Doctor Web, Ltd.

Dr.Web® Anti-virus

Enterprise Suite

Corporate network protection

Administrator manual

Version 4.33

There might be further improvements and changes in the software not described in this manual. The corrected and supplemented versions of this manual are available at http://www.drweb.com/

Russia, Moscow – Saint Petersburg

http://www.drweb.com/

Content

1. Introduction *7*

1.1. Terms and abbreviations 7

1.2. Components, purpose and main functions of Dr.Web® Enterprise Suite 8

1.3. Who is this Manual meant for 10

1.4. What is this manual about 10

1.5. Links 12

2. Dr.Web® Enterprise Suite. Building protection against viruses *14*

2.1. Anti-virus network 14

2.1.1. Anti-virus server 14

2.1.2. Anti-virus agent and anti-virus package 17

2.1.3. The anti-virus console. Administrating the anti-virus servers 19

2.1.4. Interaction scheme of components of the anti-virus network 19

2.2. Building anti-virus network 23

2.3. Anti-virus network administrators. Administrator rights 25

2.4. Program registration. Key files 25

3. Installing and uninstalling Dr.Web® Enterprise Suite components *27*

3.1. Distribution kit of the program complex 27

3.2. Requirements to OS and hardware 27

3.3. Installing the anti-virus server and the anti-virus console 29

3.3.1. Installing the anti-virus server for Windows NT/2000/XP/2003 29

3.3.2. Installing the anti-virus server for Linux, FreeBSD and Solaris/x86 33

3.4. Installing the anti-virus agent on computers 37

3.5. Removing some components of the complex 40

3.6. Upgrading the anti-virus software of version 4.32 41

4. Starting the operation. Launching the anti-virus console and building a simple anti-virus network *45*

5. User interface of the anti-virus console and the anti-virus agent *52*

5.1. Anti-virus console 52

5.2. Anti-virus agent 56

6. Administrating the anti-virus network *58*

6.1. Planning, building and modifying the network's structure 58

6.1.1. Selection of the anti-virus server 58

6.1.2. Groups. Preinstalled groups, creation of new groups. Removing groups 58

6.1.3. Adding workstations to a group. Removing workstations from a group 60

6.2. Administrating a station of the anti-virus network 61

6.2.1. Inheritance of the configuration elements of a workstation from the configuration of a group. Primary groups 61

6.2.2. Viewing the configuration of a workstation 63

6.2.3. Viewing the logs and statistics of the workstation 64

6.2.4. Setting the anti-virus software and the agent 72

6.2.5. Setting users' permissions 79

6.2.6. Launching and terminating the anti-virus scanner on workstations. Forced updating of the workstation's software 80

6.3. Administrating several workstations simultaneously. Using groups 87

6.3.1. Advantages of synchronous administration and tools for it 87

6.3.2. Manual administration of several computers 87

6.3.3. Setting a group. Using groups for setting workstations 88

6.3.4. Propagation of settings 89

6.4. Controlling protection of the local network. Remote installation of the anti-virus software 90
6.5. Setting the anti-virus server 93
6.5.1. Logging on the server. Viewing the log 93
6.5.2. Setting the server configuration 95
6.5.3. Setting the server schedule 110
6.5.4. Checking for updates of the software and the virus bases 113
6.5.5. Administrating the server repository 113
6.5.6. Server statistics 124
6.5.7. Upgrading the server software till version 4.33 124
6.5.8. Receipt of alerts 132
6.5.9. Updating the server not connected to the internet 132
6.6. Peculiarities of a network with several anti-virus servers 133
6.6.1. Building a network with several servers 134
6.6.2. Setting connections between the servers of the anti-virus network 136
6.6.3. Using the anti-virus network with several servers 139
6.7. Updating the server key and keys of workstations 141
7. Administrating the anti-virus network 144
7.1. Administrators of the anti-virus network 144
7.2. Managing the administrators' accounts 145
Appendices 147
Appendix A. Description of settings for the external DBAS 147
Appendix B. Description of parameters of the alerts system 150
Appendix C. Parameters of templates of the notification system 151
Appendix D. Specification of the network address 158
D1. Introduction 158

D2. General format of address 158
D3. Addresses of Dr.Web® Enterprise Server 160
D4. Addresses of Dr.Web® Enterprise Agent/Installer 160
Appendix E. Administrating the repository 162
E1. Introduction 162
E2. Syntax of the `.config` configuration file 164
E3. Meaning of instructions of the `.config` file 166
E4. `id` files 170
E5. Examples of administration of the repository with modification of the state file 171
Appendix F. Server configuration file 173
Appendix G. Command line parameters of programs included into ES 178
G1. Introduction 178
G2. Agent's interface module 179
G3. Agent 179
G4. Network installer 182
G5. Dr.Web® Enterprise Server 185
G6. Internal database administrating utility 190
G7. The utility of generation of key pairs and digital signature 191
G8. Administrating the UNIX-version of the server by the kill instruction 192
G9. Dr.Web® scanner for Windows 193
Appendix H. Environment variables exported by the server 194
Appendix I. Agent installation script 195

1. Introduction

1.1. Terms and abbreviations

The following terms are used in the manual (Table 1).

Table 1. Legend

Symbol	Comment
 Note, that	Important note or instruction
 Attention	Warning about potentially dangerous or fraught with errors situations
Guard	The term in position of a definition or the link to a definition
`Cancel`	Names of buttons, panes, menu items and other program interface elements
[F1]	Keyboard keys names
`C:\Windows\system`	Names of files and directories

The following abbreviations will be used in the Manual without further explanations:

- PC — personal computer
- OS — operating system
- GUI — Graphical User Interface, GUI-version of program — a version using GUI

- DB, DBAS — database, database administration system

1.2. Components, purpose and main functions of Dr.Web® Enterprise Suite

The Dr.Web Enterprise Suite program complex (further referred to as Dr.Web ES) is designed for building and administration of the complex, indivisible and reliable anti-virus protection of computers within a local network.

Standalone computers of the local network are protected by the anti-virus packages designed for correspondent operating systems installed on those computers.

Dr.Web ES provides for:

- centralized (without unnecessary access of the personnel) installation of anti-virus packages on the protected computers (workstations and servers of the local network)
- centralized setting of parameters of the anti-virus packages
- centralized updating of the virus bases and programs on protected computers
- monitoring of the virus events, as well as the state of the anti-virus packages and the OS on all protected computers

Dr.Web ES allows both to leave a user right to modify the settings and to manage the anti-virus package, as well as to flexibly restrict modifications, or even forbid them at all.

Dr.Web ES has a "client-server" architecture. Its components are installed on computers of the local network and exchange information using network protocols (more detailed description of interaction of the complex‘ components goes below). The computers on which the interacting components of Dr.Web ES are installed we shall call as

anti-virus network. The anti-virus network includes the following components.

- *Anti-virus agent*. This component is installed on a protected computer; it installs updates and manages the anti-virus package as instructed by the *anti-virus server* (read below). The agent also sends information on the virus events and other necessary information about the protected computer to the anti-virus server
- *Anti-virus server*. This component is installed on one of the computers of the local network. The anti-virus server stores distribution kits of anti-virus packages for different OSs of protected computers, the updates of the virus bases, of the anti-virus packages and the anti-virus agents, users' keys and settings of packages of the protected computers and sends them by requests of agents to correspondent computers. The anti-virus server keeps one log of events of the whole anti-virus network and separate logs for each protected computer.
- *Anti-virus console*. This component is used for the remote administration of the anti-virus network by editing the settings of the anti-virus server and settings of protected computers stored on the anti-virus server and on protected computers.

The anti-virus server can be installed on any computer of the local network, not only on that performing a function of the local network's server. Still, the important requirement to this computer is its maximum accessibility for other computers. The protected computers themselves should be both workstations and servers of the local network.

The anti-virus console can be installed on computers outside the local network; it only requires a TCP/IP connection between the console and the anti-virus server.

The anti-virus network can include several anti-virus servers. The layout of such configuration is described in this Manual in p. 6.6

The software of the described components is multiplatform. The list of supported OSs, network interfaces and system requirements for correspondent components is in next sections.

1.3. Who is this Manual meant for

This manual is meant for the *administrator of the anti-virus network* — an employee of a company — owner of the local anti-virus network, who is in charge of the anti-virus protection of computers (workstations and servers) of this network.

The administrator of the anti-virus network should work under the system administrator rights, be competent in the strategy of the anti-virus protection and know in details the Dr.Web anti-virus packages for all OSs used in the system.

Several opening sections of the Manual should also be read by chief managers of a company responsible for taking a decision what anti-virus protection system is to be purchased and installed.

1.4. What is this manual about

This Manual contains the description of general principles and details of the complex anti-virus protection in the local network by Dr.Web ES. The Manual does not describe Dr.Web anti-virus packages for protected computers.

The examples of settings and management of the anti-virus package are shown on a protected computer operated by Windows.

General information on how to build the anti-virus protection is described in details in Section 2.

Installation of the complex software is described in Section 3.

Building of elemental anti-virus network on several computers of the local network with the help of the anti-virus complex is described in Section 4.

The interface of components of the program complex is described in Section 5.

Typical tasks, solved by the administrator of the anti-virus network with the help of the described above means, are described in Section 6.

- *Management* of the structure of the whole anti-virus network (adding and exclusion of new components, change of the topology of the anti-virus network, etc.) is described in p. 6.1.
- Administration of protected computers (including the settings of the anti-virus package and management of tasks of this package) is described in p. 6.2.
- Usage of groups of protected computers for their more simple administration and aggregation of statistics on them is described in p. 6.3.
- *Setting and administration* of the server of the anti-virus protection is described in p. 3.

Co-administration in the anti-virus network is described in section 7.

The present manual describes the basic options of the program complex allowing to create an efficient system of centralized anti-virus protection in the local network. The customized options of the software installation and record-keeping are not the subject of this Manual.

1.5. Links

Many parameters in Dr.Web ES are set as *regular expressions* Processing of regular expressions is made by the PCRE program library, developed by Philip Hazel.

Description of the used version of the regular expressions language is at http://info.drweb.com/products/esuite/doc/pcre/

The library is distributed with open source codes, the copyright belongs to the Cambridge University, Great Britain. All source texts of the library can be downloaded from ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

This software uses the Regina REXX interpreter, legally protected by General public license GNU. To download the source texts of the software or receive additional information visit the web-site of Regina at http://regina-rexx.sf.net

This software uses the JZlib library by JCraft, Inc. The library is legally protected by BSD-based license, read details at http://www.jcraft.com/jzlib/LICENSE.txt

The source text can be downloaded from http://www.jcraft.com/jzlib/index.html

This software uses the Common Codec package produced by Apache Jakarta Project, distributed and protected by the Apache Software License. See details at http://www.apache.org/licenses/LICENSE-1.1 The source text can be downloaded from http://jakarta.apache.org/

This software uses the JCIFS package, distributed and legally protected by the General public license GNU Lesser. Full source text can be downloaded from http://jcifs.samba.org

2. Dr.Web® Enterprise Suite. Building protection against viruses

This section describes the general strategy of the anti-virus protection.

2.1. Anti-virus network

The interacting computers, where the components of the Dr.Web ES anti-virus complex are installed, are called the *anti-virus network*. The software component installed on some computer will be called *the element* of the anti-virus network (if several different components are installed on one computer, we shall regard these components as different elements).

Below are described the elements of the anti-virus network performing different functions, and the algorithm of their interaction.

2.1.1. Anti-virus server

The anti-virus network has at least one anti-virus server.

The anti-virus server software is developed for the "server" operating system (presently, there are versions for Windows NT/2000/XP/2003, Linux, FreeBSD and Solaris/i86).

The installation directory of the anti-virus server has the following structure (the notation of the server variant for Windows is used):

- `var` — the directory contains subdirectories: `repository` – the so-called *updating directory*, where the actual updates of the virus base, of files of the anti-virus packages and components of the program complex are placed to. The directory contains subdirectories for separate functional software components, inside them reside the subdirectories for different OSs. The directory should be accessible for writing for a user under the name of which a

server is run (in Unix-based OSs this is, usually, `drwcs`, in Windows — `LocalSystem`).
`templates` — reports' templates

- `bin` — executable files of the anti-virus server
- `Console` — the directory contains files of the anti-virus network's console (for more details read p. 4)
- `doc` — the directory contains the documentation of the program complex
- `etc` — the directory contains files of additional settings of the program complex
- `Installer` — contains the program initializing the installation process of the program complex on a protected computer

The content of the centralized installation directory and the updating directory is automatically downloaded from the updating server via HTTP, as scheduled for the server; it can also be manually placed to these directories by the administrator of the anti-virus network.

The anti-virus server performs the following tasks:

- calls, receives and stores the detailed log on configuration of the hardware and the software of protected computers
- requests the versions number of the anti-virus package and dates of creation and version numbers of the virus bases on each protected computer
- installs the anti-virus packages on a selected computer or on a group of computers

- updates the content of the centralized installation directory and the updating directory
- updates the virus bases and executable files of the anti-virus packages, as well as executable files of the program complex on protected computers

The anti-virus server collects and logs information on operation of the anti-virus packages, which is sent to it by the software of the complex from the protected computers (anti-virus agents, details read below). The logging is made in the general events log file designed as the database. In a small local network the internal database can be used in the general log file of events. For large networks external database should be used.

The following information is collected and stored in the general log file of events:

- versions of the anti-virus packages on protected computers
- the time and date of installation and updating of the software of the workstation, stating the version of the software
- the version and the date of the virus bases update, stating their versions
- the operating system's version installed on protected computers, the processor type, location of system directories of OS, etc.
- accounts used on a protected computer for access to the directory of the centralized installation and the updating directory
- the configuration and the mode of anti-virus packages (usage of heuristic modes, the list of checked files, the actions upon detection of computer viruses, etc.)

- virus events, including the name of the detected virus, the date of its detection, the taken actions, the result of curing, etc.

The anti-virus server notifies the administrator of the anti-virus network on virus events connected with the program complex' operation. The administrator of the anti-virus network is notified by e-mail or through the standard broadcasting system of Windows. The setting of events provoking notifications and other notification parameters are described in p. 6.5.2.4.

The program complex can also be used in the *servers cluster mode.* In this mode, the anti-virus server software is installed on several computers; the servers are set up so as to use jointly the common external database, and the agents are connected to one (any) available server of the cluster. Usage of a cluster increases reliability and productivity of the anti-virus network, but considerably complicates its administration. Below the network administration is described as for the one server mode; the settings for clusters are only mentioned, without any details.

2.1.2. Anti-virus agent and anti-virus package

The anti-virus protection on computers of the local network is performed by the Dr.Web anti-virus packages designed for correspondent OSs.

In Dr.Web ES these packages are operated by one component of the complex (anti-virus agent), which is installed on a protected computer and stays constantly in memory. In view of this, the architecture and the operation of the packages have certain peculiarities. In particular, the user key of the anti-virus package,

which defines possible limitations of its functionality, and the configuration of the package are sent to the package by the anti-virus agent and never stored in a file accessible for the package. This data, in its turn, is sent to the agent from the anti-virus server. Thus, the anti-virus package stops immediately functioning, if the agent fails to operate; or it stops functioning after a computer reboot, if there is no connection with the server (if more than 24 hours passed since the user key was received from the agent).

The anti-virus agent performs the following functions:

- Executes tasks set by the anti-virus server (such as installation and updating of the anti-virus package, launch of scanning, etc.), if necessary, files of the anti-virus package are called for execution via special interface
- Sends results of the tasks performed by the anti-virus server
- Notifies the anti-virus server on predefined events arising during the operation of the anti-virus package

Every anti-virus agent is connected to the anti-virus server and makes part of one or several registered on this server *groups* (for details read p. 6.3). The transfer of information between the agent and the predefined server is made via the protocol used in the local network (IP, IPX or NetBIOS). The number of simultaneously run agents depends upon the limitations of the protocol and cannot exceed 256 with NetBIOS. If using the IP and IPX protocols, their number is practically unlimited.

A protected computer with the installed agent, in compliance with its function in the anti-virus network, will further be called as *workstation* of the anti-virus network. One should remember that such computer can be both – a workstation and a server of the local network, depending on its functions in the local network.

2.1.3. The anti-virus console. Administrating the anti-virus servers

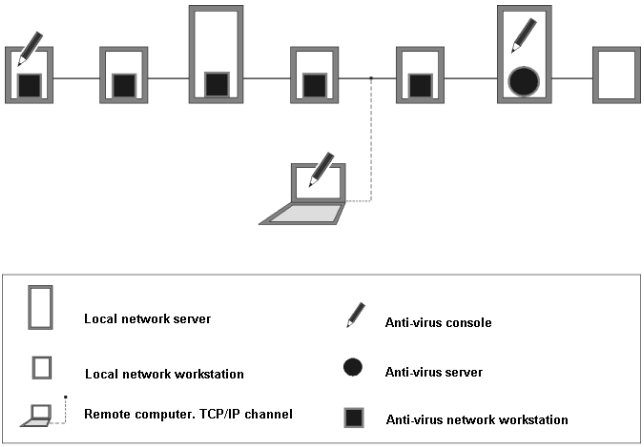
The administration of the anti-virus network as a whole (including the changes in its set and structure), as well as of all its components is performed by the *anti-virus console*.

Actually, the anti-virus console is an external interface of the anti-virus server; the editing of settings of workstations of the anti-virus network, the launch of tasks on them is performed through a server the workstations are connected to.

The anti-virus console is a platform-independent application and can be installed on a computer with any OS supporting Java virtual machine. The connection between the console and the server is provided via TCP/IP, and the console can be outside the protected local network.

2.1.4. Interaction scheme of components of the anti-virus network

Pic. 1 describes the general scheme of the local network fragment, where the protecting anti-virus network is organized.



Picture 1. Physical structure of the anti-virus network

Below is described the detailed interaction between the elements of the anti-virus network.

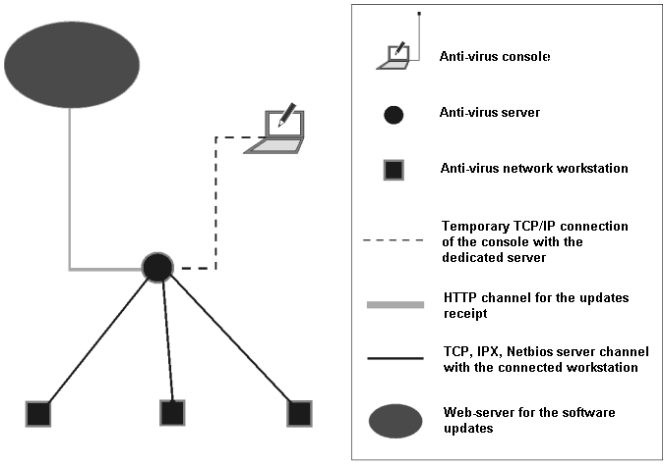
When the anti-virus server is launched, the following actions are performed:

- Files of the anti-virus server from the `bin` directory are downloaded
- The Scheduler of tasks for the server is downloaded
- The directory of the centralized installation and the updating directory, the initialization of the alarm system are downloaded
- The server's database integrity is checked
- The tasks of the server's Scheduler are performed
- The information from the anti-virus agents and the commands from console is waited

The whole stream of instructions, data and statistics in the anti-virus network obligatory flows through the anti-virus server. The anti-virus

console also exchanges the information with the server; the changes in the configuration of a workstation and the transfer of commands to the anti-virus agent are performed by the server on the basis of the console commands.

Thus, the logical structure of the fragment of the anti-virus networks looks as in pic. 2.



Picture 2. Logical structure of the anti-virus network

The following requests from the server to workstations and backwards (thin firm line in pic. 2) are sent using one of the supported network protocol (TCP, IPX or NetBIOS):

- requests of an agent for the centralized schedule's receipt and the centralized schedule of the given workstation
- the settings of the agent and the anti-virus package
- requests for the scheduled tasks to be performed (scanning, updating of the virus bases, etc.)
- files of the anti-virus packages — when the agent receives a task to install them

- updates of the software and the virus bases — when the updating is performed
- messages of the agent about the configuration of a workstation
- Statistics on the agent's operation and the anti-virus packages to be included into centralized log
- messages on virus events and other events which should be logged

The volume of traffic between the workstations and the server, depending on the settings of workstations and their quantity, can be rather substantial, that is why Dr.Web ES provides for the traffic compression option. The description of this optional mode is described below in p. 6.5.2.2.

The traffic between the server and a workstation can be encrypted. This allows to avoid the leakage of data transferred via the described channel, as well as to avoid the replacement of the SW downloaded onto the workstations. By default, this option is enabled. The description of this optional mode is described below in p. 6.5.2.2.

From the updating web-server to the anti-virus server (grey thick firm line in pic. 2) the files necessary for replication of the centralized installation directory and the updating directory are sent using HTTP, as well as overhead information about the process. The integrity of the information sent (Dr.Web ES files and anti-virus packages) is provided through the checksums: a file corrupted at sending or replaced will not be received by the server.

Between the server and the anti-virus console (dotted line in pic. 2), the information on the server configuration (including the topology of the network) and the settings of workstations is sent using TCP/IP. This information can be viewed in the anti-virus console, and, if some

settings are modified by a user (by anti-virus network administrator), the information on the changes made is sent to the server.

The connection of the console with the selected server is made only after the anti-virus network administrator is authenticated by its User ID and a password on the given server.

2.2. Building anti-virus network

This section describes the general sequence of operations for building the anti-virus network. The necessary software and their interface are further described.

To build the anti-virus network in the company local network:

1. Make a plan of the anti-virus network taking into account the topology of the local network and the degree of accessibility of computers in the network.
2. Install the software of the anti-virus server on the selected computer or computers.
3. Install the software of the anti-virus agent on workstations.
4. Install the anti-virus consoles on the anti-virus network administrator's computer.
5. Connect workstations to servers with view to the planned structure.
6. Set up the workstations.

At the stage of planning of the anti-virus network's structure one should first of all select a computer which will serve as the anti-virus server. The selection criterion should be as follows: the server must be accessible in the network by all the workstations connected to it during the whole time of their operation.

The installation of the Dr.Web ES software on the selected computer is described in p. 3. During the installation, the `Console` directory

with the anti-virus console distribution kit and the `Installer` directory with the program — the initial loader of the workstation software are created on the server. It is advisable to make these directories accessible for reading in the network.

On each computer where the workstation software is planned to be installed, the software installation program should be run from the `Installer` directory.

Run the anti-virus console on the computer used by the administrator of the anti-virus network (the launching scripts for different OSs and executable files reside in the `Console` directory).

The administrator of the anti-virus network should connect with the help of the anti-virus console to the anti-virus server and make the procedure of connection of the workstations.

After the workstations are connected, they should be set up, i.e. the configuration of the anti-virus package and the parameters of the anti-virus agent should be set up. To facilitate this task, you can use the grouping mode (read p. 6.3), which allows to set up considerable number of workstations at once. The program complex has a substantial quantity of predefined groups, including the grouping by the OS of the workstations with different level of details.

To install the server, the console and the initial installation program of a workstation a single access is required (physical or remote administration and launch of the program) to correspondent computers. All further actions are made from the computer of the anti-virus network's administrator (including the option of possible external infiltration to the local network) and do not require access to servers or workstations.

2.3. Anti-virus network administrators. Administrator rights

Accounts of the anti-virus network's administrators are divided into two groups:

- full rights accounts
- "read only" accounts

Administrators using the rights of the first group can view and edit configuration of the anti-virus network and settings of its separate elements, as well as create new administrator accounts.

Administrators using the "read only" rights can only view the settings of the whole network and of its separate elements, but cannot change them. They can also view the list of available administrator accounts.

After the system is installed, it will have one account with full rights.

Creation, deletion and editing the administrator accounts are described in p. 7.

2.4. Program registration. Key files

User's rights to use the anti-virus are regulated by two special files (a server key file and a key file for a workstation).

The key file has a write-protected format and must not be edited. Editing the file makes it invalid. Therefore, it is not recommended to open your key file with a text editor, which may occasionally corrupt it.

Users who have purchased the anti-virus from the Doctor Web's authorized partners obtain *license key files*. The parameters of these key files, specifying user's rights, are set in accordance with the

License agreement. Such files also contain a user and a selling company data.

For evaluation purposes there are also d*emo key files.* Such key files provide for full functionality of main anti-virus components, but have a limited term of usage and no user's support is provided.

The key files are sent to a user as a zip-archive, which contains a key file for a server called `enterprise.key` and a key file for workstations called `agent.key`.

A user can receive the key file in one of the following ways:

- sent via e-mail (usually after the registration on the web-site, read below)
- included into the anti-virus distribution kit
- supplied on a separate carrier

License key files are sent to users via e-mail, as a rule, after the registration on the special web-site (the address of the registration web-page is http://buy.drweb.com/register/), if other address is not specified in the registration card supplied with the product. Visit this page and fill in the form with the customer data, input the registration serial number into appropriate fields (provided in the registration card). The archive with key files will be set to the designated address. You will also be able to download it from the indicated web-site.

