. Trial license allows you to access full functionality of the Dr.Web plugin for a short-term period. No support is provided during trial period. On the expiration of the trial license, you will need to purchase a full license to continue working with the product.

To receive a trial license key file by email, fill in the registration form at http://download.drweb.com/demoreq/.

For more information on licensing and types of license key files, visit the **Doctor Web** official website at http://www.drweb.com.

Chapter 3. Installation

All Dr.Web family products can be installed in the same directory. The distribution packages of all family products include the following common files:

- drweb32.dll (**Dr.Web engine**)
- drwebase.vdb (main **Dr.Web virus database**)
- **Dr.Web virus database add-ons** (*.vdb)
- drweb32.ini (**Dr.Web configuration file**)

The configuration file is created common to all family products in the installation directory. Settings for each product are stored in the respective sections of the file. **Dr.Web virus database add-ons** should also be stored in the installation directory.

For more information on configuration file, see Configuration. For more information on updates, see Update.

Distribution package

The distribution package for **Dr.Web Anti-virus** includes the following files:

- drwebnw.nlm — core program module
- drwebnw.imp — component necessary to enable the On-access mode
- drweb32.dll — core program module (**Dr.Web engine**)
- drwebase.vdb — main **Dr.Web virus database** (more supplementary virus databases may be included in the distribution, named after the format DRW*vvvnn*.VDB, where *v.vv* is the **Dr.Web Anti-virus** version number for which the supplementary database was issued, and *nn* is the serial number of the supplementary database issued for this version)
- en-drwnw.txt — program documentation in English
- ru-drwnw.txt — program documentation in Russian (the

distribution package may also contain manuals in other languages)

- drwebupn.nlm — **updater** for executable files and virus databases (a new component supplied starting from this version; for more information, see Chapter 8. Update).

Besides, the distribution package may include language resource files named <language>-drwnw.dwl (for example, ru-drwnw.dwl, de-drwnw.dwl, etc.).

Installing Dr.Web Anti-virus

To install Dr.Web Anti-virus

1. Create an installation directory on your server (for example, DRWEB).
2. Unpack the **Dr.Web Anti-virus** distribution archive into the installation directory.

Selecting Language Modes

The default interface language of the program is English. To set a different language, modify the settings in the [NetWare] section of the configuration file.

To change language mode

You must unload **Dr.Web Anti-virus** before editing the configuration file. Otherwise your changes will be lost, since the program overwrites this file after each session with recently used settings.

1. Open the **Dr.Web** configuration file for editing in a text editor. By default, the configuration file is located in the installation directory and is called drweb32.ini.
2. In the LngFileName string of the [NetWare] section, specify in

quotation marks the name of the language resource file.

The language resource files have names like <language>-drwnw.dwl. For example, ru-drwnw.dwl, de-drwnw.dwl, etc.

3. Save changes in the configuration file.

Launching Dr.Web Anti-virus

Dr.Web Anti-virus can be launched either from the server, or from a remote console.

To launch Dr.Web Anti-virus

Run the following command from the server or a remote console:

`load [`*<full server path>*`]drwebnw`, where *<full server path>* is the path to the **Dr.Web Anti-virus** installation directory on the server. If the directory directory is on the search path, you need not enter the full path.

If drwebnw.nlm fails to load and the following (or similar) message appears: "`...Module drwebnw.nlm cannot be loaded until CLIBAUX loaded...`", it means that you have not installed latest updates and patches for Novell NetWare. You can find required updates at http://support.novell.com/patches.html.

To provide e-mail notification of the administrator, the tcpip.nlm module is to be loaded on the server and the TCP/IP protocol set up. Otherwise, the following error message will be displayed at **Dr.Web Anti-virus** startup: "`TCPIP.NLM not loaded (error <error number>). Some additional features are not available.`"

Chapter 4. Configuration

Dr.Web Anti-virus settings can be configured via the **Setup** menu, or the drweb32.ini configuration file.

Configuration File

All configuration settings are contained in drweb32.ini. This file is common for all **Dr.Web** family products and is located in the same directory as the program module drwebnw.nlm. If the configuration file is missing, the program will use the default settings. In any case all settings of the last session are saved to the configuration file automatically.