Demo key files can be sent upon a request made through the web-form at http://download.drweb.com/demo/. The demo key request will be examined and, if satisfied, the archive with key files will be sent to the designated address.

The usage of the key files received during the program installation is described in p. 3.

The usage of the key files for the already installed program complex is described in p. 6.7.

3. Installing and uninstalling Dr.Web® Enterprise Suite components

3.1. Distribution kit of the program complex

The distribution kit of the program complex is supplied in two variants, depending on the OS of the anti-virus server:

- To install the anti-virus server operated by Unix-based OSs – as two files of Zip format
- To install the anti-virus server operated by Windows NT/2000/XP/2003 – as executable files (installation wizard), or a file in the MS Installer format (`*.msi`)

The distribution kit contains the following components:

- The anti-virus server software for the correspondent OS
- The anti-virus agent software and the anti-virus packages software for the supported OSs
- Virus bases
- The anti-virus console software and launching scripts for main OSs
- Manuals, templates, examples

In addition to the distribution kit, the files with a server key and a key for workstations can also be supplied.

3.2. Requirements to OS and hardware

The requirements for installation of the Dr.Web ES include:

- Local network based upon the IP, IPX or NetBIOS protocols (all protected computers and the anti-virus server should be included into this network)
- For the anti-virus server – a computer with processor Pentium III-667 or higher, operating memory 128 MB or higher (256

MB, if using the inbuilt database), free space on the hard drive 1 GB (20 Mb for executable files, the rest – for logs and the built-in database), Windows NT/2000/XP/2003, Linux, FreeBSD or Solaris/x86 operating systems

- To automatically receive the content of the centralized installation directory and the updates from the updating server an access to the servers of the Dr.Web global updating system through the Internet should be established for the anti-virus server
- The anti-virus console requires a computer operated by Windows, or a computer with Sun JRE version 5.0 Update 1 or higher (requirements to the Os and the computer are determined in this case by the JRE requirements)
- the connection via TCP/IP should be provided between the server and the console
- the anti-virus agent and the anti-virus package require a computer with processor Pentium II-400 or higher, operating memory 32 Mb or higher, free space on the hard drive 128 Mb or higher (8 Mb for executable files, the rest – for logs), Windows 95/98/Me/NT/2000/XP/2003

In addition, to install the anti-virus server for Windows a computer should have MS Installer 2.0. This program is included into Windows 2000 (with SP3) or higher versions. If using earlier versions of Windows, you should download and install MS Installer 2.0

For more details visit
http://msdn.microsoft.com/library/default.asp?
url=/library/en-us/msi/setup/about_windows_installer.asp

There should be no other anti-virus software installed on the workstations of the anti-virus network (other versions of the Dr.Web anti-virus programs including).

When the software for the anti-virus server for FreeBSD is installed, the computer system software should include the libiconv library version 1.8.2 or higher. This library can be downloaded from ftp://ftp.freebsd.org

3.3. Installing the anti-virus server and the anti-virus console

The installation of the anti-virus server is the first step in the installation of the program complex. Unless and until it is successfully installed, no other components of the complex can be installed.

The installation procedure depends upon the server version installed (for Windows or Unix-based systems). Nevertheless, the set of the adjusted during the installation parameters and the structure of the software installed coincide.

All parameters set during the installation can be changed in future by the anti-virus network's administrator in the course of the server's operation.

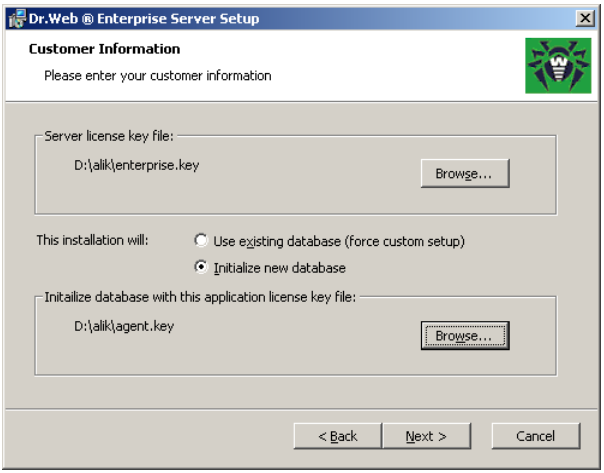
3.3.1. Installing the anti-virus server for Windows NT/2000/XP/2003

Below is described the installation of the anti-virus server for Windows. The set and the order of steps may somewhat differ depending on version of the distribution.

The distribution file and other files, called during the program's installation, should reside on local drives of a computer where the server software is installed; these files should be accessible for LOCALSYSTEM user.

To install the anti-virus server on a computer operated by Windows:

7. Double click the distribution file in the Explorer. A window of the Installation wizard with information on the program will open. Press `Next`.
8. A window with the text of the License agreement will open. You should accept the License agreement to continue installation. In the group of buttons in the bottom part of the window select `I accept the terms in the License Agreement` and press `Next`.
9. A window of selection of license key files will open (pic. 3).



Picture 3. Selection of license key files

In the `Server license key file` field press `Browse`, and then select the `enterprise.key` license key file for the server in the standard Windows window. In the `Initialize database with this application license key file` field

set the key file for the workstation software (the agents and the anti-virus packages).

In the `This installation will` group of buttons select `Use existing database…`, if you want to save the server database of the previous installation, or `Initialize new database`, if it is necessary to create new database.

Press `Next`.

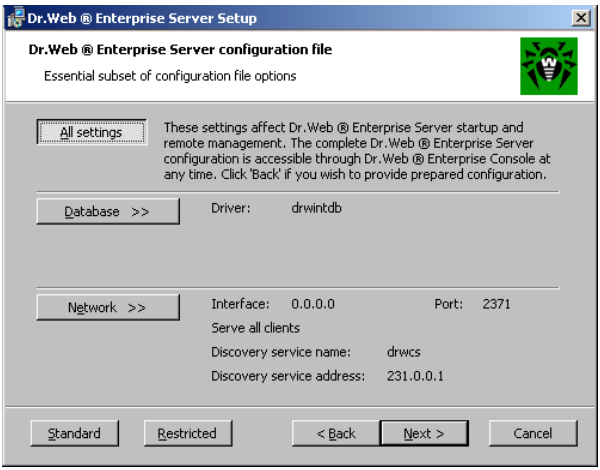
10. A window for selection of the installation mode will open. For rapid installation, chose `Novice`, for selective installation, chose `Custom`. If the rapid installation is chosen, all parameters are installed with their default values; steps 5 to 7 (read below) are omitted.

    Press `Next`.

11. If the selective installation is chosen, a window for selection of the installed components and the installation directory will open. Select the components which should be installed in the hierarchy list. IF necessary, change the installation directory, press `Browse` and select the installation directory in the standard Windows window. Press `Next`.

12. In the next window you can chose the language of the notification templates, set the mode of usage and naming of the system shared directory for installation of the agent, specify the mode of usage of the server in the existing cluster and choose the cluster (read p. 6.6), specify the command line mode for the server launch and for its installation as the Windows service (read Appendix G), as well as install the predefined configuration file of the server, instead of that created by the installation program (read Appendix F).

13. On the next page (pic. 4) the main settings stored in the configuration file of the server are specified (read Appendix F).



Picture 4. Main server settings

Press `Database` to set parameters of the database. In the `Driver` group of buttons the DBAS type used for the centralized logging is specified. `IntDB` instructs to use the built-in tools of the program complex. In large networks with 100-200 computers or more, such configuration may slow down the operation. If you want to use the external DBAS, select `ODBC`.

Press `Network` to set up the network protocol for the server (only one network protocol can be specified; additional protocols can later be set up). Apart from the address and the port's interface, the multicast mode and the local access restriction to the server can be specified.

You can also press `Standard` to specify the default network settings, or press `Restricted` to set up the settings under which the server can be administrated from the console only launched on the same computer (later, after the settings of the server are specified, the network settings can be modified).

Press `Next`.

14. In the next window input the anti-virus system's administrator's password. Press `Next`.
15. The installation program's further actions do not require a user intervention.

Usually, the installed ES server is administrated with the help of the anti-virus console. The installation program also puts the elements allowing to set up and to administer the server into the main Windows menu.

The `Dr.Web(R) Enterprise Server` directory is placed to the `Programs` menu and contains the following elements:

- Launch icon of the anti-virus console
- The icon leading to the complex' documentation
- The `Server control` directory

The `Server control` directory contains the instructions for launch, reboot and termination of the server, as well as logging and other server instructions described below in Appendix G5.

3.3.2. Installing the anti-virus server for Linux, FreeBSD and Solaris/x86

To install the anti-virus server for Unix-based OSs:

1. Create the `drwcs` user and the `drwcs` group containing it in the system (usually, the user script makes it automatically). Select the directory where the server will be installed and desarchive both distributions into it. Then go to the directory and modify the owner of the unpacked files by the `chown -R drwcs:drwcs *` instruction
2. Go to the installation directory and open the `etc/drwcsd.conf` server configuration file in the text editor.

Edit this file, if necessary, to specify the parameters' values different from the default ones. The file contains all values of the parameters, the alternative including; all except for the necessary are commented (by the ";" symbol at the beginning of the line). To change the selected parameter's value, comment up the old value and uncomment the new one.

3. By default, the line with the `drwintdb` value is active (uncommented), which means that internal DBAS is used. If the external database is used (in Unix-based OSs PostgreSQL can be used), the line with the `drwpgsql` value should be activated. In this case, the `using` value should also be edited as it is advised in Appendix A.
4. If sending of e-mail notifications on virus events connected with the program complex' operation is supposed to be used, uncomment the `alert` value and edit the `alerter` value.
5. If any network (transportation) protocol except for IP is supposed to be used, uncomment the `IPX/SPX` or `NetBIOS` values.
6. If necessary, edit other values and parameters and close the file saving the changes made.
7. Create the `var` subdirectory in the server installation directory and move there the `repository` subdirectory; specify the access rights for the created subdirectory with the following instructions:

```
mkdir var
mv repository var
chown -R drwcs:drwcs var
```

8. In the `templates` directory the report and notification templates reside. The subdirectories of this directory contain the templates in different languages. Copy the content of the necessary subdirectory to the `templates` directory and edit

the templates, if necessary (read more details on the format of templates in Appendix C). After that move the `templates` directory to the `var` directory and specify the access rights to it:

```
mv templates var
chown -R drwcs:drwcs var/templates
```

9. Place the server key file to the `etc` subdirectory of the installation directory. The file should have the name `enterprise.key`

10. Install the `LD_LIBRARY_PATH` environment library so as it points to the `lib` directory, for example, if the anti-virus server is installed to the `/opt/drwcs` directory, the sequence of instructions should be as follows:

```
LD_LIBRARY_PATH=/opt/drwcs/lib:$LD_LIBRARY_PATH
export LD_LIBRARY_PATH
```

11. Run the `drwsign` utility to create the pair of open-locked encryption key. Place the locked key to the `etc` directory and specify the access rights to it for those users only who will run the anti-virus server. Place the open key to the installation directory of the agent. For this, the following sequence of instructions is used (the path with regard to the installation directory, the `Installer` subdirectory in this case is the installation directory of the agent):

```
bin/drwsign genkey etc/drwcsd.pri etc/drwcsd.pub
chmod 600 etc/drwcsd.pri
chown drwcs:drwcs etc/drwcsd.pri
mv etc/drwcsd.pub Installer
```

The agent's installation directory should be network-accessible.

12. Place the `agent.key` user key file to the `etc` subdirectory, then initialize the server database. Use the following instruction for this:

```
bin/drwcsd -var-root=./var -verbosity=all
   -log=var/server.log initdb agent.key - - password
```

where `password` is the password of the anti-virus server administrator.

To keep a user key file in secret, the file of the key is presented to workstations by request, but it is not stored on them (it is stored in the main memory). The `agent.key` file should be deleted after its installation on the server. The copy of the file should be kept on a movable carrier in a safe place. The peculiarities of operation of the anti-virus agent on mobile computers (often disconnected from the network) are described in p. 3.4.

13. Make sure that the `drwcs` user is the owner of all files in the installation directory and its subdirectories, and that the `var` directory is accessible for it for reading and then launch the server by the following instruction:

```
bin/drwcsd -var-root=./var
                -verbosity=all -log=var/server.log
```

To automate the administration of the anti-virus server use the `drwcs.sh` shell-script located in the `bin` directory. Study it carefully and edit as necessary. This script provides for somewhat different and more conventional scheme of location of files of the anti-virus complex accepted in most contemporary UNIX systems — the customary part of the package files is located in `/opt/drwcs`, and files, modified during the operation (and therefore requiring their location in the file system for which the write access is necessary) — in `/var/drwcs`.

3.4. Installing the anti-virus agent on computers

Before to install the anti-virus agent on a computer, make sure there is no other anti-virus software installed there. If any anti-virus is present, deinstall it.

To install the anti-virus agent on a computer, access from this computer the network installation directory of the agent (this is the `Installer` subdirectory of the server installation directory and can be moved later) and run the `drwinst` program. The anti-virus agent' software will be installed on the computer (but not the anti-virus package).

The cited instruction allows additional parameters. To view the report on the agent's installation in a real time mode, use the `-interactive -verbosity=all` parameter.

If the address of the server is not recognized by the agent automatically (the Multicast mode is unavailable), specify explicitly the server's address as follows below:

```
drwinst -interactive -verbosity=all 192.168.1.3
```

When the agent is installed, the program installs the software of the anti-virus workstation on the computer. The installation takes several minutes.

You can also remotely install the anti-virus agent on a workstation by using the anti-virus console. This operation is described at the end of p. 6.4.

The administrator can also place the `agent.key` user key to the installation directory of the anti-virus agent. This action provides for stable functioning of the anti-virus protection on the workstation temporary disconnected from the server (otherwise, in 24 hours after the disconnection, the anti-virus software starts functioning in the demo mode). The virus bases and the software on the disconnected workstation are not updated.

An agent key stored on a workstation can be stolen. Do not needlessly store the agent key on the workstation.

If the Active Directory service is used in the protected local system, you can remotely install the anti-vitrus agent on workstations.

For this:

1. Dowload the anti-virus agent installer for networks with Active Directory (`Es-agent.msi`) from www.drweb.com.
2. Install the anti-vitrus agent on the local network server supporting the Active Directory service:
   ```
   msiexec /a Es_agent.msi
                   ESSERVERADDRESS=<ip_of_ES_server>
                    ESSERVERPATH=<public_server_key>
   ```
   where the `ESSERVERADDRESS` parameter sets the IP-address of the server the agent will be connected to, the `ESSERVERPATH` parameter sets the full path to the public key of the ES server (it

is, by default, drwcsd.pub in the Installer subdirectory of the ES server installation directory). Both parameters are obligatory. Make the installation to the directory with the shared access on the network and remember this directory.

3. On the local network server supporting the Active Directory service, select Administrative Tools submenu in the Programs and then select the Active Directory Users and Computers item.
4. In the domain to which the computers are included on which the anti-virus agents are supposed to be installed, create the Organizational Unit (further called OU) with the name ES and include the computers the agent will be installed into it.
5. In the contextual menu of this OU ES select the Properties item. A ES Properties window will open
6. Go to the Group Policy pane. Press the Add button and create the element of the list with the name ES policy. Double click it. A Group Policy Object Editor window will open.
7. In the hierarchy tree select Computer Configuration, then Software Settings, and then select the Software Installations element. In the contextual menu of this element, select the New item, in the opened submenu select the Package item. Specify the direcitory where the agent's installer was installed during the administrative installation in p. 2 (thepath to the directory should be specified in the network addresses' format, even if this directory is locally accessible).
8. The anti-virus agent will be installed on selected computers during the nearest registration in the domain.

The OU name and elements of the `Group Policy` list can be arbitrary.

3.5. Removing some components of the complex

The components of the program complex can be removed from computers, if necessary.

To remove the software from a workstation, run the `drwinst` instruction with the `–uninstall` parameter (or with the `–uninstall –interactive –verbosity=all` parameters, if you want to control the process of removing) in the installation directory of the anti-virus agent.

Example:

```
drwinst –uninstall –interactive –verbosity=all
```

For successful removing the `uninstall.rexx` file should reside in the same directory. The file is placed to the directory during the agent's installation, but, if installation fails, it will not appear in the directory (a message about it will be generated by the deletion procedure in the described above mode example). In such case, place the file to the directory manually by copying it from the `var/repository/20-drwagntd/win` subdirectory of the server installation directory.

The server software is removed by the OS standard tools. (for example, if using a server for Windows the `Add-remove programs` element of the Control panel is used).

It is not advisable to install the complex' software on computers where it was already installed (even unsuccessfully). The software should be removed from the computer first. Still, if the program complex version 4.32 or higher is installed, it should be updated instead of removed, as it is described in p. 3.6.

3.6. Upgrading the anti-virus software of version 4.32

It is recommended to upgrade the program version 4.32 or higher till current version. This will save the database of the anti-virus server and the data encryption keys and will allow not re-install the anti-virus agent on workstations. Following description presupposes the software version 4.32 is upgraded till version 4.33.

To upgrade the software:

1. Make sure the anti-virus agents on workstations are upgraded till version 4.32c. If your anti-virus network timely receives software upgrades, this action will be done automatically. To check if the upgrade was made, select the agent's installation directory in the Explorer (this is usually `\Program Files\DrWeb Enterprise Suite` on the system hard drive), and then select the `drwagntd.exe` file. In the context menu of the file's icon, select the `Properties` item; in the opened window in the `Version` pane read the version number which should be `4.32.3.9270`.
2. If this file is of an earlier version, run full upgrading of the agent on the server as it is described above in p. 6.5.5 (this mode is enabled by default). Wait until upgrading files are received on

the server and upgrading is made on the workstations. To make sure the server received the upgrade files, check the `drwagntd.exe` file version, in the `var\repository\20-drwagntd\win` directory as described above.

3. Terminate the server (read p. 5.1).
4. If using external database, remember the access parameters.
5. Copy the following files (the notations of the Windows file system and the paths relative to the server installation directory are used) to the separate directory (in future it may be `C:\ES_432_Backup`; the name and the location of the directory is inessential):
   `var\dbinternal.dbs`
   `etc\drwcsd.pri`
   `Installer\drwcsd.pub`
   `etc\enterprise.key`
6. Uninstall the server software by using standard OS tools (read p. 3.5).
7. Install the server software version 4.33. The installation is similar to that described in p. 3.3, but it has several important differences listed below.

Do not upgrade the server software by default. Study carefully how to install and save parameters of previous version in contrast to the default installation procedure. Should you fail to do this, it may result in lost of data of previous installation!

8. Update all products. For this, select the `Check for updates` item in the `Administration` menu and then

select `All Dr.Web(R) Enterprise Products` (read p. 6.5.4).

9. When the updating is finished, the agents will ask to reboot the workstations. After reboot the updated program is ready for work. Still, if at previous stages for some agents the updating till version 4.32c was not made, after the updating of these agents is finished, a message on a critical updating error will be generated. For such workstations forced updating should be launched, read p. 6.2.6.

To install the anti-virus server software of version 4.33 for Windows:

1. Run installation procedure, accept the license agreement.
2. In the `Customer Information` window in the `Dr.Web® Enterprise Server Key` field, press `Browse` and select the saved `enterprise.key` file.
3. In the same window, select `use existing database` in the group of buttons.
4. In the `Setup actions` window, check the `Install existing Dr.Web® Enterprise Server cryptography keys` box and press `Select`, and then in the opened window select saved private and public encryption keys.
5. In the `Dr.Web® Enterprise Server configuration file` window press `Database`. A window for setting the database will open.
6. If the external database is used (ODBC), set DNS, login and password. If the internal database is used, specify the path to the saved `dbinternal.dbs` file (it is recommended to create

a server installation directory and create a `var` subdirectory in it and copy this file to this subdirectory).

7. The completion of the installation procedure runs as usual.

To install the anti-virus server software version 4.33 for Unix-based systems:

1. Install the server as it is described in p. 3.3.2.
2. If the external PostgreSQL database is used, set the database parameters in `etc/drwcsd.conf` file. If the internal database is used, copy the saved `dbinternal.dbs` file to the `var` subdirectory of the installation directory.
3. Copy saved `enterprise.key` and `drwcsd.pri` files to the `etc` subdirectory; copy `drwcsd.pub` to the `Installer` subdirectory.
4. Do not terminate the database and run the instruction
```
bin/drwcsd -var-root=./var
   -log=./var/log/server.log upgradedb update-db
```
5. When the instruction is completed, run the server.

4. Starting the operation. Launching the anti-virus console and building a simple anti-virus network

For further operations with workstations no access to them is required (neither physical, nor network-aware), still the changes in the settings of the server are to be made (and of the workstations on the server) and the instructions to the server are to be sent. For this, the anti-virus console should be run on the computer of the administrator and the connection with the server should be established. The examples below describe the launch of the anti-virus console from the administrator's computer operated by Windows. With other operating systems the actions are the same.

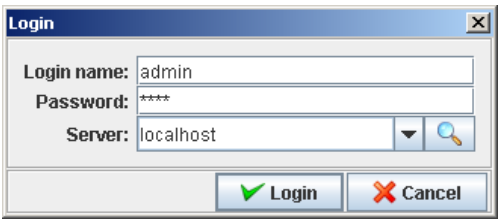
The program files of the console, as well as the launching scripts for certain OSs, reside in the server installation directory in the `Console` subdirectory. This directory should be network accessible, or moved to the computer of the anti-virus network's administrator.

The console should not be placed to the directory the path to which contains the ! symbol (exclamation mark).

To run the anti-virus console:

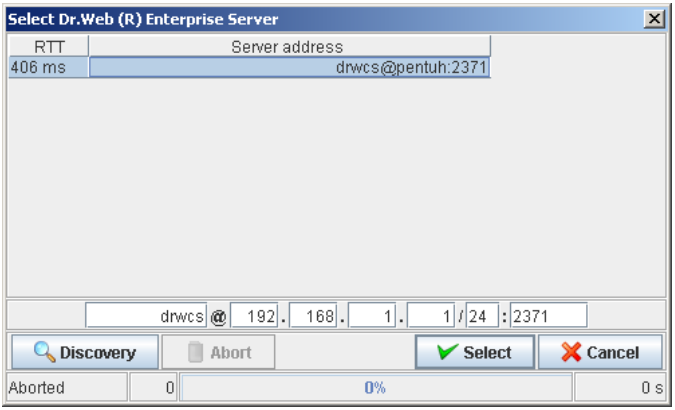
- If you work under UNIX-based OS, run the script `drwconsole.sh`
- If you work under Windows – run `drwconsole.exe`

A window for login on the server will open (pic. 5).



Picture 5. Login on the server

If no server address is specified in the `Server` entry field, input it manually or use  to find available servers. A search window will open (pic. 6).



Picture 6. A server search window

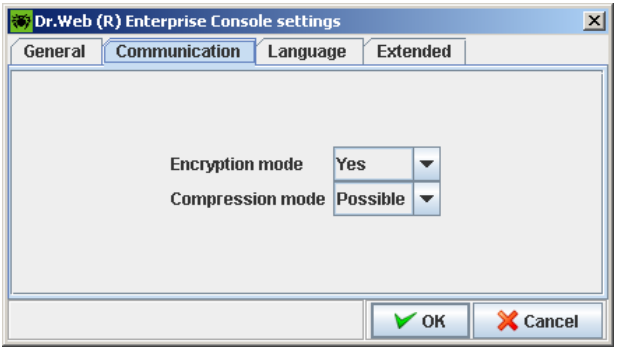
In the entry fields of the bottom part of the window the initial search address is specified. Edit it, if necessary (the format of the network address is described in details in Appendix D). Press `Discovery`. The list of discovered servers will be displayed in the upper part of the window. Select the necessary server in this list and press `Select`.

Input the registration name and the password of the anti-virus network administrator (the `admin` user name and the `root`

password are used during the installation; it is advisable to change the password, read p. 7.2).

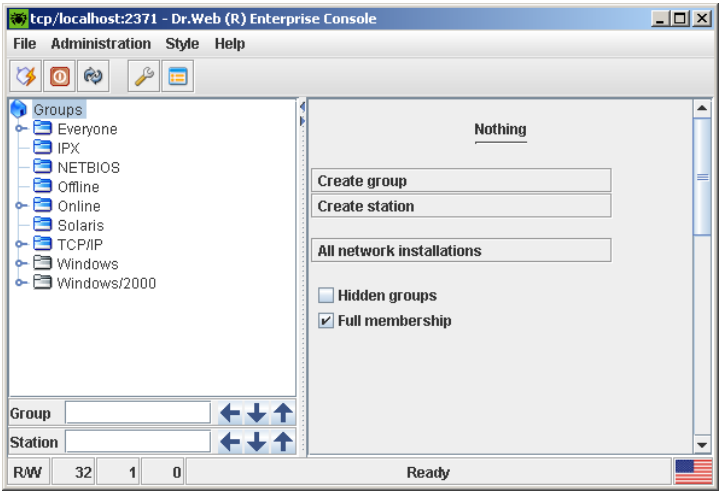
Press `Login`.