General Settings

You can configure **Dr.Web Anti-virus** general settings in the **Setup** menu.

The **Setup** menu allows you configure the following settings:

Setting	Description
Scan settings	The standard parameters applicable by default to all scans unless individual options are set (for more information, see General scan settings).
Virus bases	The names of the virus databases used. Masks are allowed.
Move files to	The directory where to move infected files to. This directory is used by all the processes.
Rename files to	The mask to use when generating extensions of renamed files. This mask is used by all the processes.
If virus found	Additional actions to perform on detection of viruses:

Setting	Description
	• **Create flag file** — create a flag file, i.e. a zero-length file indicating a certain event (in this case, virus detection on the server). It makes sense if your system is running some application that can monitor and respond to this flag. The name of the flag file is specified through **Setup | Miscellaneous | Flag file name**. • **Ring the bell** — enable sound alert on the server console. • **Disconnect station** — disconnect the workstation from which the virus attack is initiated. • **Send message** — send a message to the workstation from which the virus attack is initiated.
Miscellaneous	Miscellaneous options: • **Disconnected users** — views the list of disconnected users. Press DEL to delete a disconnected user from the list. This will allow the user to reconnect to the server. • **Send messages to** — lists the users or groups that are always notified of virus detection on the server. This **Dr.Web Anti-virus** version supports this option under NetWare 4.x and higher provided that the user or group is in Bindery Context set on the server. • **E-mail notification** — defines e-mail notification of virus detection, when a virus is detected during on-access scanning. • **Disconnect message**, **Virus found message**, **Suspected file message** — the texts for the corresponding messages. • **Flag file name** — the name of the flag file.

Optional Settings

Most settings can be configured through the menu system. However, certain settings can be changed only by editing the configuration file as described below.

The configuration file is a text file that can be edited in any text editor. This file is shared by all the **Dr.Web** family products. Settings used by **Dr.Web Anti-virus** are grouped in following sections:

- `[NetWare]` — general settings
- `[NetWare:Transit]` — transit directories settings

[NetWare]

The [NetWare] section of the configuration file allows you to configure the following settings:

Setting	Description
LngFileName	The name of the language resource file used by **Dr.Web Anti-virus**. For example, LngFileName = "ru-drwnw.dwl". If this setting is an empty string (LngFileName = "") **Dr.Web Anti-virus** uses the built-in language (English).
TempPath	The directory in which **Dr.Web Anti-virus** creates temporary files. For example, TempPath = "SYS:\TEMP". If the specified directory does not exist, **Dr.Web Anti-virus** creates it at start. If TempPath is not specified, the temporary files are created in the installation directory. Temporary files are deleted automatically as they become unnecessary
UpdateFlags	The list of files whose modification requires that Dr.Web virus databases be automatically reloaded

Setting	Description
	Dr.Web Anti-virus implements an automatic databases reload feature which allows to start using new **Dr.Web virus databases** and add-ons without restarting **Dr.Web Anti-virus**. For this, one or more files are assigned as flag files in the UpdateFlags string. When any of the files is modified, all virus databases are reloaded. The interval between checks of flag files is set in the UpdatePeriod string. For example, you may use the drwtoday.vdb file as a flag file(a hot **Dr.Web virus database add-on**).
UpdatePeriod	The interval (in minutes) at which the files listed in UpdateFlags are repeatedly checked for modification. Set UpdatePeriod=0 to disable automatic databases reloading. If you use the Updater, it is recommended to set UpdatePeriod=0.
EnableDelete ArchiveAction	Use this setting to enable or disable deleting of archives (for information on handling of infected archives, see Infected archives, mail and containers). The default value is No (disabled), to enable deleting, set EnableDeleteArchiveAction=Yes.

To configure optional Dr.Web Anti-virus settings

⚠ You must unload **Dr.Web Anti-virus** before editing the configuration file. Otherwise your changes will be lost, since the program overwrites this file after each session with recently used settings.