The registration on the server is impossible if the traffic's encryption and compression settings of the console and the server are incompatible. If this is the reason of failure of the registration, select the `File` item in the main console menu in the upper part of the window, then select the `Dr.Web(R) Enterprise Console settings` in the opened submenu. A window for editing the settings will open. Go to the `Protocols` pane (pic. 7). Select the same settings in the `Encryption mode` and `Compression mode` in the dropdown lists as set for the server and press `OK`. The settings of the console and the server are compatible; the compatibility may be broken, if you yourself have earlier changed one of these settings.



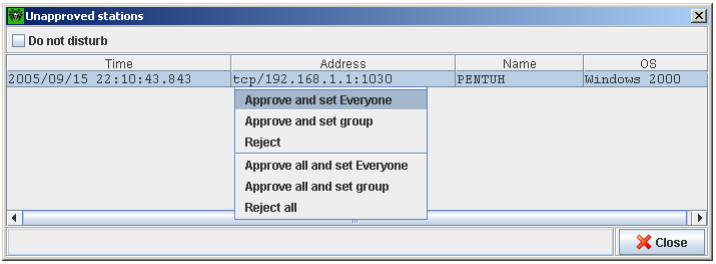
Picture 7. Console settings

In case of a successful registration on the server the main console window will open (pic. 8). In this window the information on the anti-virus network stored on the server can be viewed.



Picture 8. Main window

The new workstations approval mode is set as the default setting of the anti-virus server. In this mode the new workstations are not automatically connected, but placed by the server into the list of *unapproved* workstations. To let the server connect the new station, select the `Administration` item in the main console menu, in the opened submenu select the `Unapproved stations` item. A list of detected but not approved workstations will open (pic. 9).

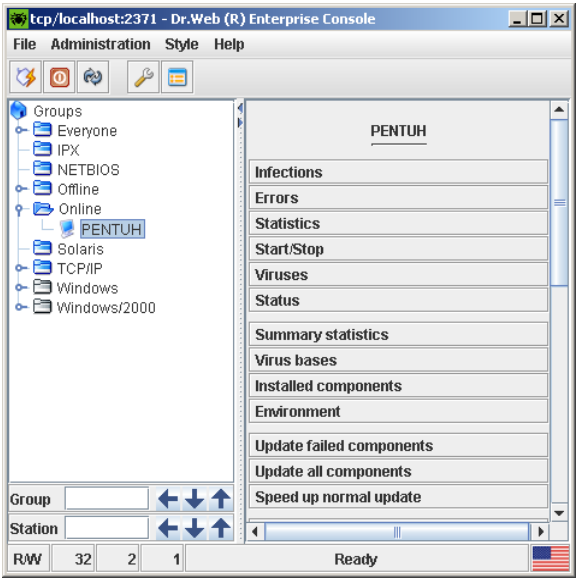


Picture 9. Unapproved stations

Select the station in the list, then chose the `Approve and set Everyone` item in the contextual menu.

If the `Approve and set Everyone` item will be chosen instead of the `Approve and set group` item, you can chose another *primary* group for the given workstation. Read more about primary groups in p. 6.2.1.

A station will be connected to the server and the anti-virus network will look as below in pic. 10.



Picture 10. A workstation is connected to the anti-virus network

The workstation is placed to the `Everyone`, `Online` predefined groups of workstations and to the groups complying to the OS' family and to the definite OS (in the picture it is Windows and Windows/2000 accordingly).

The installation of the missing software components onto a workstation (the agent and the anti-virus package) does not further require an administrator's intervention.

To complete the installation of certain components of the anti-virus workstation a computer reboot may be required. In this case the installation program of the anti-virus agent will generate a correspondent information window.

By default, not all groups are displayed in the hierarchy list (directory) of the network's elements (part of groups, the so-called *hidden* groups are displayed, if they are not empty, though). To display the directory in full, select the `Show hidden groups` item in the contextual menu of any element of the directory.

5. User interface of the anti-virus console and the anti-virus agent

5.1. Anti-virus console

The anti-virus network is administrated through the anti-virus console interface.

The following elements form the main console window (read above in pic. 8):

- Main menu line (in the upper part of the window)
- Control panel (under the main menu)
- Hierarchy list (directory) of the anti-virus network (left part of the window)
- Information pane in the bottom part of the window

The search panel is located near the directory (it resides under the directory).

The setting of parameters of the elements of the anti-virus network's directory is made in the contextual menu of these elements.

By default, the toolbar resides in the right part of the console window. It contains the list of settings dubbing the set of elements of the lower level of the contextual menu. Below the modification of settings of the contextual menu is described only.

The console operates in the standard graphical user interface, which is an analogue to that used in Windows and in the graphical environments of Unix-based OSs. The tasks solved with the help of this interface are described in details in the next section. Below goes the brief overview only.

The `File` menu contains the following elements:

- `Connect Dr.Web(R) Enterprise Server` — ask for registration on the server; if the console is connected to the

server, it is disconnected from the current server before the connection

- `Dr.Web(R) Enterprise Console settings` — allow to specify the parameters of connection to the server, the language of the interface, console log details, etc.
- `Disconnect Dr.Web(R) Enterprise Server` — disconnect from the current server;
- `Exit` — disconnect from the server and terminate the program

The `Administration` menu contains the following items:

- `Administrators` — opens the window for administrating the accounts of the anti-virus network's administrators (read p. 7.2)
- `Configure Dr.Web(R) Enterprise Server` — opens the window with main server settings (read p. 6.5.2)
- `Configure repository` — repository setting (simple editor and detailed per-component setting, read p. 6.5.5)
- `Dr.Web(R) Enterprise Server schedule` — opens the window for scheduling tasks for the server (read p. 6.5.3)
- `Neighborhood` – opens the window for managing the connections between the servers of the anti-virus network with several servers (read p. 6.6)
- `Edit templates` – opens the window of the editor of the notifications' templates (read p. 6.5.2.4)
- `Alerts` — viewing the server messages (read p. 6.5.8)
- `Statistics` — viewing the server statistics (read p. 6.5.6)

- `Show Dr.Web(R) Enterprise Server log` — opens the window for modifying the server protocol (read p. 6.5)
- `Unapproved stations` — opens the window with the list of unapproved stations (read p. 0)
- `Remote data` — displays information on the anti-virus network's operation received from other servers (read p. 6.6)
- `Check for updates` — opens the window to check the updates of the software regardless the schedule and other server settings
- `Network browser` – this component scans the local network to define if the workstation's anti-virus software was installed on the computer and the set of its components
- `Show version` — opens the window with the detailed information about the version of the anti-virus server
- `Restart Dr.Web(R) Enterprise Server` — initiate the current anti-virus server reboot (connection between the server and the console will be interrupted)
- `Shutdown Dr.Web(R) Enterprise Server` — terminate the current anti-virus server

The `Style` menu allows to modify the external outlook and the theme of the console.

The toolbar buttons dub the menu items `File`—`Remote server`, `File`—`Exit`, `Server`—`Configure server`, `Server`—`Server schedule`. Besides, there is the  (`Refresh`) button in the toolbar.

The anti-virus console allows to set up not only the parameters of the server, but also the parameters of the connected workstations, which are stored on the server, as well as the configuration of the network.

An element or elements which are to be set up should first be selected in the anti-virus network directory. Possible options will be displayed in the contextual menu of this element (elements) of the directory.

The search panel facilitates the search of the necessary element. The panel allows to find all groups or stations the names of which coincide with the definite line, begin with it, end with it, and also those the names of which coincide with the regular expression specified in the search line.

To access rapidly the most items and sub items of the menu hot keys are used. They are listed in Table. 2.

Table 2.

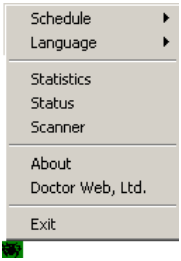
Hot key	Menu — submenu item
Alt-C	File — Connect server
Alt-P	File — Console settings
Alt-D	File — Disconnect server
Alt-X	File — Exit
Alt-M	Administration — Administrators
Alt-F	Administration — Configure Dr.Web(R) Enterprise Server
Alt-Y	Administration — Configure repository — Entire repository settings
Alt-S	Administration —Dr.Web(R) Enterprise Server schedule
Alt-N	Administration — Neighborhood
Alt-T	Administration — Edit templates
Alt-L	Administration — Alerts

Alt-I	Administration — Statistics
Alt-O	Administration — Show Dr.Web(R) Enterprise Server log
Alt-A	Administration — Unapproved stations
Alt-R	Administration — Remote data
Alt-V	Administration — Show version
Alt-U	Administration — Check for updates
Alt-B	Administration — Network browser
Alt-H	Help — About program

5.2. Anti-virus agent

Being run in the Windows environment, the anti-virus agent generates an icon in the task bar (pic. 11).

Some functions of administration of the workstation are accessible through the contextual menu of this icon (pic. 11).



Picture 11. The icon and the contextual menu of the anti-virus agent

The settings accessible through the agent's contextual menu depend upon the configuration of the workstation specified by the means of the anti-virus network.

The icon's outlook depends on whether or not the workstation is connected to the server and on other parameters:

- Black picture on the green background — the agent operates correctly and connects to the server
- The icon is red-crossed — the agent does not operate and the server is inaccessible
- Red exclamation mark in the icon's background — the agent requests the workstation's reboot
- The icon's background is red — updating error of the package components

In case of critical updating error:

1. Investigate the reason of error by studying the log files of the agent and of the Updating module on the workstation (by default, they reside in the `logs` subdirectory of the agent's installation directory, and are `drwagntd.log` and `drwupgrade.log` files accordingly).
2. Remove the reason of error.
3. Run the forced updating of the workstation (read p. 6.2.6).

6. Administrating the anti-virus network

6.1. Planning, building and modifying the network's structure

6.1.1. Selection of the anti-virus server

The selection criterion of the server on which the software of the anti-virus server is installed and the procedure of creation of the server are described above in p. 2.1.1.

6.1.2. Groups. Preinstalled groups, creation of new groups. Removing groups

The grouping is designed for easy administration of the workstations of the anti-virus network.

Grouping of stations allows to specify the settings for all workstations in the group with one line, as well as to initialize certain tasks on all stations. The groups can also be used for building (structuring) the list of workstations.

During the program complex' installation the so-called *preinstalled* groups are created

The `Everyone` preinstalled group includes all workstations.

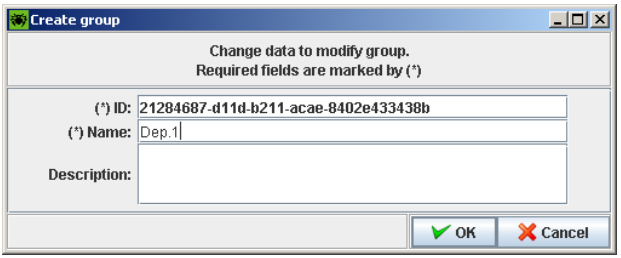
The set of the `Online` and the `Offline` groups is changing automatically during the server's operation; the first of them includes all active workstations (responding to server's requests), the other group — all disabled.

Other preinstalled groups contain the workstations operated by certain OSs or families of OS, and also those using certain network protocols. The set of preinstalled groups cannot be modified manually.

You can create your own groups and include the connected workstations into them.

To create a new group:

1. Select the `Create group` item in the contextual menu (the item is enabled regardless what elements of the directory are chosen). A window for group creation will open (pic. 12).



Picture 12. Creating a new group

2. The `ID` entry field is filled in automatically. You can also edit it, if necessary. The identifier should not contain blanks.
3. Input the group name into the `Name` entry field.
4. Make comments in the `Description` entry field.
5. Press `OK`.

You can also delete the groups created by you (preinstalled groups cannot be deleted). For this, select the group, and then select the `Cancel` item in the contextual menu.

Originally, the groups created by you are empty. The procedure of adding the workstations into them is described in the next section.

All groups reside on one hierarchy level of the directory. Nesting of groups is impossible.

6.1.3. Adding workstations to a group. Removing workstations from a group

To add a workstation (not preinstalled) to a group:

1. Select the necessary group in the directory.
2. In the contextual menu, select the `Stations` item. A window for setting the group will open (pic. 13).

Picture 13. Adding a workstation to a group

3. Mark the station to be added to the `Known groups` list and press  .

The same procedure is applied for removing a workstation from a group; the stations to be removed are selected in the `Members` list and then the  button should be pressed.

You can also add a workstation to a group using the station's settings, read p. 6.2.1.

You cannot modify the set of preinstalled groups.

6.2. Administrating a station of the anti-virus network

The anti-virus network operated by Dr.Web ES provides for centralized setting of anti-virus packages on workstations. The complex allows:

- to set the configuration parameters of anti-virus programs
- to schedule scanning launch tasks
- to launch separate tasks on workstations, regardless the settings of the schedule
- to update the workstations, after the updating error as well – with error state reset

At the same time, the administrator of the anti-virus network can enable a user of a workstation to set the configuration and to launch tasks, to prohibit these actions or to restrict them.

The configuration of the workstation can be modified even when it is temporary disconnected from the server. These changes will be accepted by the workstation as soon as the connection with the server is established.

6.2.1. Inheritance of the configuration elements of a workstation from the configuration of a group. Primary groups

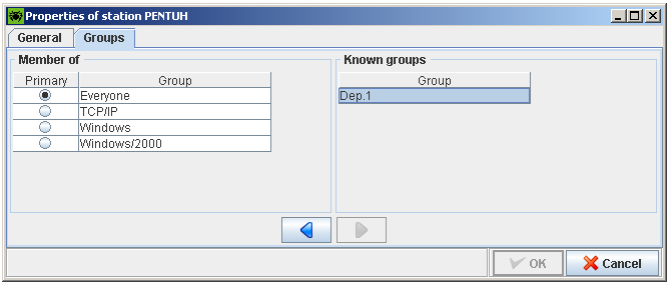
When a new workstation is connected, the elements of its configuration are adopted (inherited) from one of the groups it belongs to (*primary* group). If the settings of the primary group are modified, these changes are inherited by the workstations included into the group. When creating a workstation, you can specify what

groups will be regarded as primary. By default, this is the Everyone group.

If Everyone is not the primary group, and the specified primary group does not have customized settings, the settings of the Everyone group are inherited.

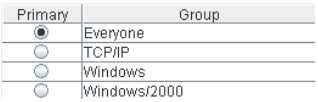
To find out what group is primary and to change it, if necessary, do the following:

1. Select the Properties item in the contextual menu. A Properties of station.. window will open. Go to the Groups pane (pic. 14).



Picture 14. Groups of a workstation

2. If necessary, reassign the primary group by pressing the Primary radio button against the necessary group (pic. 15).



Picture 15. Selection of a primary group

3. Press OK.

You can also make the group primary for all workstations included into it. For this, select the necessary group in the directory, and then select the `Become primary` item in the contextual menu.

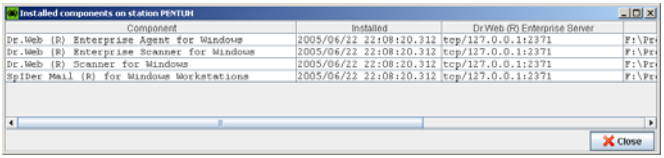
You can also assign the certain group as primary for the selected workstations. For this, select the necessary workstations in the directory (you can also select groups – the action will be applied to all the workstations included into them), then select `Assign as primary group` in the contextual menu. A window with the list of groups which can be assigned as primary for these workstations will open. Select the necessary group and press `OK`.

By default, the network structure is displayed so as to demonstrate the inclusion of a station into all groups the member of which it is. If you want the workstations to be displayed in the network directory in primary groups only, deselect `Full membership` in the contextual menu.

6.2.2. Viewing the configuration of a workstation

To view what components of the anti-virus package are installed on a workstation:

1. Select the workstation in the directory of the console main window.
2. Select the `Installed components on station` item in the contextual menu. A window with the list of the installed components will open (pic. 16).



Picture 16. The list of the installed components of the anti-virus protection

3. Study the list and press `Close`.

The list of the installed components depends on the OS of the workstation.

To view what virus bases are installed on the workstation:

1. Select the `Virus bases` item in the contextual menu. A window with the list of the installed virus bases and their descriptions will open.
2. Study the list and press `Close`.

The same procedure is applied to view the workstation's neighborhood. For this, press the `Neighborhood` item in the toolbar.

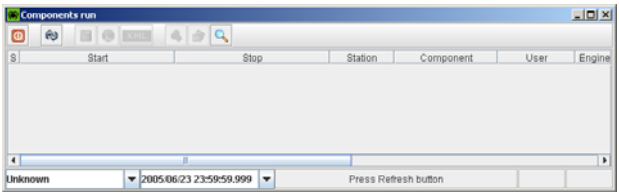
6.2.3. Viewing the logs and statistics of the workstation

You can view the results of operation of the workstation's components — updates of software, anti-virus scannings and anti-virus monitoring.

Being installed with the default settings, i.e. without any interference of the anti-virus network's administrator, the anti-virus guard and, periodically, the tasks to update the software are run on the workstation, as well the anti-virus scanning.

To view the list of components run on the workstation:

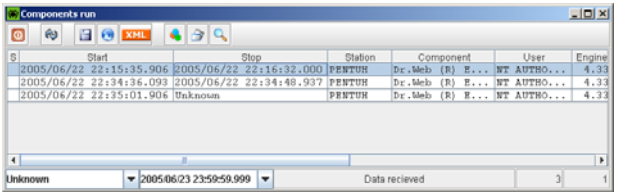
1. Select the `Tables` item, in the contextual menu, in the opened submenu select the `Start/Stop` item. A `Components run` window will open (pic. 17).



Picture 17. Components run (no data is loaded)

2. In the dropdown lists in the left bottom part of the window select the time interval for which the data should be displayed (by default, all data available is displayed).

3. To load data into this window, press  . A table with the data on the run components will be loaded into the window (pic. 18).



Picture 18. Data on the tasks performed

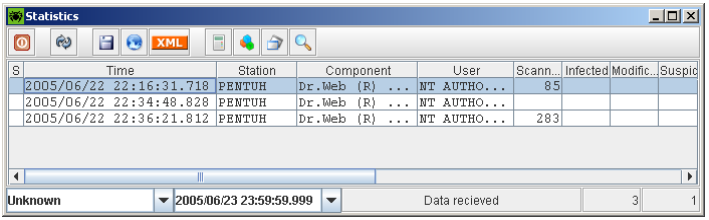
4. To view any line of the table in a more suitable mode, select the necessary line in the table and press  (or double click the necessary line). A window with the detailed information on the necessary line will open.

If several lines are selected in the table, the detailed information on each line will be displayed in a separate window.

5. To save the table for printing or future processing, press (to save it in the CSV format), or (to save it in the HTML format), or (to save it in the XML format).

To view the statistics on operation of the anti-virus programs on the given station:

1. Select the `Tables` item in the contextual menu, in the opened submenu select the `Statistics` item in the toolbar. A statistics window will open (with no data loaded).
2. In the dropdown lists in the left bottom part of the window select the time interval for which the data should be displayed (by default, all data available is displayed).
3. To load data into this window, press . The statistics table showing the results of operation of the anti-virus programs on the given station will be loaded (pic. 19).



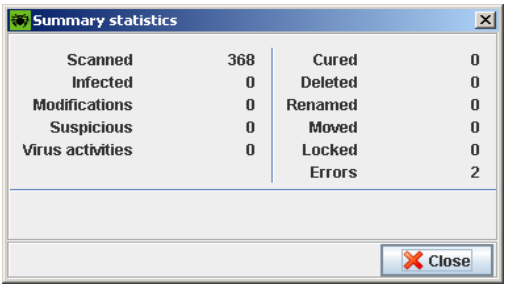
Picture 19. Statistics of anti-virus programs' operation on a workstation

4. To view any line of the table in a more suitable mode, select the line in the table and press (or double click the necessary

line). A window with the detailed information on the given line will open.

If several lines are selected in the table, the detailed information on each line will be displayed in the separate window.

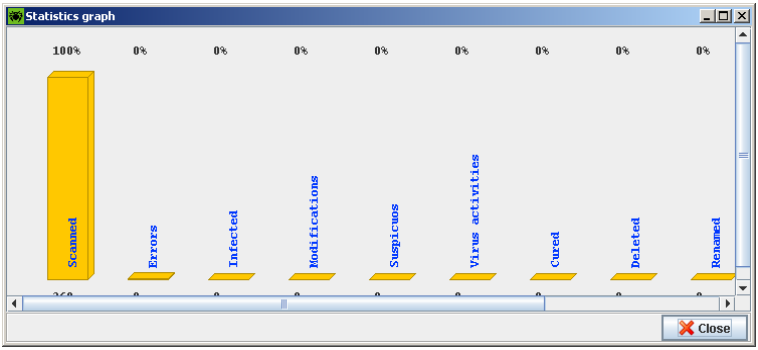
5. To save the table for printing or future processing, press  (to save it in the CSV format), or  (to save it in the HTML format), or  (to save it in the XML format).
6. To view the summary statistics not splitted on sessions, press  . A window with summary statistics will open (pic. 20).



Picture 20. Summary statistics

The summary statistics window can also be opened from the contextual menu of the station. For this, select the `Summary statistics` item.

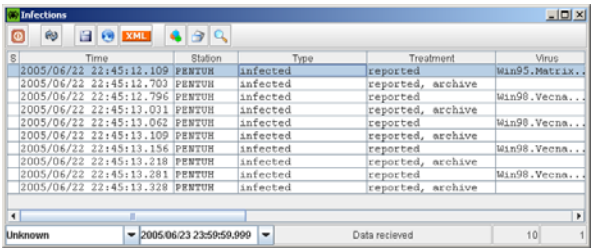
7. To view the statistics as the diagram, press  in the statistics' window. A statistics graph window will open (pic. 21).



Picture 21. Statistics graph

To view the report on infected viruses (the list of infected objects, the virus and actions of the anti-virus, etc.):

1. Select the `Tables` item in the contextual menu, and then select the `Infections` item in the opened submenu. A window for viewing the detected infections will open (with no data loaded).
2. In the dropdown lists in the left bottom part of the window select the time interval for which the data should be displayed (by default, all data available is displayed).
3. To load data into this window, press  . The table with the infected objects detected on the given station will be loaded into this window (pic. 22).

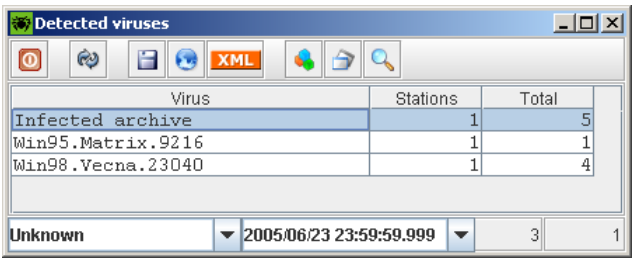


Picture 22. Infections

4. The formatting of data in this table is the same as for the statistics table described above.

To view the grouped data on the types of viruses detected on stations:

1. Select the `Tables` item in the contextual menu, and then select the `Viruses` sub item. A `Detected viruses` window will open (with empty data).
2. In the dropdown lists in the left bottom part of the window select the time interval for which the data should be displayed (by default, all data available is displayed).
3. To load the data into this window, press  . The table with the detected viruses will be loaded into this window (pic. 23).



Picture 23. Detected viruses

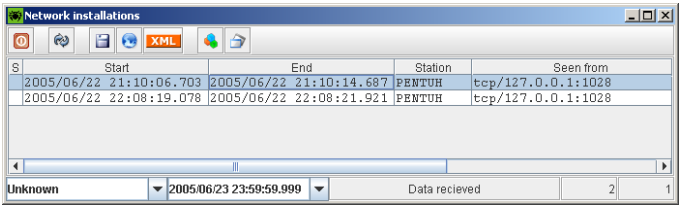
4. The formatting of data in this table is the same as for the statistics table described above.

To view the list of the workstation's software settings:

1. Select the `Network installations` item in the contextual menu. A `Network installations` window will open (with no data loaded).

2. In the dropdown lists in the left bottom part of the window select the time interval for which the data should be displayed (by default, all data available is displayed).

3. To load the data into this window, press  . The table of installations tasks will be loaded into the window (pic. 24).

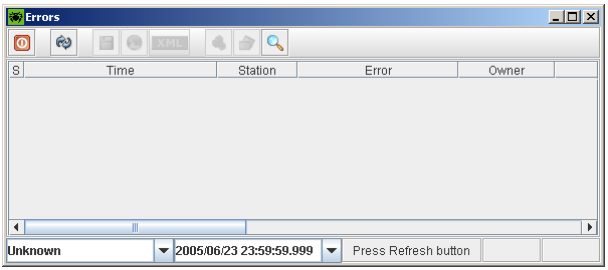


Picture 24. Network installations

4. The formatting of data in this table is the same as for the statistics table described above.

To view the list of scanning errors on the given station for some period of time:

1. Select the `Tables` item in the contextual menu, and then select the `Errors` item in the opened submenu. A window for viewing the list of scanning errors will open (pic. 25).

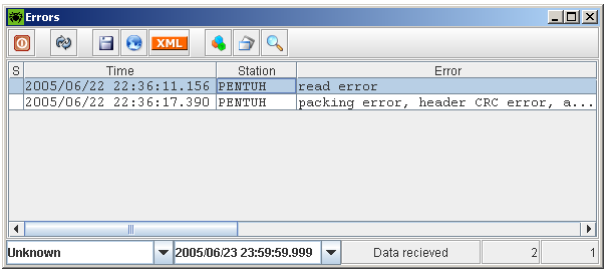


Picture 25. Requesting the list of scanning errors

2. In the dropdown list in the left part of the window select the date and time of the beginning of the period, in the dropdown

list in the right part of the window select the date and time of the end of the period.

3. Press  . The list of scanning errors will be loaded into the window (pic. 26).



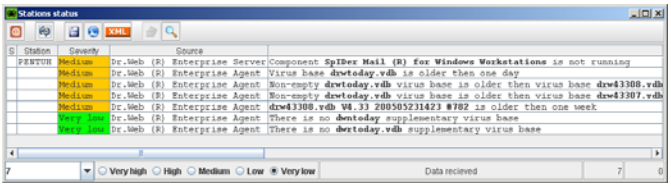
Picture 26. List of scanning errors

4. The formatting of data in this table is the same as for the statistics table described above.

To view the data on an unusual and (possibly) requiring interference condition of workstations for a definite period:

1. Select the `Table` item in the contextual menu, in the dropdown menu select the `Status` item. A window for setting the request will open (with empty data).

2. Press  . The data on the workstations' condition will be loaded into the window (pic. 27).



Picture 27. Stations status

3. To limit the list of the stations' status by the data of certain gravity, select the level of gravity in the group of radio buttons in the lower part of the window. By default, the `Very low` gravity level is chosen and the full list is displayed.
4. The list will also include the stations disconnected for several days from the server. Input this number into the entry field in the left bottom part of the window or select it in the dropdown menu.
5. The formatting of data in this table is the same as for the statistics table described above.

6.2.4. Setting the anti-virus software and the agent

6.2.4.1. Editing parameters of the anti-virus package components

The default configuration files for all connected workstations (inherited from preinstalled groups) are stored on the server. To edit the settings for the given workstation of any anti-virus component, select it in the toolbar. The following components become available:

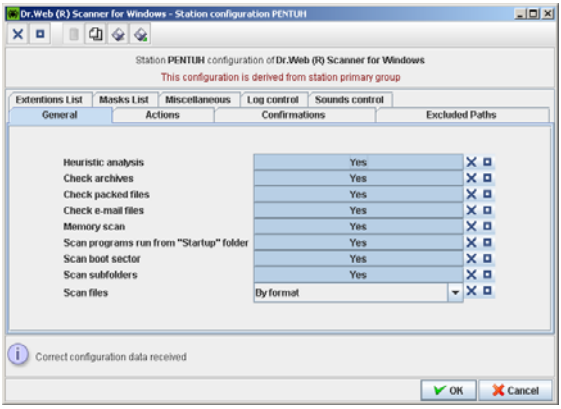
- Dr.Web Scanner for Windows
- SpIDer Guard XP
- SpIDer Guard ME
- SpIDer Mail for Windows workstations

Below is described the editing of settings by the example of the scanner.

To modify the setting of the scanner for Windows on a workstation:

1. Select the `Configuration` item in the contextual menu, and then select the `Dr.Web® Scanner for Windows` item in

the opened submenu. A `Station configuration` window will open (pic. 28).



Picture 28. Editing scanner's configuration

2. Edit the necessary parameters in the panes of this window.

The set of parameters and the recommendations on how to specify them are located in the User manual for the anti-virus package. At the same time, the console interface somewhat differs from the interface of correspondent components of the anti-virus:

- To modify the parameters values, which can be specified as `Yes` or `Now`, click the necessary value
- Entry fields and dropdown lists have standard interface
- To restore the value the parameter had before the editing, press 
- To enable the parameter's default value, press  .

3. To restore the values all parameters had before the editing, press  in the toolbar in the upper part of the window. To enable the default values for all parameters, press  in the

toolbar. To export parameters to the specially formatted text file, press  . To import parameters from such file, press 

4. Press `OK` to confirm the changes made, or press `Cancel`, to restore the state of the configuration before editing, or press  (`Delete`), to delete a specific configuration for the given workstation (the configuration inherited from groups will be specified again).

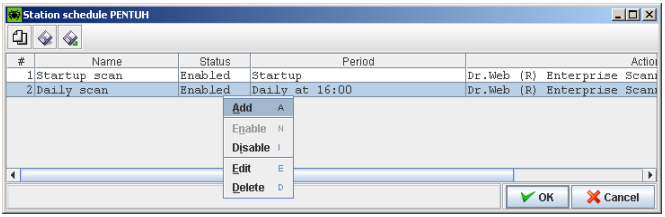
The components of the anti-virus packages are set up similarly.

If SpIDer Guard is run on a workstation, and the infected objects are detected by the scanner, in these cases when the actions of the scanner (opening of infected files) provoke SpIDer Guard's reaction, for these objects the actions set for SpIDer Guard are applied, and not for the scanner. To avoid this (and to speed up the scanning) in SpIDer Guard's settings the default `Smart` mode should be preserved, and the quarantine directory of the scanner should be added into the paths excluded from search.

6.2.4.2. Editing the schedule of the automatic launch of tasks on a workstation

You can edit the centralized schedule (stored on the server) of tasks of the given workstation. For this:

1. Select the `Schedule` item in the contextual menu. A window for editing the schedule will open (pic. 29).



Picture 29. Station schedule

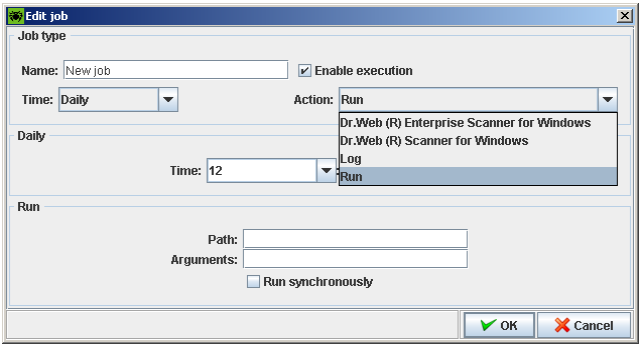
2. You can remove the existing tasks, add new tasks or edit the existing tasks. You can also disable the task or enable the task disabled before. This action is described in details below.
3. When editing of the schedule is finished, press `OK` to accept changes, or press `Cancel` to close the window without any changes in the schedule.

If after the editing an empty (without any task) schedule will be created, the console will offer you either to use the schedule inherited from groups, or to use the empty schedule.

To remove any task, select it in the list and then select the `Delete` item in the contextual menu.

To add a new task:

1. Select the `Add` item in the contextual menu. A window for creation of a new task will open (pic. 30).



Picture 30. Editing (adding) a task

2. Input the name of a task into the `Name` entry field.
3. In the `Action` dropdown list select the type of the task. After the selection is made, the bottom part of the window will look differently, depending on the action selected.

   If `Run` is selected, input the full name (with the path) of the executable file to be launched into the `Path` entry field, input the command line parameters for the program to be run into the `Arguments` field.

   If `Dr.Web(R) Scanner for Windows` is selected, input the scanner command line parameters into the `Arguments` field.

   If `Dr.Web(R) Enterprise Scanner for Windows` is selected, a window for setting the scanning described in p. 6.2.6 will open.

   If `Log` is selected, input the text of the message sent to the server into the `String` field.
4. Set the time the task has to be launched. For this, select first one of the launching modes in the `Time` dropdown list:
   - `Daily`

- Monthly
- Weekly
- Hourly
- Shutdown
- Ever X minutes
- Startup

For Startup and Shutdown modes there should be no additional parameters; the task will be launched at a start or when the station is shutdown.

For Every X minutes mode the X value should be specified.

If X equals to 60 or more, the task will be launched every X minutes. If X is less than 60, the task will be launched on every minute of the hour divisible to X.

For the Hourly mode the integer from 0 to 59 setting the minute of every hour when the task is launched should be specified.

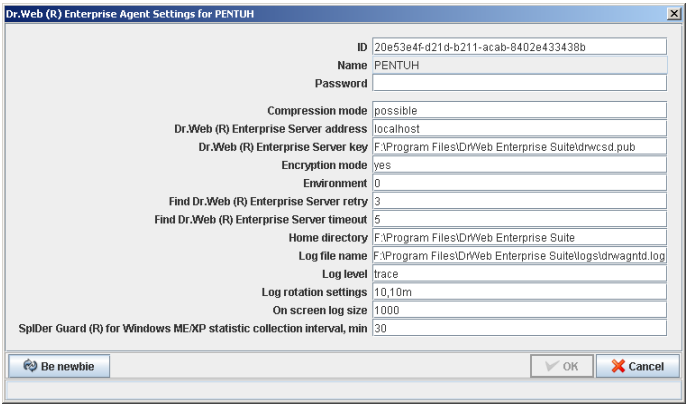
For the Daily mode the hour and the minute should be input — the task will be launched daily on the time specified. For the Weekly mode, the day of the week should be selected in addition, and for the Monthly mode — the date (day of the month).

5. When all parameters for the task are input, press OK.

   To edit the existing task, select it in the list and then select the Edit item in the contextual menu. Further actions are similar to the procedure of creation of a new task.

6.2.4.3. Viewing and editing the configuration of the anti-virus agent

To view and edit the configuration of the anti-virus agent, select the `Configuration` item in the contextual menu, and then select the `Dr.Web® Enterprise Agent` item in the opened submenu. A window for setting up the agent will open (pic. 31).



Picture 31. Setting the anti-virus agent

Any changes in these settings incompatible with the server settings (for example, changes in the encryption and compression modes and in the encryption key) will result in disconnection of the agent from the server.

If any changes in the agent's settings are made, the `OK` button becomes accessible. Press this button to accept changes in settings. To reject changes in settings and to close the window press `Cancel`.

To instruct the server to connect the station anew, press `Be Newbie`.

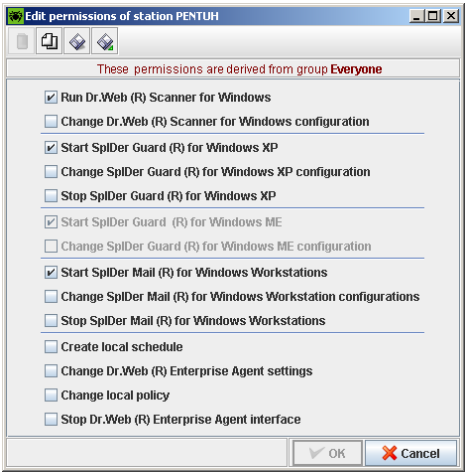
Viewing and editing of the agent's settings disconnected from the server is impossible.

6.2.5. Setting users' permissions

The anti-virus packages on the workstations are operated by the anti-virus agent. The configuration parameters of the anti-virus means are downloaded by the agent from the server and presented to the anti-virus programs. Such architecture allows to administrate users' access to settings of the anti-virus on the workstation, including the disabling of the intrusion.

To set the permissions for a user of a workstation to administrate the anti-virus package:

1. Select the `Permissions` item in the contextual menu. A window for editing permissions will open (pic. 32).



Picture 32. Editing permissions

2. By default, a user is authorized to launch each component, but not to edit the configuration of the given component or terminate them. To change (enable or disable) any permission, check or uncheck any checkbox.
3. To accept the changes in permissions, press `OK`.

To reject changes (and to close the editor window), press `Cancel`.

To cancel the permissions' configuration and to restore the default configuration inherited from the preinstalled groups, press  (`Delete`) (read p. 6.3.3. for more details).

You can also export permissions' data into the specially formatted file by pressing the  button, or import this parameter from such file by pressing the  button.

When the complex is installed and approved by administrators and users, it is recommended to use the default settings. In future, it is advisable to reduce user permissions to minimal.

6.2.6. Launching and terminating the anti-virus scanner on workstations. Forced updating of the workstation's software

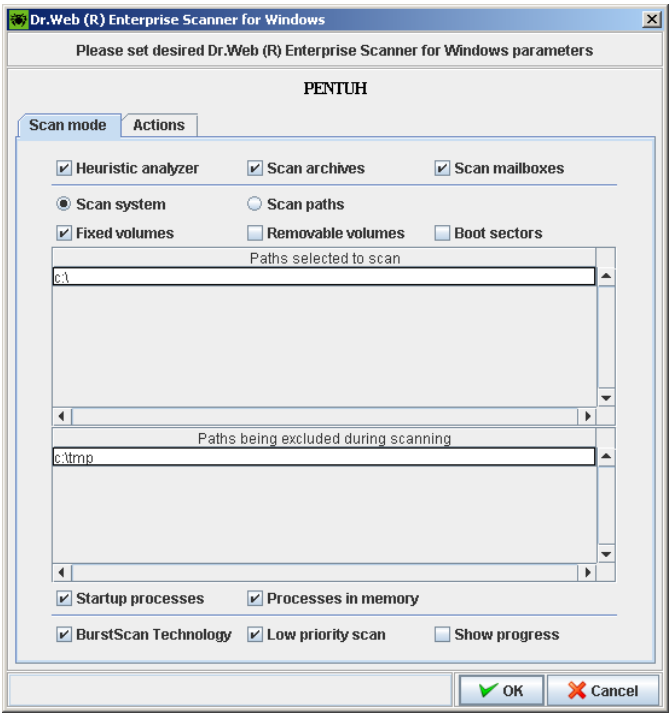
You can launch the task of the anti-virus scanning on a workstation and set the parameters of this scanning.

You can view the list of all scannings active at present (both run manually by you or users and those run on the schedule).

You can terminate a task for scanning the anti-virus station (both run manually by you or users and those run on the schedule).

To launch the task for scanning:

1. Select the `Check for viruses` item in the contextual; menu. A window for setting the task will open (pic. 33).



Picture 33. Setting the scanning

2. Specify the scanning parameters and the set of objects of the file system to be scanned (these actions are described in details below).
3. Press `OK`, to run the scanning on the workstation.

Below are cited the recommendations on how to set the scanning parameters.

The Heuristic analyzer box is checked by default, the scanner makes attempts to detect the unknown viruses. Under this mode the scanner may trigger false alarms.

The Scan archives box checked by default instructs the scanner to search for viruses in files packed into file archives and containers of different types.

The Scan mailboxes box checked by default instructs to scan mailboxes.

To specify what objects should be selected for scanning, choose one of the two alternative modes — either Scan system or Scan paths. If Scan system is selected, specify what system drives should be checked (if Fixed volumes and Removable volumes checkboxes are selected, all drives of these types are checked). If Scan paths is selected, the lists of scanned paths are selected, and, if necessary, the list of paths excluded from search (the way how they should be specified is described below). The paths excluded from search can also be specified in the Scan system mode.

Select the Boot sectors checkbox to instruct the scanner to scan boot sectors of drives selected for scanning (or those drives where the files selected for scanning reside). The boot sectors of logical drives and the main boot sectors of physical drives are scanned.

The Startup processes box checked by default instructs to scan the files automatically launched at the system startup.

The Processes in memory box checked by default instructs to scan the processes run in the main memory.

The BurstScan technology box checked by default instructs to use this technology, considerably increasing the scanning speed in modern systems.

The Low priority box checked by default instructs to launch the scanning if other processes are deactivated only.

If necessary, check the Show progress box (this mode considerably increases the network traffic).

The Infected files dropdown list sets the scanner's reaction upon detection of a file infected with a known virus:

- The Cure action (enabled by default) instructs the scanner to restore the state of the file system as it was before infection (full recovery is usually impossible, functionally correct state should be restored). If curing is impossible, the action specified for incurable files is applied (read below).
- The Report action instructs to only report about the detection of a virus (read p. 6.5.2.4 on how to set notifications)
- The Move to action instructs to move infected files to the quarantine directory
- The Delete action instructs to delete infected files

The Incurable files dropdown list sets the scanner's reaction upon detection of a file infected with a known incurable virus (and when the attempt to cure it failed). By default, the Move to action is specified, and other described above variants are available too (except for Cure).

The Suspicious files dropdown list sets the scanner's reaction upon detection of a file presumably infected with a virus (reaction of the heuristic analyzer). Possible actions are the same as for incurable files (by default, it is Move to, as well as Delete, Report).

At scanning including the OS installation directory it is advisable to select the `Report` action for suspicious files instead of the default `Move to` action.

The `Infected archives` dropdown list sets the scanner's reaction upon detection of an infected or suspicious file in a file archive or a container. The reaction is set for the whole archive. Possible actions are the same as for incurable files (by default, it is `Move to`, as well as `Delete`, `Report`).

The `Infected boot sectors` dropdown list sets the scanner's reaction upon detection of an infected or suspicious boot sector. The `Cure` action is specified (by default, it is disabled for suspicious and incurable) and `Report`.

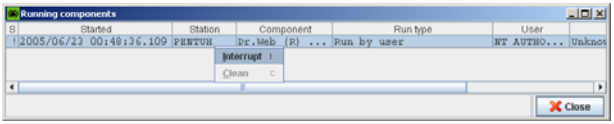
The `Adware` dropdown list sets the scanner's reaction upon detection of this type of unsolicited software. Possible actions are `Move to` (by default), `Ignore`, `Delete` and `Report`.

The same way the reaction upon detection of dialers is set.

The scanner's reaction upon detection of other kinds of unsolicited programs is set in the same way. The default scanner settings in these cases are illustrated.

To view the list of scannings performed and, if necessary, to terminate some of them:

1. In the contextual menu, select the `Components run` item. The list of running components will open (pic. 34).



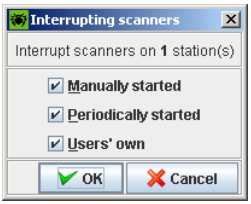
Picture 34. Components run

2. If any task should be terminated, select it in the list and then select the `Interrupt` item in the contextual menu. The task remains in the list, but is marked by the `X` symbol in the first column.
3. To clear the list from interrupted tasks, select the `Clean` item in the contextual menu.

You can also interrupt all scannings at once, if certain criterion is met. This is especially useful if such instruction is sent to numerous stations at once.

To interrupt all scannings of a definite type:

1. Select the `Interrupting scanners` item in the contextual menu. A window for setting the type of interrupting scannings will open (pic. 35).



Picture 35. Setting scannings interruptions

2. Check the boxes against the types of scannings you want to interrupt immediately.
3. Press `OK`.

Usually, the software of a workstation is updated automatically. Still, if necessary, you can update it manually, after previous unsuccessful automatic updating too.

To run the updating of the software of a workstation:

1. Select the `Speed up normal update` item in the contextual menu of the workstation or a group.
2. In the opened submenu select the `Update failed components` item, if you want to update only those components, the previous updating of which failed, and reset the error state; select the `Update all components` item, if you want to forcedly update the failed components, as it is described above, or select the `Speed up normal update` item, if you want to update only when the error state is reset.

You can also update with the help of the anti-virus agent.

For this:

1. Permit a user of the given workstation to make changes in settings of the anti-virus agent (read p. 6.2.5).
2. Select the `Synchronize` item in the contextual menu of the agent's icon
3. In the opened submenu, select the `Only failed components`, if you want to update only those components which were updated with the error and to reset the error state, or `All components`, if you want to launch the updating of the failed components, as it is described above and for all other components.

6.3. Administrating several workstations simultaneously. Using groups

6.3.1. Advantages of synchronous administration and tools for it

The company's anti-virus network can have tens, hundreds or even thousands computers. Individual administration of large number of workstations is very labour-consuming and unproductive.

The Dr.Web ES program complex provides for simultaneous administration of numerous stations. For this, the complex includes several options:

- To view the settings and specify instructions for several workstations selected in the directory manually
- The integration of workstations into groups on the basis of the OS and of the family of the OS, as well as arbitrary integration
- The complex allows to specify settings for groups and these settings will affect both the computers inside the group, and those included into it earlier
- Inheritance of settings of any workstation or a group by other groups

Below goes the detailed description of these options and their application.

6.3.2. Manual administration of several computers

To administrate several workstations simultaneously, select these stations in the network directory.

The following options of administration of the selected stations become enabled in the contextual menu:

- Viewing the statistics (including infections, viruses, launch /termination and installation) and the summary statistics
- Launch, viewing and termination of tasks for scanning

6.3.3. Setting a group. Using groups for setting workstations

The program complex allows to combine the workstations into groups. Each station makes part of the `Everyone` group, as well as of the group correspondent to the OS of the stations and to the family of the OS. There is an option to set uniform settings for the whole group, and these settings will be inherited by all workstations belonging to the group (if later personal settings will not be specified for them).

Immediately after the installation, the default and uniform for all workstations settings will be specified for the `Everyone` group. These settings are inherited by all other groups and all workstations. You can later specify different default settings for different OSs by changing the settings for definite groups.

You can also arbitrary create new groups and include computers into them, for example, in accordance with the company's anti-virus protection policy.

To specify the settings of a group (the default settings of workstations in a group):

1. Select a group in the network's directory.
2. Select the necessary setting in the toolbar and edit it.

The group's settings include the configuration of the anti-virus programs, the schedule and setting of permissions. These settings are similarly edited, as described in p. 6.2 for the workstation.

The agent's settings are not included into the group's configuration and cannot be specified through the groups' procedure.

For the separate group and for several selected groups you can run, view and terminate the tasks for scanning. The same way you can view the statistics (including infections, viruses, launch/termination, scanning and instillation errors) and summary statistics for workstations of the group or several groups.

When viewing or editing the elements of the workstation's configuration inherited from Primary group, a colorful inscription becomes visible in correspondent window `These permissions are derived from group Primary`.

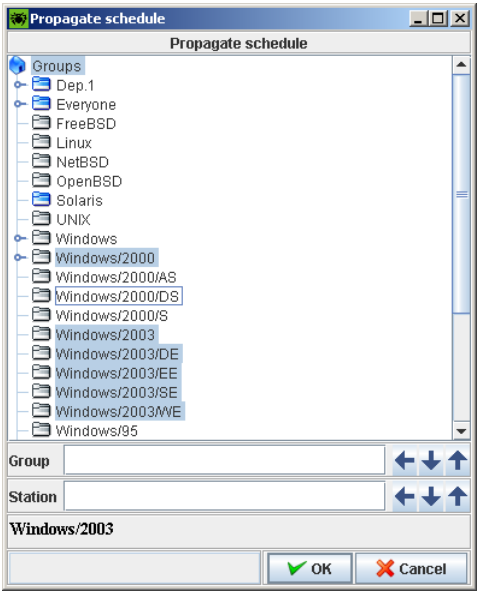
If you modify the configuration of a workstation, this inscription will disappear and the  (`Delete`) button will become enabled in the toolbar. You can restore the configuration inherited from the primary group; press this button for this.

6.3.4. Propagation of settings

Configuration settings of anti-virus programs, the schedules and permissions of users of a group, or of workstations can be copied (*spread*) into a group or several groups and workstations.

For this:

1. In the window for editing the configuration of the anti-virus component (read p. 6.2.4.1), the schedule (read p. 6.2.4.2) or permissions (read p. 6.2.5) press  (`Propagate`). A window of the network's directory will open (pic. 36).



Picture 36. Directory of the anti-virus network

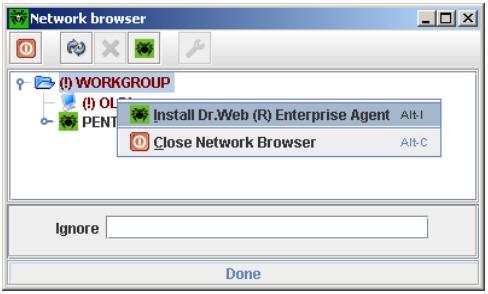
2. Select in this list the groups and stations you want to propagate the setting.
3. To enable changes in the configuration of this group, press `OK`, to reject the action and close the window – press `Cancel`.

6.4. Controlling protection of the local network. Remote installation of the anti-virus software

The directory of the anti-virus network in the main console window displays only those computers which are already included into the anti-virus network. The program complex allows also to discover computers (workstations and servers of the local network) on which anti-virus protection by Dr.Web Enterprise Suite is not installed yet and, in some cases, to install remotely this protection.

For this:

1. Select the `Network browser` item in the `Administration` menu. A window of the same name with no data loaded will open.
2. Input the list of domains (work groups) the data on which should be omitted into the `Ignore` entry field. If this field is not specified, a report on the whole available local network will be generated.
3. Press  . The directory (hierarchy list) of computers of the local network stating those where the anti-virus software is installed or not will be loaded into this window (pic. 37).



Picture 37. A network browser window. The local network directory

Unfold the elements of the directory corresponding to work groups (domains).