1. Open the **Dr.Web** configuration file for editing in a text editor. By default, the configuration file is located in the installation directory and is called drweb32.ini.
2. In the `[NetWare]` section, set general settings.
3. Save changes in the configuration file.

[NetWare:Transit]

Dr.Web Anti-virus supports the so called "transit directories" used, for instance, in some e-mail systems. This mechanism employs several directories on the server, one of which servers as transit and other directories are used for sorting. **Dr.Web Anti-virus**, uses three post-transit destinations that receive and hold the following files:

- Normal (uninfected, clean) files
- Infected files
- Suspicious files

At startup and during scan sessions, depending on the scan results, **Dr.Web Anti-virus** moves files from the transit directory to respective post-transit directories

⚠ Enable on-access scanning to have files sorted from the transit directory.

The [NetWare:Transit] section of the configuration file allows you to configure the following directory settings:

Setting	Description
TransitPath	The transit directory.
CheckedFiles	The directory for normal (uninfected) files.
InfectedFiles	The directory for infected files.
SuspiciousFiles	The directory for suspicious files.

To configure transit directories settings

⚠ You must unload **Dr.Web Anti-virus** before editing the configuration file. Otherwise your changes will be lost, since the program overwrites this file after each session with recently used settings.

1. Open the **Dr.Web** configuration file for editing in a text editor. By default, the configuration file is located in the installation directory and is called drweb32.ini.
2. In the `[NetWare:Transit]` section, set transit directories settings.
3. Save changes in the configuration file.

Anti-virus Scan Settings

Anti-virus scan settings are configured via the **Scan settings** item of the **Setup**, **Scheduler** and **On-access** menus.

Through the **Setup** menu, you can set general scan parameters applicable by default to all scans. On the **Scheduler** and **On-access** menu, you can set individual parameters for the respective processes.

General Scan Settings

In the **Scan settings** item of the **Setup** menu you can select catalogs and file types to be scanned (not to be scanned), program reaction to virus detection, etc.

The **Scan settings** item of the **Setup** menu allows you to configure the following settings:

Setting	Description
Options	Basic options.

Setting	Description
Infected files	Handling of infected files.
Suspicious files	Handling of suspicious files.
Incurable files	Handling of infected files that cannot be cured.
Adware	Handling of adware.
Dialers	Handling of dialers.
Jokes	Handling of jokes.
Riskware	Handling of riskware.
Hacktools	Handling of hacktools.
Infected archives	Handling of infected archives.
Infected mail	Handling of infected e-mail files.
Infected containers	Handling of infected containers.
File types	Files to scan.
Exclude paths	Paths to exclude from scan process.
Exclude files	Files to exclude from scan process.
CPU_usage factor	Priority of this scan.

Options

These basic settings include:

- **Heuristic analysis** — enable/disable the heuristic analyzer during scanning. This scan method is intended to enhance scanners' ability to apply signatures and identify modified versions, which allows to detect unknown viruses with high efficiency.
- **Check archives** — enable/disable checking of files within archives.
- **Check mail files** — enable/disable checking of e-mail files (UUENCODE, XXENCODE, BINHEX and MIME).

Infected Files

This option tells the scan process how to handle an infected file:

- **Log only** — notifies of virus detection only, specifying the infected file and the virus.
- **Move** — moves the infected file to a special directory. You can specify this directory in the basic options: **Setup | Move files to**. Note that this directory is used by all scan processes.
- **Delete** — deletes the infected file.
- **Rename** — renames the infected file. The renamed file has the same name, but receives a different extension. You can set the mask for generating the extension in the basic options: **Setup | Rename files to**. Note that this mask is used by all scan processes.
- **Cure** — removes the virus code from an infected file.

Suspicious and Incurable Files

Suspicious files are the files reported by the **Dr.Web heuristic analyzer** as possibly infected by an unknown virus.

Incurable files are the files that are infected by a familiar virus, however they cannot be cured.

Program actions over suspicious and incurable files are similar to those for infected files section above, but the **Cure** option is inapplicable.