The computers where the anti-virus software is not installed, as well as the work groups containing them, are marked in the directory by red and the (`!`) symbols.

Computers to which the given user has no access rights are marked in the directory by the (`?`) symbol.

Computers inaccessible at the moment the information on which is still listed in the Master Browser service in Windows, are marked in the directory by the (??) symbols.

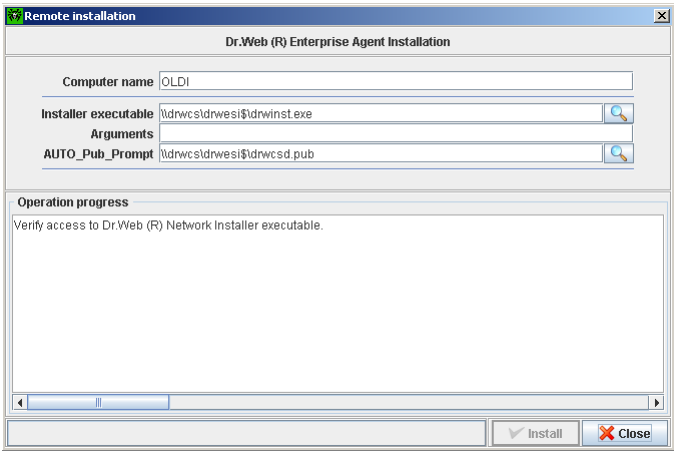
Computers operated by Windows 95/98/Me will be shown as unprotected, if the File and printer sharing for Microsoft Networks is not enabled on them in the I want to be able to give others access to my files mode.

The elements of the directory corresponding to computers can be additionally unfolded and the set of the installed components can be viewed.

If you use the version of the console operated by Windows, you can remotely install the anti-virus software (the anti-virus agent) on the discovered unprotected computers run under Windows NT/2000/XP/2003.

For this:

1. Select the unprotected computer in the Network browser window.
2. In the contextual menu of this computer, select Install Dr.Web(R) Enterprise Agent.
3. A window for setting the agent's installation task will open (pic. 38).



Picture 38. Remote installation of the agent

4. Input the computer network name into the `Computer name` entry field.
5. In the `Installer executable` field the full name of the network installer is specified. Edit it, if necessary.
6. If necessary, input the network installer command line parameters into the `Arguments` field (read more in Appendix G4.)

6.5. Setting the anti-virus server

6.5.1. Logging on the server. Viewing the log

The anti-virus server logs events connected with its operation. By default, the syslogd service is used for logging under UNIX; under Windows the log file resides, by default, in the `var` subdirectory of the server installation directory; its name is `drwcsd.log`. This is an ordinary text file.

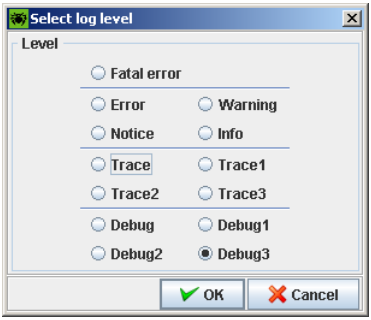
The server's log is used for debugging and for corrections of malfunctioning in case of abnormal operation of the program complex.

The administrator can view the extracts from the server log in the anti-virus console window. Before to open the window for viewing the extracts from the log, the details level of the displayed data can be set up.

The extracts from the log since the moment it is opened are displayed in this window; you cannot view the earlier entries here.

To select the log level of the server's selective log and view the extracts from the log in the console window:

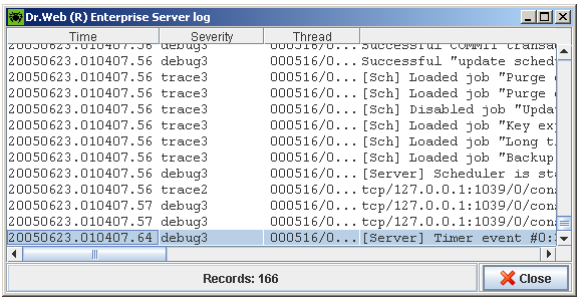
1. In the `Administration` menu of the anti-virus console select the `Show Dr.Web(R) Enterprise Server log` item. A `Select log level` window will open (pic. 39).



Picture 39. Setting the log

2. Mark the radio buttons providing for the necessary log level of the selective log.
3. Press `OK`.

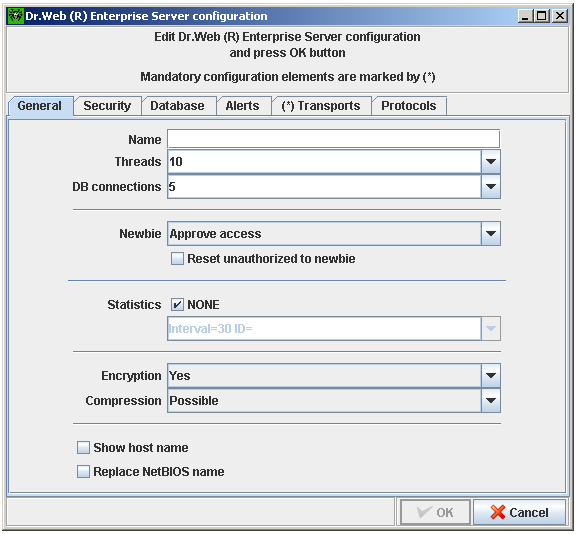
4. A `Dr.Web(R) Enterprise Server log` window with extracts from the log with the specified log level will open (pic. 40).



Picture 40. Server log

6.5.2. Setting the server configuration

To set the configuration parameters of the anti-virus server, select the `Configure Dr.Web(R) Enterprise Server` item in the `Administration` menu of the console. A window for setting the server will open (pic. 41).



Picture 41. Configuring the server (general parameters)

The `Name` parameter in the `General` pane defines the name of the given server (or the cluster of servers); if it is not specified, the name of the computer where the anti-virus server software is installed is used.

The `Threads` and `DB connections` parameters administer the setting of interaction of the server with the OS and the DBAS. Select the necessary value in the dropdown list, or input it manually.

In the `Newbie` dropdown list the link policy for new workstations is specified. This parameter is described in details below.

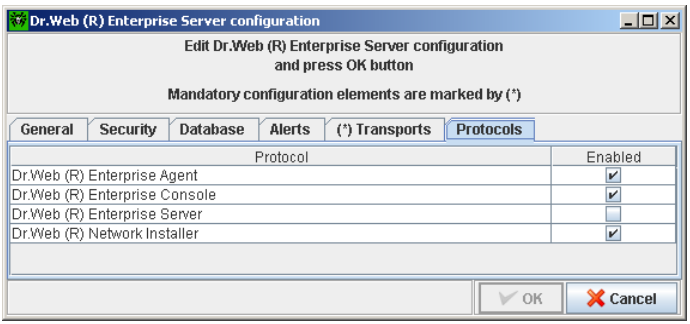
The `Statistics` checkbox instructs whether or not the statistics of operation of the anti-virus server should be sent to the Internet server. If necessary, You can set up the connection parameters at the nearest entry field.

In the `Encryption` and `Compression` dropdown lists the traffic encryption and compression policy between the anti-virus server, the

agents and the consoles is selected. The parameters are described in details below.

In the `Database` pane the DBAS for storage of the centralized log of the complex and for its setting is selected. The parameters are described in details below.

In the `Protocols` pane (pic. 42) the mode of using protocols of interaction of the server with other ES components is specified.



Picture 42. Server configuration (allowed protocols)

By default, the interaction with the anti-virus agents, consoles and agent's installation programs is enabled; the interaction of the server with other ES servers is disabled.

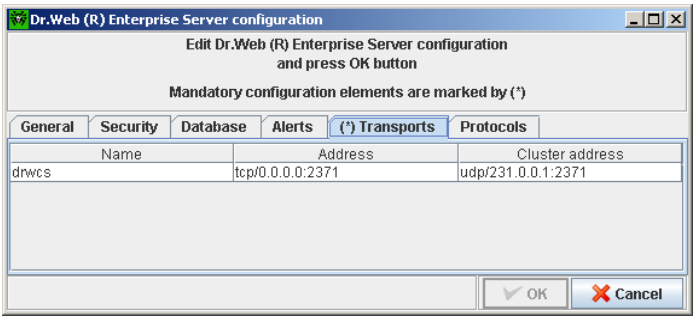
If multiserver network configuration is specified (read p. 6.6), enable this protocol by checking the correspondent box.

The parameters in the `Alerts` pane allow to set up the style of notifications of the anti-virus network's administrators and other employees about virus attacks and other events detected by the complex. These settings are described in detail below.

In the `Alerts` pane the list of events on which the notifications should be sent is specified.

In the `Transports` pane (pic. 43) the parameters of the transportation protocols used by the server are set up. In the

network with multicasting enabled, the components of the program complex configure the transports automatically.

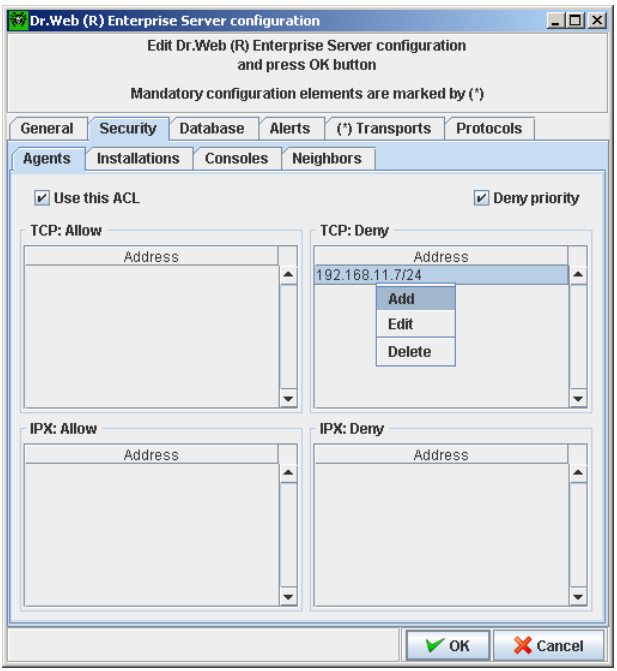


Picture 43. Server configuration (setting transportation protocols)

For each protocol the name of the anti-virus server can be specified in the `Name` field; if no name is specified, the name specified in the `General` pane is used (read above). If the protocol name differs from that specified in the `General` pane, the name from the description of the protocol is used.

If several servers in the cluster mode are used in the anti-virus network (read p. 2.1.1), they should have common settings of the UDP transportation protocol.

In the `Security` pane (pic. Picture 44) the restrictions for network addresses from which the agents, the consoles, the network installations and other ("neighboring") servers will be able to access the given server are set.



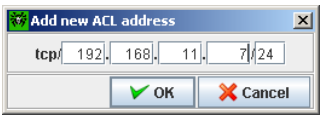
Picture 44. Server configuration (security settings)

On this pane the `Agents`, `Instillations`, `Consoles` and `Neighbors` additional panes are designed to set the restrictions for correspondent types of connections.

To set access restrictions for any type of connection, go to the correspondent pane.

To allow all connections, uncheck the `Use this ACL` box. Check this box to set lists of allowed or denied addresses.

To allow any TCP-address, include it into the `TCP:Allow` list. For this, right click this list and select the `Add` menu item in the dynamic menu. A window for editing the address will open (pic.Picture 45).



Picture 45. Setting the network address

Input the network address and press `OK`.

You can delete addresses from the list and edit the addresses included into the list.

To deny any TCP-address, included into the `TCP:Deny` list.

The addresses not included into any of the lists are allowed or denied depending whether the `Deny priority` box is checked or not: if the box is checked, the addresses not included into any of the lists (or included into both of them) are denied; otherwise, such addresses are allowed.

The restrictions for IPX-addresses are similarly set.

6.5.2.1. New stations connection policy. Approval of connection

To se the connection policy for new workstations, select one of three values in the `Newbie` dropdown list in the `General` pane:

- `Approve access` (this is the default mode, if not changed during the server installation)
- `Deny access`
- `Allow access`

Usually it is recommended to use `Approve access`. The new stations will be put into the list of new (unapproved) stations.

To connect physically the detected workstations:

1. Select the `Unapproved stations` menu item in the `Administration` menu.

2. In the opened Unapproved stations window, select the necessary station and then select the Approve and set Everyone or Approve and set group item in the contextual menu, depending on what group you want to assign for connected workstations (if you want to connect all unapproved stations at once, select one of the items Approve all...)

If the Allow access mode is used, the automatically detected stations are connected without further requests to the administrator.

In the Deny access mode the server does not connect the stations automatically. The administrator should manually create accounts for stations and give access passwords to them.

For this:

1. Select the Create station item in the contextual menu of any element of the network directory. A window for creation of a new workstation will open (pic. 46).

Picture 46. Creation of a new workstation

2. The ID field is filled in automatically. You can edit the ID field, if necessary (it should not contain blanks and should be unique).
3. Insert the station's name into the Name entry field, the password and the confirmation of the password should be inserted into appropriate fields.
4. Make comments, if necessary, in the Description field.

5. Press OK.

6.5.2.2. Using traffic encryption and compression

The program complex allows to encrypt the traffic between the server and workstations (the anti-virus agents), as well as between the server and the consoles. This mode is used to avoid leakage of user keys and other data on the hardware and users of the local network.

The program complex uses the cryptographically strong and convenient tools of encryption and digital signature based upon the concept of public-private keys, which allows to spread keys and to encrypt automatically.

The encryption policy is set separately for each component of the program complex; the settings of other components should be compatible with other settings of the server.

To choose the encryption policy on the server, select one of two variants in the Encryption dropdown list in the General pane:

- Yes — the traffic encryption with all components is obligatory (it is set by default, if the parameter was not modified during the installation)
- Possible — the traffic will be encrypted with those components the settings of which do not prohibit it
- No — encryption is not supported

To coordinate the settings of the encryption policy on the server and other component (the agent or the console) one should remember, that certain combinations of settings are unacceptable and, if selected, it will result in disconnection of the server and the component.

The Table 3 describes what settings provide for encryption between the server and the components (+), when the connection will be non-encrypted (–) and what combinations are unacceptable (Error).

Table 3. Compatibility of settings of the encryption policy on the server and the connected component

Server settings / Components settings	Yes	Possible	No
Yes	+	+	Error
Possible	+	+	-
No	Error	-	-

Encryption of traffic considerably loads the computers which capacities are close to the minimal system requirements for the components installed on them (read p. 3.2). In those cases, when the security considerations do not require the traffic encryption, you can disable this mode. For this, you should switch step by step the server and the components to the Possible mode first, avoiding creation of incompatible pairs - console-server and agent-server. If this rule is broken, it may result in lost of connection with the component and its reinstallation.

By default, the console and the anti-virus agent are installed with the `Possible` encryption setting. This means, that, by default, the traffic will be encrypted, but it can be disabled by editing the settings of the anti-virus server.

Users of the complex version 4.32 and earlier should remember about the change in this setting in version 4.33.

As the traffic between the components (especially between the server and the workstations) can be rather considerable, the program complex provides for compression of this traffic. The setting of the compression policy and the compatibility of settings on different components is the same as that described below for encryption, the only difference is that the default setting for compression is `No`.

By default, the console and the anti-virus agent are installed with the `Possible` compression setting. This combination means that, by default, the traffic will be compressed, but it can be disabled by editing the settings of the server without editing the settings of components.

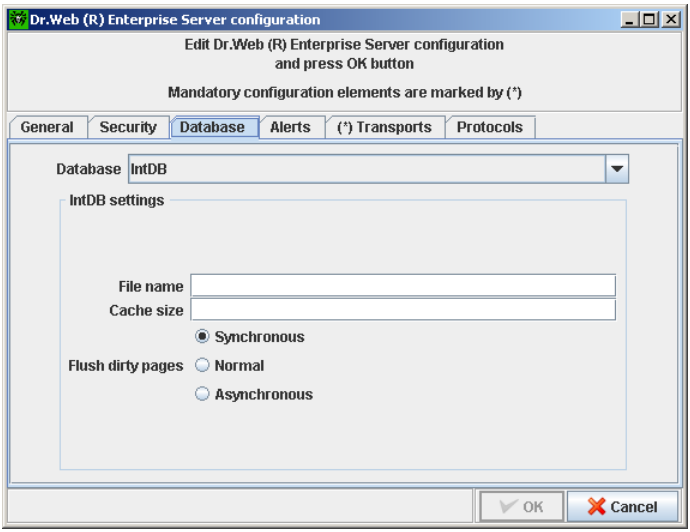
Users of the complex version 4.32 and earlier should remember about this change in setting in version 4.33.

The compression mode enabled reduces the traffic, but considerably increases the load over the computers.

6.5.2.3. Setting the operation with database

To specify parameters of the centralized logging of the anti-virus network, go to the `Database` pane (pic. 47) and select the type of the base in the `Database` dropdown list:

- `IntDB` – internal DB (component of the anti-virus server)
- `ODBC` (for servers running under Windows) or `PostgreSQL` (for servers operated by Unix-based systems) – external DB



Picture 47. Server configuration (setting the DBAS)

For the internal DB, if necessary, input the full path to the database file into the `Path` entry field and specify the cashe size and the data log mode.

The parameters for the external DB are described in details in Appendix A.

By default, the internal DBAS is specified. This mode considerably increases the load over the server. It is recommended to use the external DBSA in large networks.

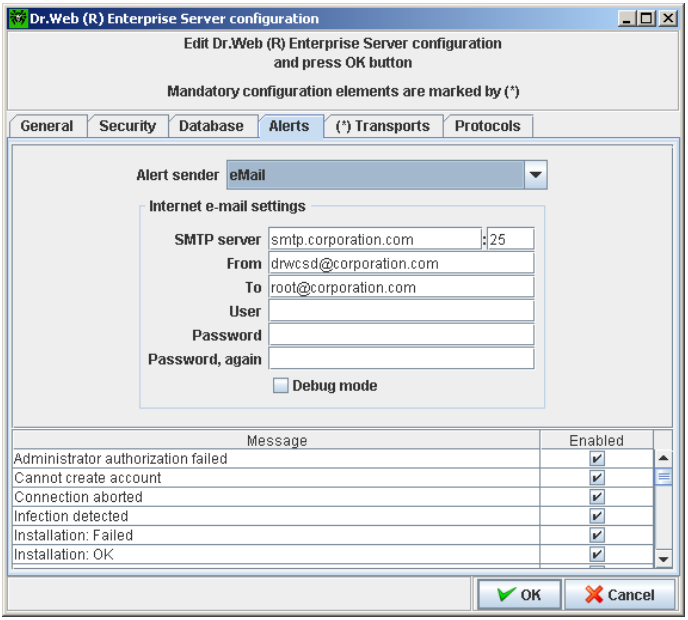
If external DBAS by Oracle is used, the ODBC-driver, which is supplied with this DBAS should be installed. It is strongly recommended not to use the ODBC-driver by Oracle supplied by Microsoft.

If several servers are used in the cluster mode in the anti-virus network (read p. 2.1.1), all servers are set up to use common external DB.

6.5.2.4. Setting alerts

To set the mode of sending alerts about the events connected with the operation of the program complex, go to the `Alerts` pane (pic. 48) and select the necessary mode of alerts in the `Alert sender` dropdown list:

- `None` — do not send messages (default mode)
- `eMail` — send via e-mail
- `Windows network message` — send using Windows Messenger (for servers under Windows only)



Picture 48. Server configuration (setting alerts)

To send notifications via e-mail specify, if necessary, the address of the SMTP-server, the sender's address and the recipient's address, user name and password of SMTP-server.

For messages in the Windows network, specify the list of names of computers – recipients of messages.

In the bottom part of the pane, check the boxes against the events on which the notifications should be sent.

The text of the message is determined by the template of the message. The templates of messages are stored in the `var/templates` subdirectory of the server installation directory. You can edit the template for the text of the message sent at a definite event.

When a message is generated, the program complex replaces the variables of the template (in braces) with the definite text, which depends upon the current parameters of the complex. The available variables are listed in Appendix C.

We strongly recommend to use the console templates editor for editing the templates (read below).

If you use the external editor for editing templates, remember, that the text of the templates should be obligatory UTF-8 encoded.

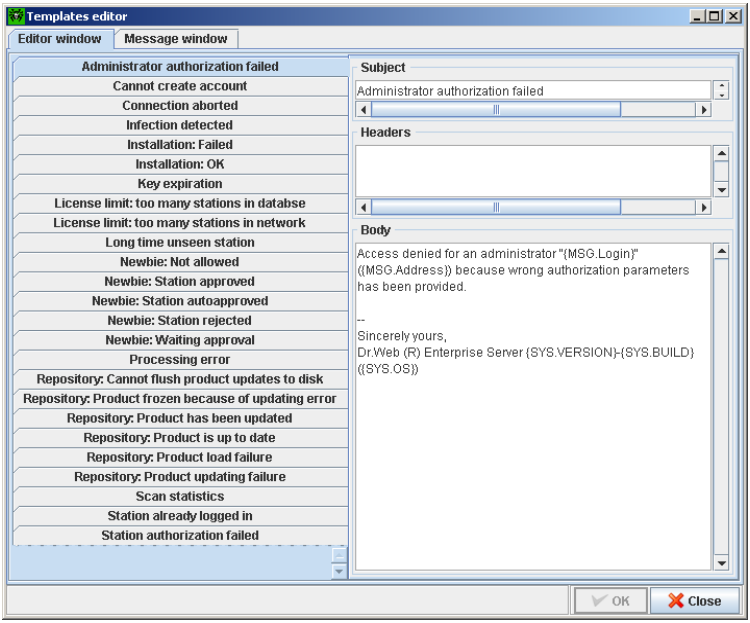
Below goes the template's example for the "Infection detected " event (the template's name is `Infection.template`):

```
; $Id: Infection.template,v 1.4 2005/05/25 15:11:23 john Exp $
; Local Variables:
; coding: iso-8859-1
; End:
Infection
Look ahead! Virus attack at {GEN.StationName} has been
detected!


The {MSG.Component} from {GEN.StationName}
({GEN.StationAddress}) running by {MSG.RunBy} reported
{MSG.ServerTime:10} at {MSG.ServerTime:11:12} that object
"{MSG.ObjectName}" owned by {MSG.ObjectOwner} is
{MSG.InfectionType} {MSG.Virus} virus and was {MSG.Action}.


--
Sincerely yours,
Dr.Web (R) Enterprise Server {SYS.VERSION}-{SYS.BUILD}
({SYS.OS})
```

For editing the templates, the console templates editor can be used. For this, select the `Edit templates` item in the `Administration` menu. A window for editing templates will open (pic. 49).



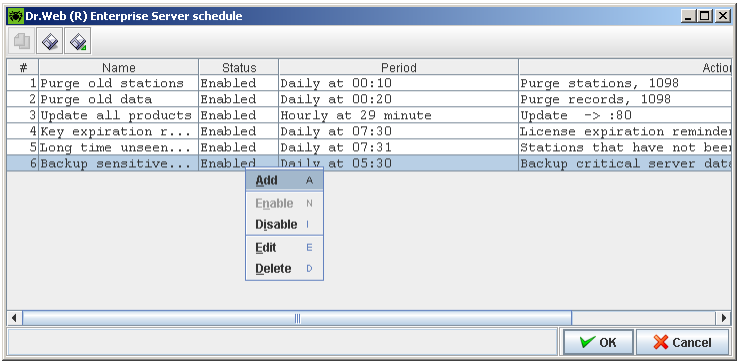
Picture 49. Editor of templates

To edit any template, select it in the list in the left part of the window. In the `Subject` entry field you can edit the subject of the message. In the `Headers` entry field additional headers of the e-mail message are specified. In the `Body` entry field the message text is specified.

6.5.3. Setting the server schedule

To schedule the tasks for the server:

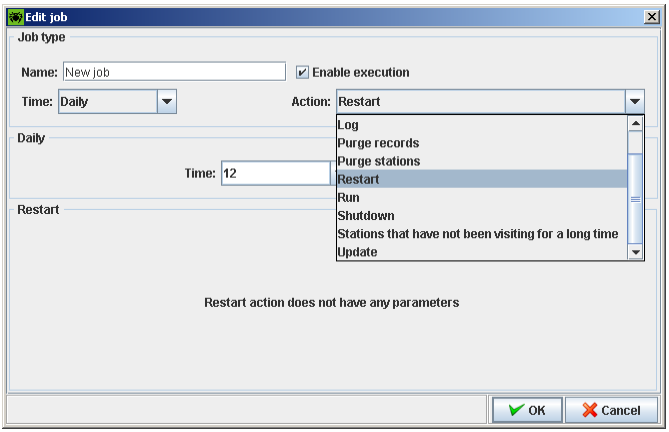
1. In the `Administration` menu select the `DrWeb(R) Enterprise Server schedule` item. A window for setting the list of tasks for the server will open (pic. 50).



Picture 50. Server schedule

2. To remove a task from the list, select it in the list and then select the `Delete` item in the contextual menu.
3. To edit parameters of the task, select it in the list and then select the `Edit` item in the contextual menu. A window for editing parameters will open.
4. To add new task onto the list, select the `Add` item in the contextual menu. A window for editing the task will open. You can also disable this task, or enable the task disabled before. This action is described in details below.
5. To save the changes in settings, press `OK`. To reject changes, press `Cancel`.

When new task is created or the existing task is edited, a window for inputting the parameters is opened (pic. 51, an example for creation of a new task is shown).



Picture 51. Editor of tasks of the server

To edit the parameters of the task:

1. Input the name of the task it will be displayed in the schedule into the `Name` entry field.
2. Select the type of the task in the `Action` dropdown list. The bottom part of the window with the parameters of this type of the task will change its outlook (below the parameters of the task for different types are described).
3. Select the time intervals the task is to be launched and set the time accordingly in the `Time` dropdown list (this action is similar to that for setting the time in the schedule of the workstation, read above p. 6.2.4.2).
4. Press `OK`.

The `Shutdown` and `Restart` tasks have no parameters.

To enable the `Run` task, specify the path to the executable file of the server in the `Path` field, specify the launch command line parameters in the `Arguments` field.

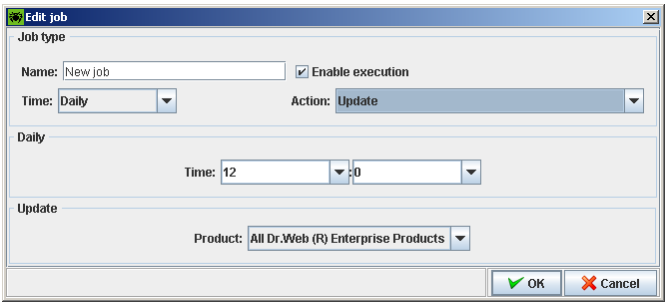
To enable the `Log` task, specify the text of the message which is logged.

To enable the `Purge records` and `Purge stations` tasks, specify the period on the expiry of which the records or stations are considered outdated.

To enable the `Stations that have not been visiting for a long time`task, specify the period on the expiry of which the station is considered as not visiting the server for a long time.

The `Backup critical server data` task is designed to create the backup copy of the server critical data (the database, the server license key file, the public encryption key). You should specify the path to the directory where this data will be saved (the empty path means the default path) and maximum quantity of backup copies (the `0` value means this restriction is canceled). Read more in Appendix G5.9.

If the `Update` task is selected, the window looks as below in pic. 52.



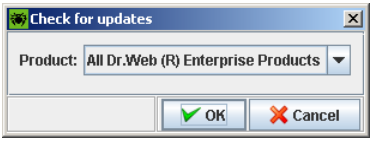
Picture 52. Setting the Update task

In the Product dropdown list select the product updated by this task:

- All Dr.Web® Enterprise Products
- Dr.Web® Enterprise Agent
- Dr.Web® Enterprise Server
- Dr.Web® Enterprise Updater

6.5.4. Checking for updates of the software and the virus bases

To check for updates of any Dr.Web ES family product on the updating server, select the Check for updates item in the Administration menu. A Check for updates window will open (pic. 53).



Picture 53. Check for updates

The checks of updates are set similarly to the receipt of updates (read above p. 6.5.3).

6.5.5. Administrating the server repository

6.5.5.1. Introduction

The *repository* of the anti-virus server is designed for receipt and propagation of updates of the ES components.

For this, the repository operates by the set of files (p*roducts*). Each product resides in the separate subdirectory of the repository directory located in the var directory, which during the installation with the default settings is the subdirectory of the server root

directory (read more in Appendix G). The functioning of the repository and the administration of it are made for each product independently.

To administrate the updating the repository uses the idea of *revision* of a product. The revision is a definite determination for the definite moment of time of the state of product files (including file names and checksums) and has its unique number. The repository synchronizes the revisions of products as follows:

- (a) to the anti-virus server from the product's updating site (via HTTP)
- (b) between different anti-virus servers in multiserver configuration
- (c) from the anti-virus server to workstations

The repository allows a user to set up the following parameters:

- List of updating sites in (a) operations.
- Restriction in set of product files requiring synchronization of type (a) (thus a user is enabled to track only necessary changes of certain files or categories of files)
- restriction of parts of the product, requiring synchronization of type (c) (a user can choose what should be installed on the workstation)
- control of shift to new revisions (independent testing of products before installation is possible)
- adding own components to products
- independent creation of new products for which the synchronization will be made too

At present, the distribution includes the following products:

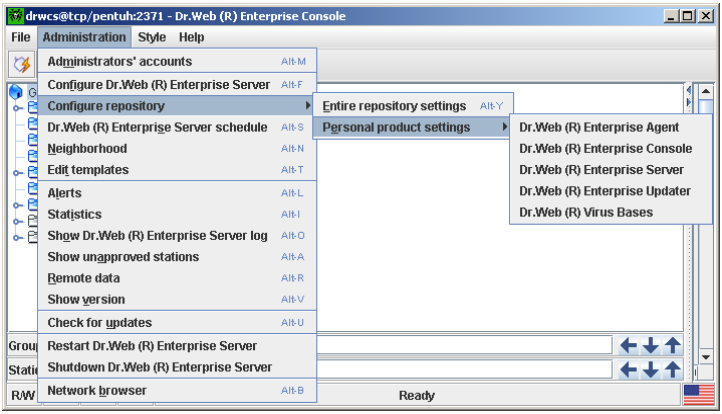
- Anti-virus server
- anti-virus console

- Anti-virus agent (the software of the agent and the anti-virus software of the workstation)
- Updater (the utility for updating the files of the anti-virus agent)
- Virus bases

Read more about the repository in Appendix E.

You can configure the repository for every product or on the whole. The setting of configuration for separate products is described below. The general configuration (simple editor of the repository configuration) is described in p. 6.5.5.7.

To set up the server repository, select the `Configure repository` item in the `Administration` menu, in the opened submenu select the `Personal product settings` item, and in the opened submenu select the product (pic. 54).

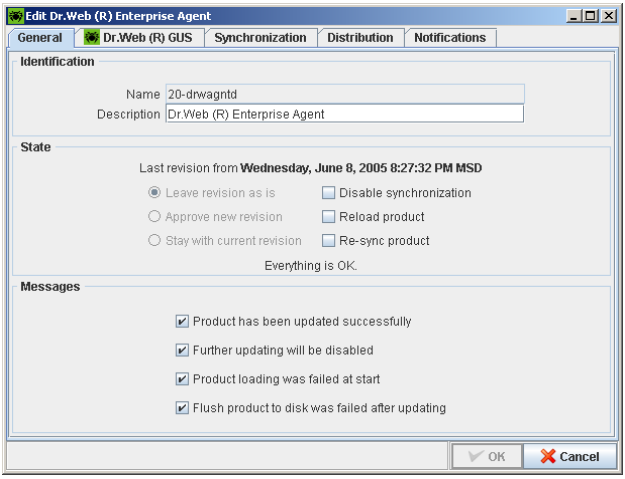


Picture 54. Configuring the repository (selection of a product)

Further example describes the actions for the anti-virus agent.

6.5.5.2. General parameters of the repository

A window for setting up the repository for the selected product will open (pic. 55) in the `General` pane.



Picture 55. General settings of the repository

In the `Description` entry field the names of products (the names under which the product can be seen in the console's interface) are displayed. You can edit this field, if necessary.

You can disable further product's synchronization. For this, check the necessary box.

To reload the product, (for example, to clear the error), check the `Reload product` box.

If the product's synchronization was interrupted (read below p. 6.5.5.4), the group of radio buttons in the left part of the pane becomes accessible. You can specify the repository's reaction to incomplete synchronization:

- `Leave revision as is` — the synchronization is prohibited

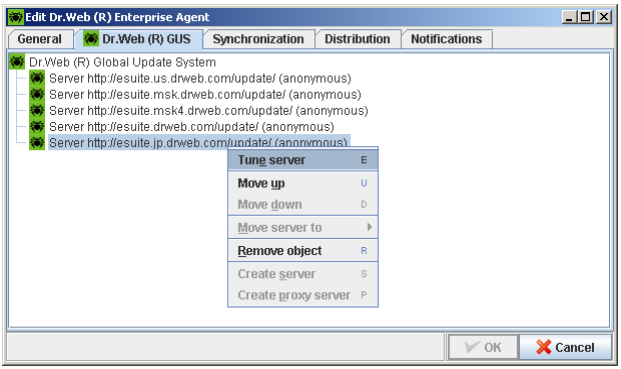
- `Approve new revision` – allows the transfer to new revision (for this the settings which provoked the termination of the synchronization should be edited, read below in p. 6.5.5.4)
- `Rollback to previous revision` – restoration of the previous revision

You can also specify the list of notifications sent by the server when administrated by the repository. For this, check (save) the boxes against the names of events the notifications should be sent about. Additional setting of notifications is made in the `Notifications` pane, read p. 6.5.5.6.

6.5.5.3. Setting the Dr.Web® Global Updating System

Go to the `Dr.Web(R) GUS` pane (pic. 56).

Users upgrading the version 4.32 or earlier should remember about the change in the URL format.

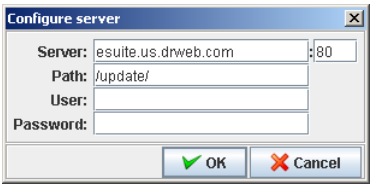


Picture 56. Setting access to GUS

In this pane the hierarchy list of accessible servers of the updating system is displayed. You can:

- remove the server from the list. For this, select the `Remove object` item in the object's contextual menu
- move up or down the server in the list (this will affect the queue of the call). For this, select the correspondent item in the object's contextual menu
- Add a server into the list. For this, select `Create server` or `Create proxy server` (read below about proxy) in the contextual menu of the root element of the hierarchy list
- Set the server address and user authorization parameters. For this, select the `Tune server` item in the contextual menu

When setting or adding the server, a window for editing the updating server settings is opened (pic. 57).



Picture 57. Setting the updating server

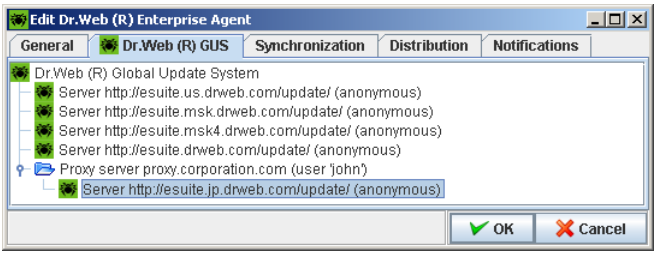
Fill in the `Server` and the `Path` entry fields with the data on server address, the port and the path on the server; fill in the `User` and the `Password` entry fields with the user name and the password on the updating server (if authorization on the server is not required, leave these fields empty). To save the changes in settings, press `OK`.

If a proxy server is used to access all or the created updating servers, add proxy server into the hierarchy list and ascribe the updating servers to the proxy server through which they will be accessed. For

this, add the proxy server into the hierarchy list and set it up (the proxy server is set in the same way as the updating server, see pic. 58).

Picture 58. Setting proxy server

Now choose the updating server which will be ascribed to this proxy server, and then select the `Move server to` item in its contextual menu. A submenu with the list of accessible proxy servers will open. Select the necessary in the list. The hierarchy list will look as below in pic. 59.

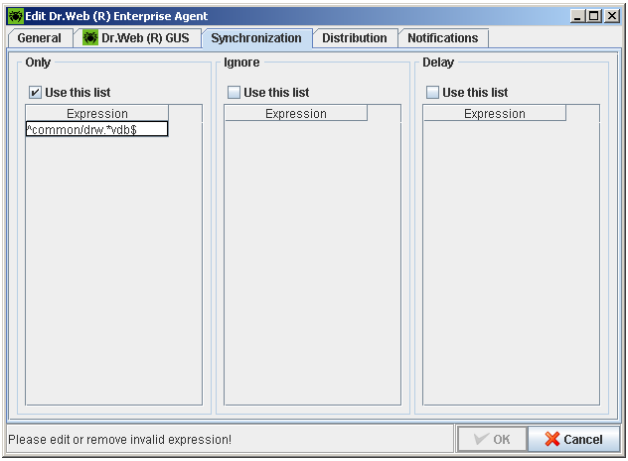


Picture 59. Ascribing the server to the proxy server

If the updating server should be disconnected from the proxy server, select the `Move server to` item in the contextual menu and then the name of the root element of the list.

6.5.5.4. Setting synchronization

Go to the `Synchronization` pane (pic. 60).



Picture 60. Setting the synchronization

In this pane, up to three lists of regular expressions which define the set of synchronized files can be specified. Each list can be enabled or disabled by the correspondent checkbox.

The `Only` list specifies the set of files to be synchronized. No file outside this set will be synchronized.

The `Ignore` list explicitly specifies the set of files which will not be synchronized.

The `Delay` list specifies the set of file names, at the synchronization attempt of which the process of synchronization will be terminated. Further actions in such cases are set in the `General` pane (read above in p. 6.5.5.2).

If several lists are enabled, they are used as follows:

- the files set by the `Only` list are picked out first
- from picked out files (or all files, if `Only` is enabled) the files set by the `Ignore` list are deleted
- the `Delay` list is used for the rest of files

To edit any list, enable it first. For this, check the `Use this list` box. Then select the `Add` item in the contextual menu. The blank of regular expression will be added into the list. Double click it and edit the expression.

To delete the element, select the `Delete` item in the contextual menu of this element.

The syntax and the values of the regular expressions of this list are described in details in Appendix E.

6.5.5.5. Setting propagation

In the `Propagation` pane the set of files to be propagated to workstations is specified. For this, the `Only` and the `Ignore` lists are used. Their setting and application is similar to the list of files' synchronization.

6.5.5.6. Setting notifications

In the `Notifications` pane additional setting of notifications on the events connected with the synchronization are specified. The main setting (the permission to send notifications of different types) is specified in the `General` pane (read p. 6.5.5.2). In this pane you can specify the set of files the updating of which will provoke sending of messages of the `Product has been updated successfully` type.

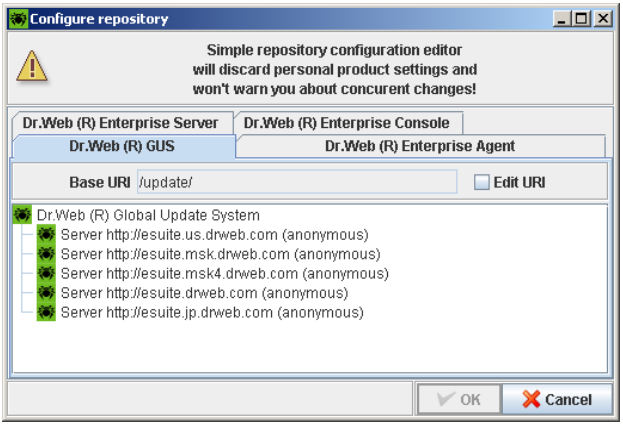
To specify the sets of files the `Only` and the `Ignore` lists are used. Their setting and application is similar to the list of files' synchronization.

6.5.5.7. Simple editor of the configuration of the repository

The simple repository configuration editor allows to specify the repository configuration parameters common for all products.

The settings specified by the simple editor cancel the settings for separate products.

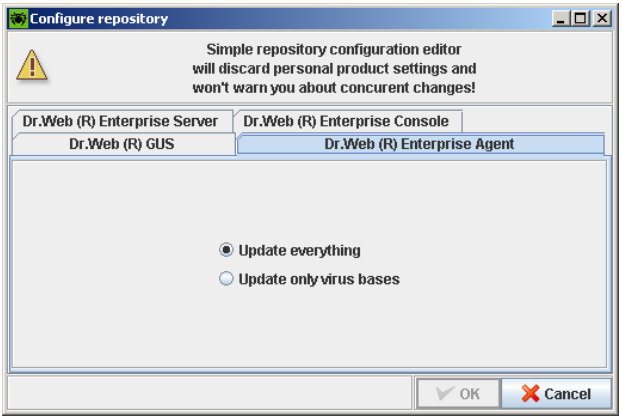
To edit the configuration of the repository for all products at once, select the `Configure repository` item in the `Administration` menu; in the opened submenu select the `Entire repository settings` item. A window of the repository simple editor in the `Dr.Web(R) GUS` pane will open (pic. 61).



Picture 61. Simple repository editor

Setting of parameters of the Dr.Web® Global Updating System is similar to the setting for separate objects, read above in p. 6.5.5.3. If non-standard URL on the updating server should be set, check the `Edit URL` box and edit the entry in the `Base URL` entry field.

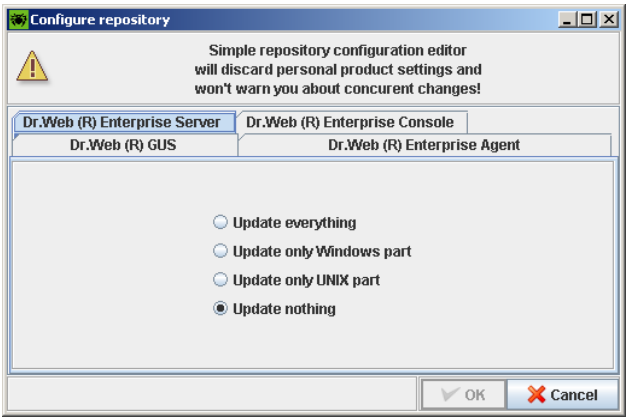
Go to the `Dr.Web(R) Enterprise Agent` pane (pic. 62)



Picture 62. Updating parameters of the agent

In the group of radio buttons specify whether all files of the workstation will be updated or the virus bases only.

Go to the `Dr.Web(R) Enterprise Server` pane (pic. 63).



Picture 63. Server updating parameters

In the group of radio buttons specify what files (for Windows, for UNIX, for both of them or none) should be updated.

The console updating settings are similar to those set for the server in the Dr.Web(R) Enterprise Console pane.

6.5.6. Server statistics

To view the server statistics, select the Statistics item in the Administration menu. A Dr.Web(R) Enterprise Server Log window in the Counters pane will open.

In this pane the following data is displayed in numerical form:

- Usage of system resources
- network traffic
- activity of clients (total quantity, active at the moment, information about newbies and installers, remote servers data)
- usage of the database
- usage of the file cache
- external interaction (messages, web-statistics, operation of the repository)

The CPU usage in the kernel mode and the number of disk write operations can be displayed as graphs in the Graphs pane. To turn on the graph representation of a counter, click the counter name. If a counter can be displayed as a graph, it is thin-underlined when the cursor is pointing at it. Counters that are displayed as graphs in the Graphs pane are thick-underlined.

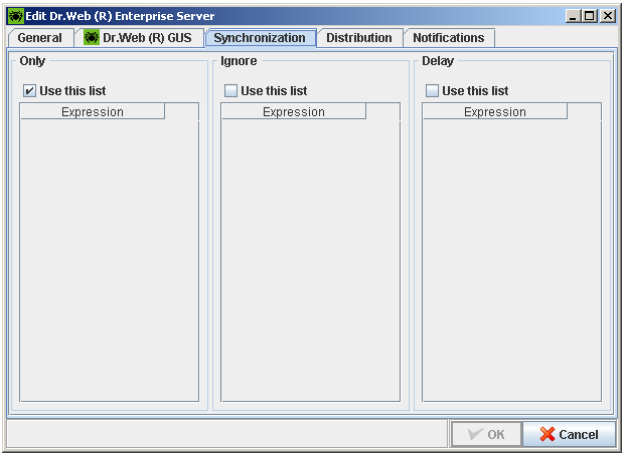
6.5.7. Upgrading the server software till version 4.33

If the program complex version 4.32 or higher is installed and stably functions in your computer, you can upgrade the software till version 4.33 by using the tools of the repository. Upgrade of the agent's software is made automatically, without a user's interference. The server software upgrade is described below. The name of the menu

items and the outlook of windows may somewhat differ depending on the upgraded version.

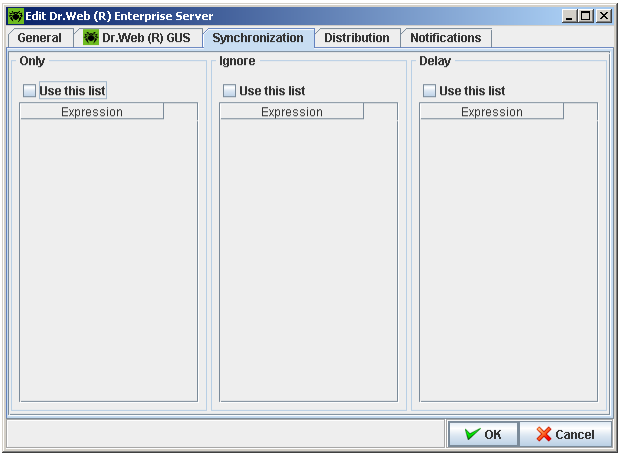
To upgrade the server software:

1. Disable usage of the communication protocols with the anti-virus agent and the server installer. For this, select the Administration item in the Configure Dr.Web(R) Enterprise Server menu. In the opened submenu go to the Protocols pane and uncheck the Dr.Web(R) Enterprise Agent and Dr.Web(R) Network Installer checkboxes. Press OK. A dialog requesting a computer reboot will open. Reject rebooting.
2. Terminate the server.
3. Download repository-432.zip and repository-433.zip file archives from the web-site with the distribution kit of the program complex.
4. Delete the content of the var\repository directory (the directory itself should not be deleted).
5. Unpack repository-432.zip and place the files and directories of this archive into the var\repository server directory.
6. Run the server.
7. In the Administration menu select the Configure repository submenu; select the Personal product settings item and then the Dr.Web(R) Enterprise Server item. A Dr.Web(R) Enterprise Server window will open. Go to the Synchronization pane (pic. 64).



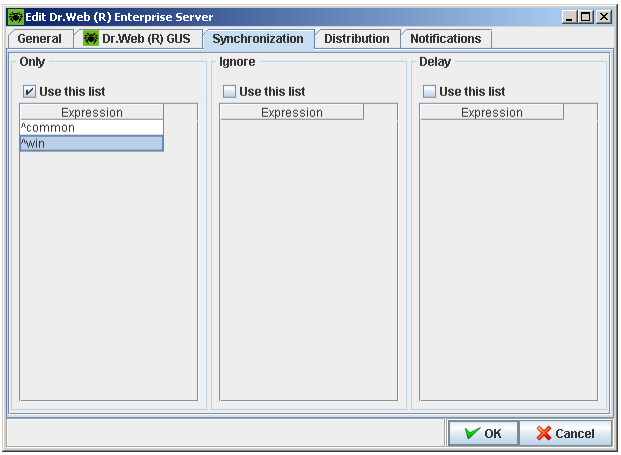
Picture 64. Server upgrade is disabled

8. The settings specified in this pane disable the server upgrade. If you want to receive updates for all platforms, deselect the `Use this list` checkbox in the `Only` field (pic. 65).



Picture 65. The updating for all platforms is set

If you want to receive updates for the Windows server only, check the `Use this list` box in the `Only` field, and then right click the `Expression` list (originally, it is empty) and select the `Add expression` tem in the contextual menu. Double click the line which will appear and edit it. Repeat this action for the next expression. As the result, the list will look as in pic. 66.



Picture 66. Updating for Windows is set

The first line `^common` sets the receipt of the part common for all platforms, the second line `^win` — specific for Windows platform.

If you want to receive updates for Linux, the list will look as follows:

```
^common
^unix
^unix-Linux
```

For FreeBSD the last line will be `^unix-FreeBSD` and for Solaris — `^unix-SunOS`.

Press OK.

9. Similar to the previous paragraph, specify the updating policy for the console. For this, select the Configure repository submenu in the Administration menu, select the Personal product settings item and then select Dr.Web(R) Enterprise Console. A Dr.Web(R) Enterprise Console window will open. Go to the Synchronization pane as described above. If you want to receive updates for all platforms, uncheck the Use this list box in the Only field. If you want to receive updates of the console for Windows platform only, check the Use this list box in the Only field and then right click the Expression list (initially, it is empty) and select the Add expression item in the contextual menu. Double click the line which will appear and edit it. Repeat this action for the next expression. As the result, the list will look as follows

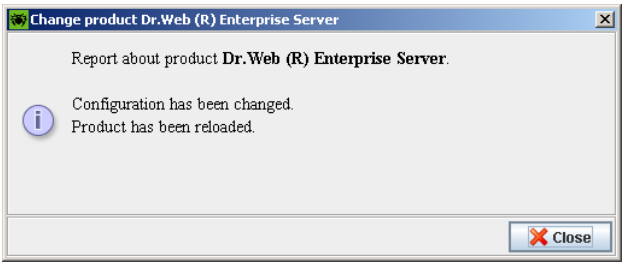
   ```
   ^common
   ^win
   ```

   If you want to receive updates for UNIX, the list will look as follows:

   ```
   ^common
   ^unix
   ```

10. If you want to connect to the Dr.Web® GUS via a proxy server, select the Configure repository submenu in the Administration menu, then select the Personal product settings item and set the proxy server address for each product, specify a user name and a password, if necessary, as it is described in p.6.5.5.3 of the "Dr.Web® Anti-virus. Corporate network protection" Administrator manual.