Adware, Dialers, Jokes, Riskware, and Hacktools

The options for malicious software of the types listed in the title are similar to those for suspicious and incurable files, but one more **Ignore** action is added.

Infected Archives, Mail, and Containers

The options for archives and files of the types listed in the title are similar to those for suspicious and incurable files.

⚠ The specified action is applied to the whole archive containing an infected or suspicious file, as well as malicious software.

Deleting of archives is disabled by default. To enable it, edit the EnableDeleteArchiveAction parameter in the configuration file.

File Types

This setting determines what files are to be scanned by the process. Choose one of the following:

- All scans all files.
- By type scans according to a preset list of extensions. The list can be viewed and edited. To add a new extension to the list, press INS. To delete an extension, press DEL. You can use masks when specifying an extension.

Excluding Paths and Files

Here you can determine which directories/volumes and files (without the paths) are to be excluded from checking in this scan process. Masks are allowed. To browse server volumes (only for **Exclude paths**), press INS in the path edit window.

CPU Usage Factor

This option specifies the priority of this scan process in the system. The higher the numerical value of the priority, the more CPU usage is allowed.

Optional Scheduled Scan Settings

You can configure optional settings of scheduled scans in the **Scan settings** item of the **Scheduler** menu.

To view the list of scheduled scan processes, select **Scheduler** in the Control Panel. To add a new process, press INS, and DEL to remove a process.

Every process to be performed according to the schedule requires the following parameters:

- **Scan settings** — individual settings for every scan (for information on the options, see to General Scan Settings). By default, the settings specified in **Setup | Scan settings** are applied.
- **Scan paths** — specify the list of directories/volumes to be checked by the process. To browse server volumes, press [Ins] in the edit window.
- **Days of week** — specify the days of week on which the process is to be started.
- **Days of month** — specify the days of month on which the process is to be started.

- **Months** — specify the months on which the process is to be started.
- **Time** or **Interval** — the time parameter specified as HH:MM; whether it is time or interval depends on the Modes setting below.
- **Modes**:
    - If the **By time** mode is enabled, the process starts at the time specified by the **Time** parameter.
    - If the **By interval** mode is enabled, the process starts once the specified period of time has elapsed; the value of the **Interval** parameter is interpreted not as a moment in time, but as a length of a time interval.
    - Besides, you may put a scheduled process on hold by selecting **Hold**. Processes with this attribute enabled remain on the list of scheduled processes and keep all the options, but they are not performed.

The value of the **Days of week**, **Days of month**, and **Months** parameters counts only in the **By time** mode and is ignored in the **By interval** mode.

A process scheduled in the **By time** mode runs on the days on which both conditions stipulated by the **Days of week** and **Days of month** parameters are satisfied at the same time.

Scan attributes are displayed in the list of processes. At the end of each line you can see the activity indicator and the launch mode:

- - — the process is included in the schedule but is inactive now
- ! — the process is active, i.e. is now running
- H — the process is put on hold
- i — the process runs by interval
- t — the process runs by time

Optional On-access Scan Settings

You can configure On-access optional settings in the **Scan settings** item of the **On-access** menu.

This scan process controls files that a workstation writes to or opens on the server. The process scans for viruses when the server executes a workstation's request for a file transaction.

When a workstation writes a new file to the server or modifies an existing file, this file is locked and cannot be accessed from other workstations until it has been checked.

Adjustable parameters:

- **Scan settings** — on-access scanning parameters (for information on the options, see to General Scan Settings)
- **Modes** — what file transactions are to be intercepted for virus check on-access:
  - **Open files** — when a workstation opens a file on the server
  - **Write files** — when a workstation modifies an existing file on the server
  - **Create files** — when a workstation creates a new file on the server

Each of these modes can be enabled or disabled. Disabling all three modes disables the on-access scanning.

Chapter 5. Integration with Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite (hereinafter, **Dr.Web ESS**) provides organization and centralized control of integrated and complex protection of anti-virus network computers.

Dr.Web Enterprise Server provides for

- centralized (without user intervention) installation of the antivirus packages on computers,
- centralized setup of the anti-virus packages,
- centralized virus databases and program files updates on protected computers,
- monitoring of virus events and the state of the anti-virus packages and OS on all protected computers.