11. A window notifying on progress in changes of the product will open. In some time a confirmation that a product has changed will be generated (pic. 67).



Picture 67. Change of product completed

12. In the `Administration` menu select the `Check for updates` item. By default, it is offered to check for updates for all products. Press `OK`.
13. Terminate the server (`Administration` menu, `Shutdown Dr.Web(R) Enterprise Server` item). The console will report it is disconnected from the server.
14. Go to the server installation directory and then go to the `var\repository\20-drwcs\common\Installer` subdirectory; copy the `drwinst.exe` file by standard OS tools to the `Installer` subdirectory of the server installation directory (the addresses are in the format for Windows). Delete all files with the `dll` and `dws` extensions in the directory where the file was moved to.
15. Replace the console files (below goes the example for Windows). For this, delete all files and subdirectories from the `Console` server directory. Copy all files and subdirectories from the `var\repository\20-drwconsole\win` directory. Copy the `var\repository\20-drwconsole\common\jars` subdirectory to the

Console\lib directory. Rename the copied Console\lib\jars directory into the Console\lib\DrWeb directory. To launch the console use the Console\bin\drwconsole.exe instruction.

16. Delete the templates subdirectory of the installation directory and create the subdirectory in the var directory with the same name; copy files with templates from the var\repository\20-drwcs\common\templates subdirectory into the created var\templates directory. If necessary, you can copy also subdirectories containing templates in different languages. If you want to use the templates in the language different from the default one, copy all files from the directory with templates in this language into the root of the var\templates directory. Remember, that if you have changed (edited) the templates, you cannot save the edited templates of the old version – you should copy files of templates over the new version and then edit them accordingly.
17. For Windows platform, go to the win-nt subdirectory and copy its content (files and subdirectories) to the installation directory. For Linux platform, go to the unix-Linux-libc2.3 subdirectory and copy all files and subdirectories of the installation directory and then enable execution of files from bin with the instruction
    ```
    chmod 755 ../../../bin/*
    ```
18. Update the database with the following instruction
    ```
    bin\drwcsd -var-root=.\var upgradedb
            var\repository\20-drwcs\common\update-db
    ```
19. Unpack repository-433.zip and replace the files and subdirectories of the var\repository directory with the files of the same name included into this archive.

20. Run the server.
21. If you connect to the Dr.Web® GUS via a proxy server, select the `Configure repository` submenu in the `Administration` menu, and then select the `Entire repository settings` item. Specify the proxy server address, user name and password, as it is described in p.6.5.5.7 of the "Dr.Web® Anti-virus. Corporate network protection" Administrator manual.
22. In the `Administration` menu select the `Check for updates` item. By default, it is offered to check for updates for all products. Press `OK`.
23. When a message on a successful updating is received, enable usage of communication protocols with the anti-virus agent and the network installer. For this, select the `Configure Dr.Web(R) Enterprise Server` item in the `Administration` menu. In the opened window, go to the `Protocols` pane and check the `Dr.Web(R) Enterprise Agent` and the `Dr.Web(R) Network Installer` boxes. Press `OK`. A dialog requesting a computer reboot will open. Approve rebooting.

If the software of several connected servers should be updated (read p. 6.6), these actions are made firstly on the server which receives updates from GUS, and at the first procedure step the `Dr.Web(R) Enterprise Server` protocol is also disabled. It is enabled on the last step.

When the described procedure is completed, the software is updated on servers receiving updates from the above mentioned server as described in this paragraph (the interserver interaction protocol is not disabled on them).

6.5.8. Receipt of alerts

By default, when a message is received from the server a `Notifications` window opens. You can also open this window any time. For this, select the `Alerts` item in the `Administration` menu. A list with subjects of alerts will be displayed in the window. To view the entire text of a message, select it in the list and then select the `Show` item in the contextual menu.

To delete a message, select the `Delete` item in the contextual menu.

To delete all messages select the `Clear` item in the contextual menu.

You can disable automatic opening of this window. For this, check the `Do not disturb` box in the bottom left corner of the window.

6.5.9. Updating the server not connected to the internet

If the anti-virus server is not connected to the Internet (it resides in the "demilitarized zone"), to receive upgrades of the anti-virus software the following sequence of actions is applied:

1. Install the anti-virus server software on a computer connected to the Internet as described in p. 3.3.
2. Terminate this server.
3. Upgrade the anti-virus software on this server by using the `drwcsd syncrepository` instruction.
4. Copy the content of the `var/repository` directory of this server to the movable carrier.
5. Copy this data from the removable carrier to the `var/repository` directory of the main (working) server.

6. Run the `drwcsd rerepository` instruction on the working server (the server can either be running or be terminated).

6.6. Peculiarities of a network with several anti-virus servers

The Dr.Web® ES program complex allows to build the anti-virus network with several anti-virus servers. In such network each workstation is ascribed to one definite server, which allows to distribute load between them.

The connections between the servers can have the hierarchy structure, which allows to optimally distribute the load over the servers taking into account the topology, capacity and reliability of your anti-virus network.

To exchange information between the servers (updates of the complex' files and information about operation of servers and workstations connected to them) a special *interserver synchronization protocol* is used.

The efficient transfer of updates is the most significant feature of this protocol:

- The updates are distributed immediately after they are received
- scheduling of updates on the server becomes unnecessary (except for those servers which receive updates from the Dr.Web® GUS servers via HTTP)

There is an option to receive updates from the Dr.Web® GUS servers using the interserver synchronization protocol. To enable this option and to coordinate the settings, contact Technical support service of Doctor Web, Ltd.

6.6.1. Building a network with several servers

The architecture of the anti-virus network in which several servers manage the same workstations (cluster of servers) is not described in present Manual.

Several servers can be installed in the local network. And each anti-virus agent connects to one of servers; each server with the connected anti-virus workstations functions as a separate anti-virus network, as it is described in previous chapters.

The program complex allows to integrate such anti-virus networks by transferring the data between the anti-virus servers.

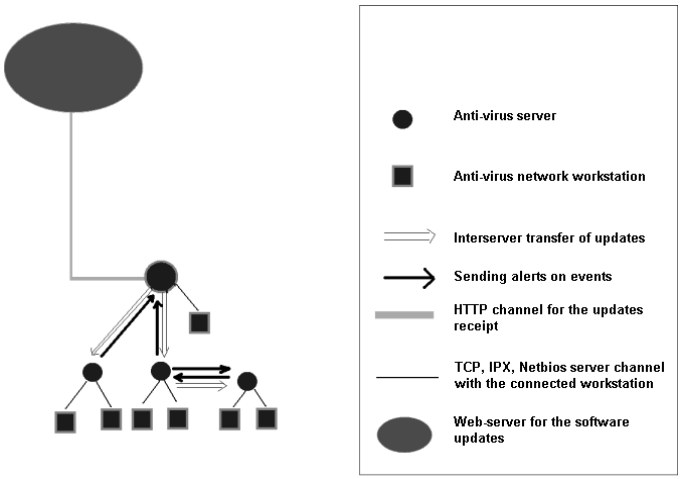
A server can send to another server:

- software updates. But only one of them will receive updates from the Dr.Web GUS servers
- information on virus events, statistics, etc.

The program complex provides for two types of connections between the servers:

- the *parent-child* type of connection, when the principle transfers updates to the subordinate and receives information about events
- connection between the peer, when the data transfer directions are set up individually

In pic. 68 the example of the multiserver structure is presented.



Picture 68. Multiserver structure

Here are some of advantages of the multiserver anti-virus network:

- receipt of updates from the Dr.Web GUS servers through one anti-virus server and their subsequent distribution in the local network to other servers directly or through intermediates
- option of distribution of workstations to several servers and decrease of load for each of them
- combination of data from several servers on one server, the option of its consolidated receipt in the console session on this server

The program complex monitors and is able to avoid cyclic data flows.

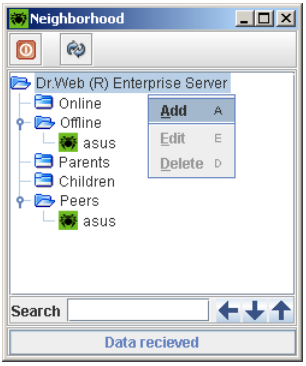
6.6.2. Setting connections between the servers of the anti-virus network

To use the complex in the multiserver mode, you should set up connections between these servers.

It is advisable to make a plan and to draw the structure of the anti-virus network first. There all supposed data flows should be defined and the decision what connections will be of the "between the peer" type, and what of them will be of the "parent-child" type should be taken. Then, for each server included into the network the connection with any "*neighboring*" server (i.e. that which is connected by at least one dataflow) should be set up.

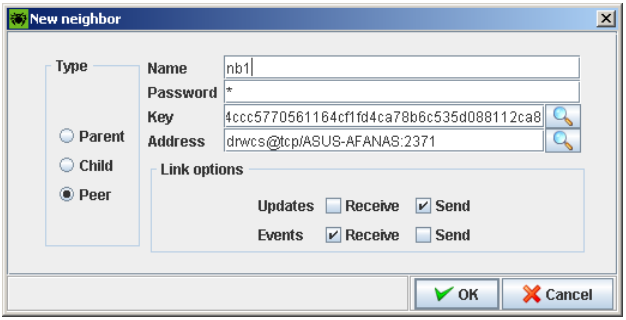
To configure the neighbors of the server:

1. Select the `Configure Dr.Web(R) Enterprise Server` item in the `Administration` menu. In the opened window for configuring the server go to the `Protocols` pane and check the `Dr.Web(R) Enterprise Server` box (read p. 6.5.2).
2. Select the `Neighborhood` item in the `Administration` menu. A window with the hierarchy list of servers of the local network "neighboring" with the given server will open (pic. 69).



Picture 69. Directory of "neighboring" servers

3. To add a server into this list, select the `Add` item in the contextual menu of any element. A window describing connections between the current and the added server will open (pic. 70).

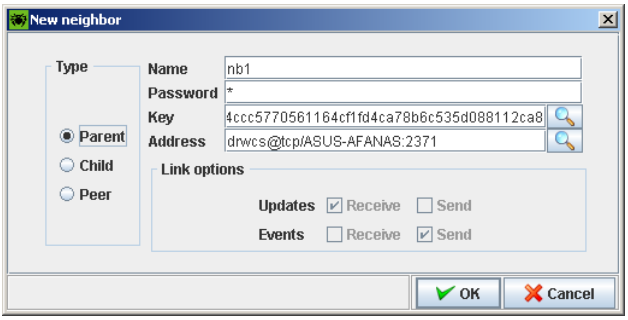


Picture 70. Adding a peer server

4. In the `Type` group of radio buttons select the necessary type of connection: `Peer`, if the connection with the peer server is established; `Parent`, if the "neighboring" server is a principal server and the current is the subordinate, and `Child`, if the connection with the subordinate server is established (and if the current server is the principle server)

5. If `Parent` is chosen, a window will look as in pic. 70.
   - Specify an arbitrary password in the `Password` entry field to access the neighboring server. The password should be the same for all the servers
   - Input the address of the neighboring server into the `Address` entry field
   - Press  on the right of the `Key` field and select a file with the public key from the neighboring server in the file system
   - Leave the `Name` field unchanged.
   - In the `Link options` area check the boxes against the approved connections from the neighboring server to the current server

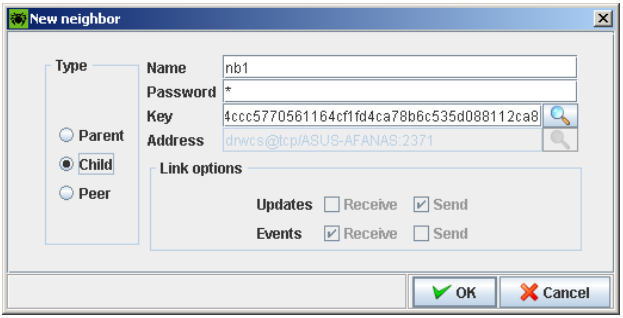
   If `Parent` is chosen, the window will look as in pic. 71.



Picture 71. Adding the parent server

In this case the connection parameters cannot be modified and are automatically installed in the "receive updates from the neighboring server and send notifications to it " mode.

If `Child` is chosen, the window will look as in pic. 72.



Picture 72. Adding a child server

In this variant, in contrast to the description of the connections with the parent server, the neighboring server address should not be specified.

6. When the parameters for the neighboring server are specified, press OK.

6.6.3. Using the anti-virus network with several servers

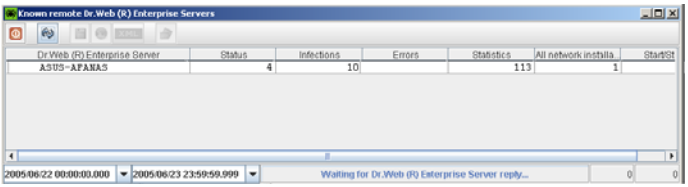
The peculiarity of the multiserver network is that the updates from the Dr.Web GUS servers can be received through some of anti-virus servers (as a rule, one or several parent servers) and the schedule for update should be set on these servers only (read p. 6.5.3). A server, which received the updates from the Dr.Web GUS servers or another server sends them immediately to all servers where such option is enabled (to all connected child servers and to those peer servers for which the setting to receive updates is specified explicitly).

The program complex automatically monitors the situations when, due to the imperfective planning of the network topology or incorrect setting of servers, the update already received from another updating source is sent again to one and the same server and the updating is not made again.

The administrator can receive the consolidate data about the most important virus events in the network segments linked with any server through intersever links (for example, in the "one is parent, the other are children" configuration described above such data is consolidated on the parent server).

To view the information on virus events on all servers linked to the current server:

1. Select the `Remote servers` item in the `Administration` menu. A window with accessible servers will open (with no data loaded).
2. Press , to load data into the table. The window will look as in pic. 73.



Picture 73. Remote servers data

3. Each line contains data on the total number of status entries available on the server (the `Status` column), on detected infections (the `Infections` column), on scanning errors (the `Errors` column) and the statistics (the `Statistics`

column), on network installations (the `All network installations` column), on launch and termination of tasks (the `Start/Stop` column). To view any line of the summary statistics of anti-viruses on the servers in more suitable form, select it in the table and press  (or double click the necessary line). A window with the detailed data of this line will open.

If several lines are selected in the table, the detailed data on each of them will be displayed in the separate window.

4. To save the table for printing or future processing, press  (to save it in the CSV format), or  (to save it in the HTML format), or  (to save it in the XML format).
5. To open the summary window with information on statuses, detected infections, scanning errors, network installations, launches and terminations of tasks, as well as statistics on stations, select the necessary server or several servers and then select the necessary item in the contextual menu. A window with the table similar to that described in p. 6.2.3. Will open.

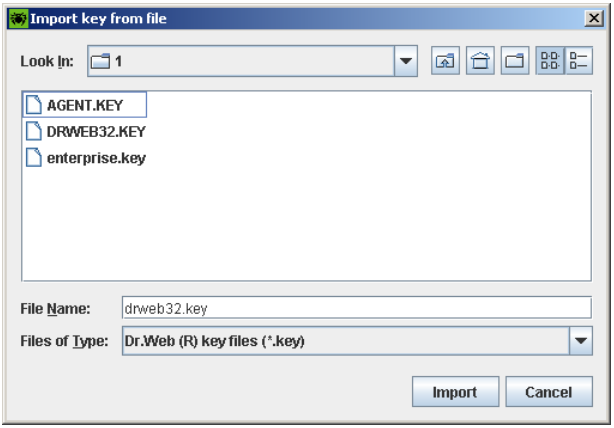
   The only difference of this table is the presence of the `Server` column.

6.7. Updating the server key and keys of workstations

The files containing the server key and the keys of workstations are placed into the program complex during the installation (read p. 3.3). In future you can receive new keys, for example, with the prolonged license term.

To install new key files into the program complex:

1. Select the Configure Dr.Web(R) Enterprise Server item in the Administration menu of the anti-virus console. In the opened submenu, select the Protocols pane (read p. 6.5.2). In this pane (pic. 42) uncheck the Dr.Web (R) Enterprise Agent and the Dr.Web (R) Network Installer boxes.
2. Select the Dr.Web (R) Enterprise Server Schedule item in the Administration menu (read p. 6.5.3) and delete all tasks from the list.
3. In multiserver networks, select the Neighborhood item in the Administration menu (read p. 6.6.2). A window with the list of linked servers will open. For each server on this list select the Delete item in the contextual menu.
4. Restart the server. For this, select the Restart Dr.Web(R) Enterprise Server item in the Administration menu.
5. Place the file with the server key (it should be called enterprise.key) into the etc directory of the server installation directory instead of the existing file.
6. In the directory of the anti-virus network select the Everyone group and then select the Import key item in its contextual menu. A window (pic. 74) will open. You will be offered to select the key file for the workstation to be imported.



Picture 74. Import of a key

7. In the `Administration` menu select the `Configure Dr.Web(R) Enterprise Server` item; in the opened submenu select the `Protocols` pane and deselect the `Dr.Web (R) Enterprise Agent` and the `Dr.Web (R) Network Installer` checkboxes.
8. Restart the server.
9. Set the server schedule (read p. 6.5.3).
10. In multiserver configuration, set the connection with the servers (read p. 6.6.2).

7. Administrating the anti-virus network

7.1. Administrators of the anti-virus network

The administrator of the anti-virus network has exclusive rights for the administration of the whole network and of the anti-virus server. The anti-virus network administrator also has full rights to administrate the anti-virus software of a workstation. He can restrict or even disable a user's interference into administration of the anti-virus software on the workstation (read p. 6.2.5).

To administrate the complex, the anti-virus network administrator may not have administrative privileges in the local network or on separate computers. The administrator's workplace (the anti-virus console) can even be outside the local network.

The complex's installation requires privileges of the local network administrator, setting up the anti-virus server requires full access to its installation directory.

It is advisable to appoint a reliable and a skilful employee as the administrator of the anti-virus network, with the experience in administration of the local network, who is competent in anti-virus protection. Such employee should have full access to the installation directories of the anti-virus server. Depending on the company's security and human resources policies, the anti-virus network administrator should either have the administrator privileges of the local network or properly contact with such employee.

There can be several administrators on the anti-virus network (on one and the same server). The administrators' accounts are divided into two groups:

- full rights accounts
- "read only" accounts

The administrators of the first group can view and edit the configuration of the anti-virus server and the settings of its separate elements, as well as create new administrator accounts.

The administrators with the "read only" accounts can only view the settings of the anti-virus network and its separate elements, but cannot modify them. They can also view the list of available administrators' accounts.

There is one account with full rights after the system installation.

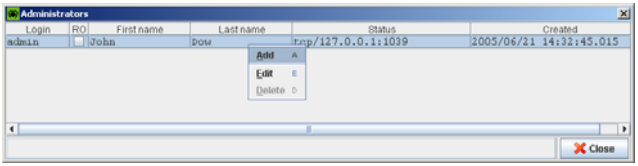
7.2. Managing the administrators' accounts

The program complex allows any administrator with full rights to edit settings (including user name and administrator password), create new and delete already existing accounts.

By default, if other was not specified during the installation, the program complex is installed with the administrator account with full rights (name - `admin`, password - `root`). If the complex was installed with the default settings, it is advisable to change the password when the administrator logs in on the server for the first time and to edit the account description.

To edit the administrators' accounts:

1. Select the `Administrators` item in the `Administration` menu. A list with administrators' accounts will open (pic. 75).



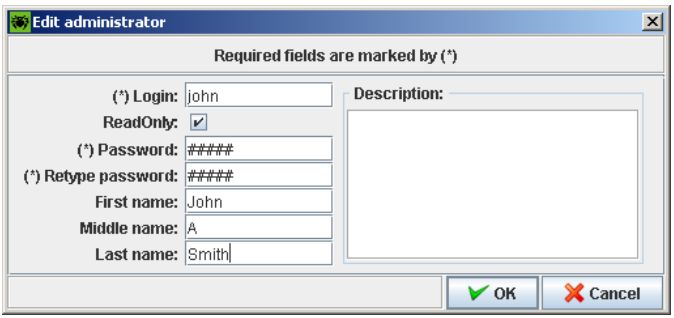
Picture 75. Administrators' list

2. To edit any account, select it in the list and then select the `Edit` item in the contextual menu. A window for editing the account will open.

To add an account, select the `Add` item in the contextual menu. A similar window will open.

To delete an account, select it in the list and then select the `Delete` item in the contextual menu.

The parameters of the edited and added account are displayed in the `Edit administrator` window (pic. 76).



Picture 76. Editing accounts

Fill in or edit the necessary fields (when new account is created, the ID, the Password and the Retype password fields should be obligatory filled in). When creating an administrator's account with full rights, deselect the `Read only` checkbox (set by default).

Appendices

Appendix A. Description of settings for the external DBAS

When setting the access to DBAS for storage and processing of the centralized log, the parameters described below are used for different types of DBAS.

Internal DBAS (IntDB) — see Table 4.

Table 4.

Name	Default value	Description
DBFILE	dbinternal.dbs	Path to the database file
CACHESIZE	2048	Database cache size in kilobytes
SYNCHRONOUS	FULL	The mode of synchronous logging of changes in the database on the disk: FULL — fully synchronous logging on the disk, NORMAL — synchronous logging of critical data, OFF — asynchronous.

ODBC (for Windows version only) — see Table 5

Table 5.

Name	Default value	Description
DSN	Drwcs	Data set name
USER	Drwcs	User name
PASS	Drwcs	Password
TRANSACTION	DEFAULT	Read below

Possible values of the TRANSACTION parameter:

```
SERIALIZABLE
READ_UNCOMMITTED
READ_COMMITTED
REPEATABLE_READ
DEFAULT
```

The DEFAULT default value means "use default of the SQL-server".

Read more here

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/odbc/htm/odbctransaction_isolation_levels.asp

PostgreSQL (for UNIX version only) — see Table 6.

Table 6.

Name	Default value	Description
Host	Unix-domain socket	PostgreSQL server host
Port		PostgreSQL server port or file name extension of the socket
Dbname	drwcs	Database name

Name	Default value	Description
User	drwcs	User name
Password	drwcs	Password
Options		Debug /trace options for sending to the server
tty		File or tty to output debug
requiressl		1 – for SSL connection request or 0 for absence of such request

Appendix B. Description of parameters of the alerts system

When setting the system of alerts on events connected with the program's operation the parameters described below are used for different types of the alerter drivers.

E-mail notifications (the `drwemail` driver) — see Table 7.

Table 7.

Name	Default value	Description
HOST	127.0.0.1	SMTP host
PORT	25	SMTP port
PASS		Smtp password
DEBUG	NO	Debug mode
FROM	drwcsd@localhost	Sender's address
TO	root@localhost	Recipient's address
HOST	127.0.0.1	SMTP host

Notifications using Windows Messenger (`drwwnetm` driver), for Windows version only — see Table 8

Table 8.

Name	Default value	Description
TO	Admin	Computer network name

Appendix C. Parameters of templates of the notification system

Texts of messages (via e-mail or Windows Messenger) are generated by the server component named the templates processor on the basis of the templates files.

The templates files consist of texts and variables enclosed into braces. When editing a templates file the variables below listed can be used.

The templates processor does not perform recursive substitutions.

The variables are written as follows:

- `{SYS.TIME}` — substitute current value of the `SYS.TIME` variable
- `{SYS.TIME:5}` – the value of first five symbols of the variable
- `{SYS.TIME:3:5}` — the value of five symbols of the variable behind the first three symbols (beginning from the fourth), if the remainder is less, it is supplemented by blanks on the right
- `{SYS.TIME:3:-12}` — the value of 12 symbols of the variable behind the first three (beginning from the fourth), if the remainder is less, it is supplemented by blanks on the left

For example, let `SYS.TIME` be equal to "`10:35:17.456`". Then, the expression `{SYS.TIME:5}` is equal to "`10:35`". The expression `{SYS.TIME:3:5}` is equal to "`35:17`". The

expression {SYS.TIME:3:-12} is equal to " 35:17.456". The expression {SYS.TIME:3:12} is equal to "35:17.456 ".

The replacement (substitution) can be used when processing the variables, for example, the expression {SYS.TIME/10/99} (under the above described conditions) is equal to "99:35:17.456", and the expression {SYS.TIME/10/99/35/77} is equal to "99:77:17.456".

There is no limitation for the number of substitution pairs.

System variables:

- SYS.TIME — current system time
- SYS.DATE — current system date
- SYS.DATETIME — current system date and time
- SYS.VERSION — server version
- SYS.BUILD — server build date
- SYS.PLATFORM — server platform
- SYS.PLATFORM.SHORT — short variant of SYS.PLATFORM
- SYS.OS — server operating system name

The environment variables have the same names as the variables specified in the environment with the ENV. prefix added (the prefix ends with the full stop).