You can configure integration of **Dr.Web Anti-virus** with **Dr.Web ESS**.

For integration with Dr.Web ESS anti-virus network, it is required:

- **Dr.Web Anti-virus for Novell NetWare** version 5.0 and later
- **Dr.Web Agent for Novell NetWare** version 6.0 and later
- **Dr.Web Enterprise Security Suite** version 6.0 and later

When **Dr.Web anti-virus solutions** are integrated with **Dr.Web ESS**, users must have appropriate permissions to configure anti-virus packages on their computers.

For details on permission restriction, see **Dr.Web Enterprise Suite Administrator Guide**.

Dr.Web Agent for Novell NetWare

Dr.Web Agent for Novell NetWare (hereinafter, **Dr.Web Agent**) is a NetWare module included in the **Dr.Web Enterprise Security Suite** anti-virus package. Actual functions performed by **Dr.Web Agent** depend on its operation mode.

Dr.Web Agent can operate in one of the following modes:

- *Standalone*
- *Enterprise*

In the Enterprise mode, Dr.Web Agent serves the following functions:

- provides a connection with the **Enterprise Server**,
- updates and sets up the anti-virus package components,
- defines operation policy of anti-virus packages according to current license,
- sends the results of scans and virus events statistics to the antivirus **Server**.

In the *Standalone* mode, **Dr.Web Agent** do not establish connection with the **Enterprise Server**. For integration with **Dr.Web Enterprise Security Suite**, select the *Enterprise* mode.

Functionality of **Dr.Web Agent** is described in **Dr.Web Anti-virus for Novell NetWare User Manual**.

Configuring Integration

If the **Dr.Web Anti-virus** is already installed on the Novel NetWare server, it is possible to connect this server to the **Dr.Web Enterprise Security Suite** anti-virus network. For integration, it is required to install and configure the **Dr.Web Agent** on the server to operate in *Enterprise* mode.

For details on installing and configuring the **Dr.Web Agent**, refer to **Dr.Web Anti-virus for Novell NetWare User Manual**.

⚠ Do not install other anti-virus programs, including other **Dr.Web** solutions, on computers with an installed **Dr.Web Agent**. Installing two anti-virus programs on one computer may lead to system crash or loss of important data.

To configure integration with Dr.Web Enterprise Security Suite

1. Launch **Dr.Web Agent**.
2. Register the remote computer at **Enterprise Server**.
3. Configure settings of **Dr.Web Anti-virus** via the **Dr.Web Control Center**.

For details on managing remote anti-virus solutions via the **Dr.Web Control Center**, refer to **Dr.Web Enterprise Suite Administrator manual**.

Chapter 6. Anti-virus Scan

The program uses several fields to display information:

- Statistics: **Next Event**, **Status**, current date and time
- Main Control Panel
- Info about the program
- Info about the license and current mode

The Control Panel facilitates setting, controlling and monitoring the operation of the anti-virus. See below the description of Control Panel elements:

Element	Description
Setup	Set main options of the anti-virus.
Monitor	Control, view and launch scans on-demand.
Scheduler	Schedule scan processes.
On-access	Configure on-access scan processes.
Log	View the event log.
Exit	Terminate **Dr.Web Anti-virus**.

Detection Methods

The **Dr.Web anti-virus solutions** use several malicious software detection methods simultaneously, and that allows them to perform thorough checks on suspicious files and control software behaviour:

1. The scans begin with *signature analysis*, which is performed by comparison of file code segments to the known virus signatures. A signature is a finite continuous sequence of bytes which is necessary and sufficient to identify a specific virus. To reduce the size of the signature dictionary, the **Dr.Web anti-virus solutions** use signature checksums instead of using complete signature sequences. Checksums uniquely identify signatures which preserves correctness of virus detection and neutralization. The **Dr.Web virus databases** are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.
2. On completion of signature analysis, the **Dr.Web anti-virus solutions** use the unique **Origins Tracing™** method to detect new and modified viruses which use the known infection mechanisms. Thus the **Dr.Web** users are protected against such viruses as notorious blackmailer Trojan.Encoder.18 (also known as gpcode). In addition to detection of new and modified viruses, the **Origins Tracing** mechanism allowed to considerably reduce the number of false triggering of the **Dr. Web** heuristics analyser.
3. The detection method used by the *heuristics analyser* is based on certain knowledge about attributes that characterize malicious code. Each attribute or characteristic has weight coefficient which determines the level of its severity and reliability. Depending on the sum weight of a file, the heuristics analyzer calculates the probability of unknown virus infection. As any system of hypothesis testing under uncertainty, the heuristics analyser may commit type I or type II errors (omit viruses or raise false alarms).

While performing any of the abovementioned checks, the **Dr.Web anti-virus solutions** use the most recent information about known malicious software. As soon as experts of **Doctor Web Virus**

Laboratory discover new threats, the update for virus signatures, behaviour characteristics and attributes is issued. In some cases updates can be issued several times per hour. Therefore even if a brand new virus passes through the **Dr.Web resident guards** and penetrates the system, then after update the virus is detected in the list of processes and neutralized.

Launching Scan Processes

Anti-virus protection is implemented by means of scan processes. There are three types of scan processes.

1. Processes launched upon an explicit request of the operator.

   How to: **Monitor -> INS -> select path**.

   For more information, see Manage Active Processes.

2. Processes launched according to a schedule.

   How to: **Scheduler -> set time parameters -> Scan settings**.

   For more information on scan settings, see General Scan Settings.

   For more information on the **Scheduler** menu, see Optional Scheduled Scan Settings.

3. On-access scan. Select the necessary scan mode through the Control Panel: **On-access | Modes**.

   For more information on the **On-access** menu, see Optional On-access Scan Settings.

Standard parameters of scanning are set through **Setup | Scan settings**. These parameters will be used by default by all scans.

On-access and scheduled scanning may be customized. The options of every scheduled process may be set individually through **Scheduler | Scan settings**. The parameters applicable to on-access scanning only are set through **On-access | Scan settings**.

Managing Active Processes

To view the list of active scans, select **Monitor** in the Control Panel.

Here you can also view the statistics on any of the processes. The statistics window provides a dynamic display of the data pertaining to the process: time of operation, number of checked files, number of viruses detected by the process, etc. To open the statistics window of a certain process, select the process in the list and press ENTER.

Any active process may be cancelled by pressing DEL.

To create a process, press INS. In the editing window, use INS to view server volumes. To scan a selected directory or volume at once (on-demand scanning), press ENTER.

The options on the **Setup | Scan settings** will be applied as standard options for thus created processes.

Chapter 7. Logging

The log contains scan report data.

To view the event log and adjust logging parameters, select Log in the **Dr.Web Anti-virus** Control Panel. You can do the following:

- **View** – view log
- **Options** – configure log options
- **Clear** – clear log

Log Settings

The event log is configured via the **Log** menu on the **Dr.Web Anti-virus** Control Panel.

The **Options** menu provides the following logging options:

- **Log to file** — enables/disables logging
- **Overwrite log** — instructs to overwrite/append new data to the log every time the anti-virus is loaded
- **Log scanned files** — enables/disables logging for files that are not infected or suspected
- **Log packed files** — enables/disables logging of the names of packers of executable files
- **Log archived files** — enables/disables logging of the names of archivers used for packing the files

Chapter 8. Update

Dr.Web Anti-virus uses **Dr.Web virus databases** to detect malicious software. These databases contain details and signatures for all viruses and malicious programs known at the moment of the **Dr. Web Anti-virus** release. However modern computer viruses are characterized by the high-speed evolvement and modification. More than that, within several days and sometimes hours, new viruses emerge which can infect millions of computers around the world. To mitigate the risk of infection during the licensed period, **Doctor Web** provides you with regular updates to virus databases and **Dr.Web Anti-virus** components.

The Updater (drwebupn.nlm) downloads updates of **Dr.Web virus databases** (*.vdb files), anti-virus scanning engine (drweb32.dll), and installs them. With the help of this program you can also receive and use when updating the list of available update servers (update.drl).

The Updater is designed for operation with the scanner v. 4.44 or later.

To update necessary components, it is necessary to launch the scanner (drwebnw.nlm) prior to the updating program. Otherwise a message will be displayed that it is impossible to get the path to the virus databases (cannot get path to virus bases). A similar message will be displayed in case earlier (than 4.44) versions of the scanner are used.

When receiving updates the program notifies the scanner that it is necessary to download updated components. The scanner downloads updates irregardless of the interval and the flag of checking for available updates (the UpdateFlags and UpdatePeriod parameters in the [NetWare] section of the configuration file).

After launch the program switches to the mode of periodic querying the update servers according to the standard settings. The intervals between the queries and the addresses of the update servers are set in the command line. To terminate the program in this mode, execute the NetWare command `UNLOAD DRWEBUPN`.

The program is also terminated when the NetWare server is shut down or restarted with the instructions `DOWN`, `RESET SERVER`, `RESTART SERVER`.

If necessary, you can configure Updater options.

Update Settings

The program is set up by means of the following command line parameters (the settings are not stored in the configuration files):

- `/url`: *<url>* — the address of an update server. If this parameter is not specified, then addresses of update servers are read from the update.drl file located in the scanner catalog.
- `/user`: *<user name>* — a user name for authorization through the http protocol (at present this possibility is not used on **Dr.Web update servers**).
- `/pass`: *<user password>* — a password for authorization through the http protocol (at present this possibility is not used on **Dr.Web update servers**).
- `/purl`: *<proxy url>*`[`: *<port>*`]` — the address and port of the http-proxy server (if it is used). If no port is specified, the standard value of <port>=80 is used.
- `/puser`: *<proxy user name>* — a user name for authorization on the http-proxy server (if a proxy server is used).
- `/ppass`: *<proxy user password>* — a password for authorization on the http-proxy server (if a proxy server is used).
- `/qu` — shut down after updating is completed.
- `/uvb` — update only **Dr.Web virus databases** (*.vdb) and the **engine** (drweb32.dll), the parameter is set by default.

- `/uvb-` — update all files.
- `/dir`: *<directory>* — the catalog for storing updated files, by default the scanner catalog is used.
- `/interval`: *<minutes>* — a time interval between receiving updates, 10 min by default. Cannot be less than 1 min.
- `/nwsepscr` — create a separate screen for program notifications. By default the program notifications are displayed in the system console or Logger Screen of the NetWare server.
- `/verbose` — display a report about the connection with the update server, is used for debugging. Without an additional parameter specified, the report is added to the log file of the program.
- `/verbose:log` — the report (see `/verbose`) is written to the log file.
- `/verbose:screen` — the report (see `/verbose`) is displayed in the server console.
- `/debugoutput` — a more detailed report than `/verbose`, is used for debugging.
- `/debugoutput:log` — the report (see `/debugoutput`) is written to the log file.
- `/debugoutput:screen` — the report (see `/debugoutput`) is displayed in the server console.
- `/uptodate` — log attempts to update, even if there are no updated files.
- `/autoupdate` — restart the Updater automatically, if the drwebupn.nlm file was updated. Use this parameter with the `/uvb-` switch.
- `/maxlogsize:[` *<n>*`]` — the maximum size of the log file, is specified in kilobytes. By default is equal 512 KB.
- `/notifyskipped` — notify of all skipped files (not downloaded from the update servers).
- `/notifynotrestarted` — notify of downloaded but not started executable files.
- `/notifyrestarted` — notify of downloaded and started executable files.

- `/notifyaddr:[` *<username>*`[;` *<username>*`]...]` — names of users to receive the notifications. If no user is specified, the user with the admin name will be regarded the recipient of the notifications.
- `/notifyinterval:` *<minutes>* — a time interval between sending the same notifications, 30 min by default.
- `/notifyonce` — send the same notifications only once.
- `/help` — display a short help on the parameters and shut down.

If a recipient of notifications is specified, the program will also send notifications of its emergency termination to this user.