Shared variables of messages, the agent:

- GEN.StationName — station name
- GEN.StationID — UUID of station
- GEN.StationAddress — address of station
- GEN.LoginTime — station login time

Shared variables of messages, the server updating subsystem:

- GEN.Product – product description
- GEN.Folder – product location directory
- GEN.CurrentRevision – current version identifier
- GEN.NextRevision – updated version identifier

Message variables, according to messages (for the agent)

Installation_OK: no variables are available

Installation_Bad:

- MSG.Error — error message

Infection:

- MSG.Component — component name
- MSG.RunBy — component run by this user
- MSG.ServerTime — event time, GMT
- MSG.ObjectName — infected object name
- MSG.ObjectOwner — infected object owner
- MSG.InfectionType — infection type
- MSG.Virus — virus name
- MSG.Action — curing action

Unknown_Station:

- MSG.ID — UUID of unknown station
- MSG.Rejected — rejected — station's access denied, newbie — there was an attempt to assign the "newbie" status to a station

Station_Authorization_Failed:

- MSG.ID — UUID of station.

- `MSG.Rejected` — `rejected` — station's access denied, `newbie` — there was an attempt to assign the "newbie" status to a station

`Cannot_Add_Station`:

- `MSG.ID` — UUID of station

`Too_Many_Stations`:

- `MSG.ID` — UUID of station

sent when a new station cannot log in to the server due to the license limitations.

`License_Limit`:

- `MSG.Used` — number of stations in the base
- `MSG.Licensed` — permitted by license

sent at every server launch, if the server is run with the key allowing connection of lesser number of stations than already connected

`Awaiting_Approval`: no variables are available

`Newbie_Not_Allowed`: no variables are available

`Statistics`:

- `MSG.Component` — component name
- `MSG.ServerTime` — event time, GMT
- `MSG.Scanned` — number of scanned objects
- `MSG.Infected` — number of infected objects
- `MSG.Modifications` — number of objects infected with known modifications of viruses
- `MSG.Suspicious` — number of suspicious objects
- `MSG.Cured` — number of cured objects
- `MSG.Deleted` — number of deleted objects

- `MSG.Renamed` — number of renamed objects
- `MSG.Moved` — number of moved objects
- `MSG.Speed` — processing speed in KB/s

`Connection_Terminated_Abnormally`:

- `MSG.Reason` — reason of termination.

`Processing_Error`:

- `MSG.Component` — component name
- `MSG.RunBy` — component run by this user
- `MSG.ServerTime` — event time, GMT
- `MSG.ObjectName` — object name
- `MSG.ObjectOwner` — object owner
- `MSG.Error` — error message

`Update_Failed`:

- `MSG.Product` — updated product
- `MSG.ServerTime` — time (local) of receipt of a message by the server

`Update_Wants_Reboot`:

- `MSG.Product` — updated product
- `MSG.ServerTime` — time (local) of receipt of a message by the server

`Not_Seen_For_A_Long_Time`:

- `MSG.StationName` — station name
- `MSG.StationID` — UUID of a station
- `MSG.DaysAgo` — number of days since last visit
- `MSG.LastSeenFrom` — the address a station was seen from for the last time

`Rejected_Newbie`:

- `MSG.AdminName` — administrator name
- `MSG.AdminAddress` — administrator console address

`Approved_Newbie`:

- `MSG.AdminName` — administrator name
- `MSG.AdminAddress` — administrator console address

`AutoApproved_Newbie`: no variables are available.

`Administartor_Authorization_Failed`:

- `MSG.Login` — login
- `MSG.Address` — network console address

`Unknown_Administartor`:

- `MSG.Login` — login
- `MSG.Address` — network console address

Variables of messages, according to messages (for server updating subsystem)

`Srv_Repository_UpToDate`: no variables are available.

`Srv_Repository_UpdateFailed`:

- `MSG.Error` — a message on error
- `MSG.ExtendedError` — detailed error description

`Srv_Repository_Cannot_flush`: no variables are available.

`Srv_Repository_Frozen`: no variables are available.

`Srv_Repository_Load_failure`:

- `MSG.Reason` — reason of error.

`Srv_Repository_Update`:

- `MSG.AdddedCount` — number of added files

- MSG.ReplacedCount — number of replaced files
- MSG.DeletedCount — number of deleted files
- MSG.Added — list of added files (each line for each name)
- MSG.Replaced — list of replaced files (in separate line)
- MSG.Deleted — list of deleted files (in separate line)

The variables of the last template do not include the files marked as "ignored in notification" in the product configuration file, read Appendix E3.

The variables of the server messages notifying about coming license expiration.

Key_Expiration:

- MSG.ObjType – object using the ending key (server/station/group)
- MSG.ObjId — GUID of object
- MSG.ObjName — object name
- MSG.Expiration — date of license expiration
- MSG.Expired — 1, if the term has expired, otherwise 0

Appendix D. Specification of the network address

D1. Introduction

The specification contains the following symbols:

- variables (the fields to be substituted by definite values) are enclosed into broken brackets and written in italics
- permanent text (remains after substitutions) is written in clarendon
- optional elements enclosed into square brackets
- the defined notion is placed on the left of the `::=` symbol string, the determination is placed on the right (as in the Backus-Naur form)

D2. General format of address

The network address looks as follows:

`[<protocol>/][<protocol-specific-part>]`

By default, `<protocol>` has the `tcp` value; the default values of `<protocol-specific-part>` are determined by the application.

IP addresses:

`<interface>::= <ip-address>`

`<ip-address>` can be either DNS name or IP-address separated by dots (for example, `127.0.0.1`).

`<socket-address>::=<interface>:<port-number>`

`<port-number>` must be specified by a decimal number.

IPX addresses:

`<interface>::=<ipx-network>.<mac-address>`

`<ipx-network>` must contain 8 hexit numbers, `<mac-address>` must contain 12 hexit numbers.

<socket-address>::=<interface>:<socket-number>

<socket-number> must contain 4 hexit numbers.

Connection – oriented protocol:

<protocol>/<socket-address>

where <socket-address> sets the local address of the socket for the server or the remote server for the client.

Examples:

tcp/127.0.0.1:2371

means tcp protocol, port 2371 on interface 127.0.0.1.

localhost:2371

the same.

tcp/:9999

value for the server: the default interface depending on application (usually all available interfaces), port 9999; value for client: default connection to host depending on application (usually localhost), port 9999.

tcp/

tcp protocol, default port.

spx/00000000.000000000001:2371

means socket spx loopback 0x2371.

Datagram – oriented protocol:

<protocol>/<endpoint-socket-address>[-<interface>]

Examples:

udp/231.0.0.1:2371

means usage of multicast group 231.0.0.1:2371 not dependent on an application's default interface.

udp/

- application-dependent interface and endpoint

udp/255.255.255.255:9999-myhost1

usage of broadcasting messages on port 9999 on myhost1 interface.

D3. Addresses of Dr.Web® Enterprise Server

1) receipt of connections:

```
<connection-protocol>/[<socket-address>]
```

By default, depending on <connection-protocol>:

- tcp/0.0.0.0:2371
  that means "all interfaces, port 2371"
- spx/00000000.000000000001:2371
  that means "all interfaces, port 0x2371"

2) server location service:

```
<datagram-protocol>/
       [<endpoint-socket-address>[-<interface>]]
```

By default, depending on <datagram-protocol>:

- udp/231.0.0.1:2371-0.0.0.0
  means usage of multicast group 231.0.0.1:2371 in all interfaces
- ipx/00000000.FFFFFFFFFFFF:2371-00000000.000000000000
  means receipt of broadcasting messages on socket 0x2371 in all interfaces.

D4. Addresses of Dr.Web® Enterprise Agent/Installer

1) direct connection to the server:

```
[<connection-protocol>/]
                        [<remote-socket-address>]
```

By default, depending on <connection-protocol>:

- tcp/127.0.0.1:2371
  means loopback port 2371
- spx/00000000.000000000001:2371
  means loopback socket 0x2371

2) server location <drwcs-name>, using the given family of protocols and endpoint

```
[<drwcs-name>]@<datagram-protocol>/
     [<endpoint-socket-address>[-<interface>]]
```

By default, depending on <datagram-protocol>:

- drwcs@udp/231.0.0.1:2371-0.0.0.0
  — location of a server with the drwcs name for tcp connection using multicast group 231.0.0.1:2371 in all interfaces
- drwcs@ipx/00000000.FFFFFFFFFFFF:2371-00000000.000000000000
  — location of a server with the drwcs name for spx connection using broadcasting messages on socket 0x2371 in all interfaces

Appendix E. Administrating the repository

E1. Introduction

The anti-virus server repository is designed to receive and distribute the updates of the ES components.

For this, the repository uses the sets of files (*products*). Each product is placed into a separate subdirectory of the `repository` directory, located in the `var` directory which, if installed with the default settings, is the subdirectory of the server root directory (read Appendix G for more details). The functions of the repository and the administration of it are independent for every product.

To administrate the updating, the repository uses the idea of *revision* of a product. The revision is a definite determination for the definite moment of time of the state of product files (including filenames and checksums) and has its unique number. The repository synchronizes the revisions of products as follows:

1) to anti-virus servers from Dr.Web GUS servers using HTTP or interserver synchronization protocol
2) between different anti-virus servers in multiserver configuration using interserver synchronization protocol
3) from the anti-virus server to workstations

The repository allows the user to set up the following parameters:

- the list of Dr.Web GUS servers in operations of type 1) using HTTP protocol (if using the interserver synchronization protocol - read p. 6.6, in this case the Dr.Web GUS servers are set as peer for which the option of the updates receipt should be enabled and the option of events transfer should be disabled)

- limitation of file sets of a product requiring synchronization of type 1) (thus, the user has the possibility to monitor only necessary changes of specific files or categories of files)
- limitation of parts of products requiring synchronization of type 3) (the user can choose what should be installed on a workstation)
- control of transition to new revisions (self testing of products before installation becomes possible)
- adding own components to products
- self-creation of new products which will be synchronized

At present the distribution kit includes the following products:

- Anti-virus server
- Anti-virus console
- Anti-virus agent (the software of the agent and of the workstation)
- Updater (the utility for updating files of the anti-virus agent)
- Virus bases

The following files located in the product's root directory are used to administrate the functions of the repository:

- Configuration file `.config` sets the file sets and the parameters of the updating server. The file has a text format, its structure is described below in pp. E2 and E3
- Status file `.id` displays the generalized state of a product (revision number and the incremental number of transaction). The format is described below in p. E4

When setting up interserver links for products mirroring (read p. 6.6) please remember that configuration files are not the part of the product and therefore are not properly handled by the mirror system. To avoid errors during the updating:

- For peer servers keep the configuration identical
- For subordinate servers, disable synchronizing of components using HTTP protocol or keep the configuration identical

After the configuration file and the status file have been edited, reboot the server.

E2. Syntax of the `.config` configuration file

The configuration file is represented as a sequence of *words* divided between each other by *separators*. The separator is any sequence of the following symbols: whitespace, tab, escape character, newline character.

A word beginning with the `;` symbol means the beginning of a comment which lasts till the end of the line.

Examples:

```
ghgh 123 ;this is a comment
123;this; is not; a comment – requires a separator
at the beginning.
```

A word beginning with the # symbol means the beginning of the stream comment; the rest of the word is specified by the end-of-comment marker.

Example.

```
123 456 #COMM from this place the COMM comment
already ended
```

To include any symbols into the word the `'` prefix is used — it is a special separating symbol for the given word (in other words, this symbol will be regarded as separator ending this word).

Example:

```
xy123 '*this is one word*this is another word
```

If a word begins with one of the `';#` symbols, it must be obligatory separated by special separators, as described above.

The `.config` file consists of comments and *instructions*. The sequence order of instructions is inessential.

The format of instructions of configuration files is case-sensitive.

The repository is case sensitive regardless the file system and the OS of the server.

The meaning of instructions is described in p. E3.

The format of instructions is described by the following symbols:

- `[...]` — fragment of the configuration file (internal structure is set in brackets, the repetition factor is set after the closing bracket, read below)
- `[...]1-` — optional fragment (0 or 1 time)
- `[...]1=` — obligatory fragment (one time)
- `[...]0+, [...]1+...` — repeat at least 0, 1 time, etc.
- `<...>` — the value specified by the user

```
[description  ]1-
```

```
[sync-with{
          [http{        [ ]1= [auth ]1- }]0+
          [http-proxy{ []1= [auth ]1- [http{...}]0+ }]0+
        }]1-

[sync-delay{     []0+ }]1-
        [sync-only{      []0+ }]1-
        [sync-ignore{    []0+ }]1-

[state-only{     []0+ }]1-
        [state-ignore{   []0+ }]1-

[notify-ignore{ []0+ }]1-
        [notify-only{    []0+ }]1-
        [notify-off{     [update]1- [delay]1-
 [flushfail]1- [loadfail]1- }]1-
```

E3. Meaning of instructions of the .config file

The `description` instruction sets the product name displayed in the console. If this instruction is unavailable, the name of the respective directory of the product is used as the product name.

Example:

```
description '"Dr.Web® Enterprise Agent"
```

The `sync-with` instruction sets the list of http-servers and http-proxy servers for updating. The `name` parameter sets the domain name or the IP-address. The `:port` construction may be absent, in this case, by default, 80 will be the port number for http-server and 3128 for proxy server.

The servers in the list are polled consequently, once the updating is successful, the polling procedure terminates.

The current version supports only base HTTP-authentication and Proxy-HTTP authentication.

Constant http-redirects (301) are cached in memory till the server reboot.

Example:

```
sync-with{
 http-proxy{ gateway:8080 auth scott:ivenhoe
    http{ esuite.drweb.com /update/a/drwagntd/ }
 }
}
```

The `sync-only` instruction explicitly specifies the sets of filenames (specified both by regular expressions in a simple form and as showed in this section, and in full form `qr{}`, as showed in p. 6.2.6), subject to synchronization. If the instruction is absent, by default, the whole content of the directory will be synchronized (excluding files `.id` and `.config`).

Example:

```
sync-only{^common/drw.*vdb$}
```

instructs to update the virus bases for the "anti-virus agent" only.

The `sync-ignore` instruction explicitly specifies the set of files which are not subject to synchronization.

If some files have been added to a product (those not present in the original set) and the `sync-only` instruction is not used, the added files should be listed in `sync-ignore`, otherwise they will be deleted during the synchronization.

The `sync-delay` instruction sets the list of files for which, if changed, the product's transition to new revision is disabled. The repository continues to distribute the previous revision and it is not synchronized (the state of product is "frozen"). If a user finds this

revision acceptable for distribution, he must edit the `.id` status file and restart the server (read p. E4).

Examples.

Automatic distribution of new revisions is disabled:

```
sync-delay{ .* } ; no automatic distribution,
                        I will test everything myself
```

The automatic distribution of revisions where the executable files are updated is disabled:

```
sync-delay{ .*\.exe$ .*\.dll$ }
```

The `state-only` and `state-ignore` instructions set (limit) the list of files for distrubution.

Example.

For the "anti-virus" product:

- The descriptions of the virus bases should be received, but not propagated
- No interface language, except for Russian, should be received
- No components designed for Windows 95/98/Me should be received

```
state-ignore{
    ; mind, that if the listed files were
    ; already distributed to agents, they will be
    ; they will be automatically deleted as soon
    ; as the revision number changes (from the
agent's point of view
    ; these files are not included into the product
any more)
  ^common/drw.*\.txt$
}

sync-ignore{
    ; If the listed files are already
    ; present in the repository,they still
```

```
    ; should not be propagated.
    ; Therefore, they should be deleted or
    ; listed in state-ignore{ } or be fully
    ; synchronized (read E4) in this
    ; configuration

;^common/ru-.*\.dwl$   we need it
 ^common/de-.*\.dwl$
 ^common/pl-.*\.dwl$
 ^common/es-.*\.dwl$
 ^win/de-.*\.*
 ^win/pl-.*\.*
 ^win-9x\.*
}
```

The instructions of the `notify` group allow to set up the notification system for separate products (the setting of the notification system is described in p. 6.5.2.4).

The repository generates the following notifications:

- `update` — when a product is usefully updated
- `delay` — when a transaction is frozen
- `flushfail` — when the flush error occurs
- `loadfail` — when the load error occurs

By default, all five types are allowed.

The `notify-off` instruction allows to disable definite types of notifications for the given product.

The `notify-ignore` and `notify-only` instructions allow to limit or specify explicitly the list of files, for which, if changed, the notification of the `update` type is sent.

If at least two of the `sync-only`, `sync-ignore` or `sync-delay` instructions are encountered in a file, the following rule is used:

- `sync-only` is applied first. The files not listed in this instruction (if any), are not processed
- `sync-ignore` is applied to the rest of files
- `sync-delay` is applied only to the remaining files (after the two previous items have been applied)

The same procedure is applied to the application order of `state-only` and `state-ignore`.

E4. `id` files

This product's state file is a text file into which the server logs the revisions of the product. Usually, the file contains a single number (current revision number). The product is synchronized if only the revision number is greater than the current number and the synchronization is performed in four stages:

- (1) two numbers are written to the `.id` file:
  `new_revision previous_revision.`
  Thus, it is marked, that the product is in an incomplete transaction from
  `previous_revision to new_revision.`
- (2) all changed files are received via HTTP and placed to the respective subdirectories with files of the following type
  `<original file name>. new_revision`
- (3) the result of transaction is written to the `.id` file
- This can be usual state, but with new number, or "frozen" state (`frozen`), if sync-delay was applied:
  `new_revision previous_revision frozen`
- (4) if not "frozen", new files replace the original files

When the server is rebooted after the `.id` file is analyzed, incomplete transaction "rolls back", otherwise, step (4) is performed.

E5. Examples of administration of the repository with modification of the state file

Complete product synchronization:

- stop the server
- delete the content of the product's directory, except for the `.id` and the `.config` files
- write `0` to the `.id` file
- restart the server

`0` revision has special meaning, as it disables propagation and the "empty" state of the product is not propagated to the agents.

Disabling of propagation:

- stop the server
- write `0` to the `.id` file
- "comment" the `sync-with` instruction in the `.config`, file to disable synchronization
- restart the server

Shift from "frozen" state to new version:

- replace the content of the `.id` file from
  `new_revision old_revision frozen`
  to
  `new_revision`
- restart the server

Roll back from "frozen" state to previous version:

- replace the content of the `.id` file from
  `new_revision previous_revision frozen`

to

```
new_revision previous_revision
```

- restart the server

At future attempts to synchronize with previsions configuration and to the same "new revision", the repository will "frozen" again. The roll back is reasonable when a suitable revision is available (for example, after successful tests in the lab) for download or when changing the configuration.

Appendix F. Server configuration file

The `drwcsd.conf` server configuration file resides, by default, in the `etc` subdirectory of the server root directory. When the server is run, non-standard location and name of the configuration file can be set by the command line parameter (read more in Appendix G).

The configuration file has a text format. The main structural elements of this file are *words*, separated by separators — whitespaces, tabs, escape characters, newline characters, and layout characters. In addition, a sequence of characters included into double quotes `"..."` is also considered as a word.

Special sequences of two characters beginning with `&` can also be included into a word. They are interpreted as follows:

- `&&` — as `&` character
- `&r` — escape character
- `&t` — tab
- `&n` — newline character
- `&v` — vertical tab
- `&f` — layout character
- `&b` — backspace character
- `&e` – character `=`
- `&l` – character `|` (vertical line)
- `&s` – whitespace character

The `&` character at the end of line is equal to `&n`.

Thus, a usual & character (which is not used to set a special sequence) should be doubled.

The comments begin with the ; symbol and continue till the end of the line.

The server settings are specified in the configuration file as instructions, each of them is one word. The instructions can be followed by instruction's parameters (one or several words).

Below are described possible instructions and their parameters. The sequence order of instructions in a file is inessential. The parameters (fragments of parameters) set by a user are in broken brackets.

`Name` <name>

Defines the name of the server (cluster) it will respond when the server is looked up by an agent or the administrator's console. The default value — empty line ("") — means usage of the computer name.

`Threads` <number>

The number of server threads which are serving clients. Must be not less than 10. By default — 10. It is recommended to double or triple this parameter, if the number of stations is greater than 100.

`DBPool` <number>

Number of database connections with the server, at least 5. By default, it is 5. It is recommended to double or triple this parameter, if the number of stations is greater than 100.

`Newbie` <mode>

Access mode of new stations, can have the `Open`, `Close` or `Approval` values (by default, it is `Approval`). Read more in p. 0.

`UnAuthorizedToNewbie` <mode>

The mode can have either the `Yes` value, which means, that the newbie status will be automatically assigned to unapproved stations

(for example, if the database has been destroyed), or the `No` value (default), which stands for a standard operation.

```
WEBStatistics "Interval=<number>
               Server=<server_address>
               URL=<directory>
               ID=<client_identifier>
               User=<user>
               Password=<password>
               Proxy=<proxy_server>
               ProxyUser=<proxy_user>
               ProxyPassword=<proxy_password>"
```

Describes the web-server where ES will publish its statistics on the detected viruses. The interval of publication is set in minutes, the default value is 30.

The default server address is `stat.drweb.com:80`

The default URL is `/update`.

ID — client's identifier (by default, it is derived from the user server key `enterprise.key`).

The `User` and the `Password` fields describe the authorization on the web-server, other fields stand for proxy server authorization. By default, the fields are empty (no authorization required).

To set the access to data collected on the statistics server, contact Technical support team (support@drweb.com).

`Encryption` <mode>

Traffic encryption mode. Possible values are `Yes`, `No`, `Possible` (the default value is `Yes`). Read more in p. 6.5.2.2.

`Compression` <mode>

Traffic compression mode. не `Yes`, `No`, `Possible` (the default value is `Possible`). Read more in p. 6.5.2.2.

`Database <DRIVER> from <PATH> using <PARAMETERS>`

Determination of the database. DRIVER — database driver name, PATH — a path where the driver must be loaded from, PARAMETERS — connection parameters between the server and the database. Read more in p. 6.5.2.3.

This instruction can only once be used in the configuration file.

Alert <DRIVER> from <PATH> using <PARAMETERS>

Determination of the "alerter". DRIVER — alerter driver name, PATH — a path where a driver must be loaded from, PARAMETERS — alerter parameters. Read more in p. 6.5.2.4.

This instruction can be used only once in the configuration file.

In this and in the next instruction the parameters of the using fields are separated by whitespaces. The parameter name is separated from the value by the = symbol (no whitespaces around it). If the parameter can have more than one value, they are separated from each other by the | symbols. If =, | symbols or whitespace are met in the parameter value, they are replaced with the &&e, &&l, &&s sequence accordingly.

transport <NAME> <STREAM> <DATAGRAM>

This describes the transport protocols and their relationship with network interfaces. NAME — name of the server (cluster), set as in the name instruction (read above), if empty line is specified, it is

taken from `name. STREAM` (for example, `tcp/`), `DATAGRAM` (for example, `udp/`) have the format described in Appendix D.

`Disable Message` <message>

Disable sending messages of a specific type, possible parameter values – message type, full list of message types is in the `var/templates` directory.

`Disable Protocol` <protocol>

Disable usage of one of the server protocols, possible values are `AGENT`, `SERVER`, `INSTALL`, `CONSOLE`. In the configuration file, by default, there is an instruction disabling the `SERVER` protocol. Read more in p. 6.5.2.

Appendix G. Command line parameters of programs included into ES

G1. Introduction

The command line parameters have higher priority than the default settings, or other constant settings (set in the server configuration file, Windows registry, etc.). In some cases, the parameters specified at launch predetermine also the constant parameters. Such cases are described below.

Some command line parameters have a key form — they begin with the hyphen. Such parameters are also called the keys.

Many keys can be expressed in various equivalent forms. Thus, the keys, which imply the logical value (yes/no, disable/enable) have negative meaning, for example, the `-admin-rights` key has a pair `-no-admin-rights` with opposite meaning. They can be specified with a definite value, for example, `-admin-rights=yes` and `-admin-rights=no`

The synonyms of `yes` are `on`, `true`, `OK`. The synonyms of `no` are `off`, `false`.

If the key value contains whitespaces or tabs, the whole parameter should be included into quotes, for example:
`"-home=c:\Program File\DrWeb Enterprise Agent"`

When describing the syntax of parameters of separate programs the optional part is enclosed into brackets `[...]`.

The names of keys can be abbreviated (last letters are omitted), if the abbreviated name does not coincide with the original part of any other key.

G2. Agent's interface module

The agent's interface module is run for each user who logs in to a computer on-line. In computers operated by Windows NT/2000/XP/2003 it is run with rights of this user. To function, the agent requires standard Windows Explorer as a user shell or any other program fully compatible with it.

Interface module start instruction syntax:

`drwagnui [`parameters_keys`]`

The following keys are allowed:

`-admin-rights` or `-no-admin-rights` — enable or disable admin mode in Windows 95/98/ME (i.e. consider or not the user working in these environments as an administrator). The administrator can, for example, change the agent's settings. For Windows NT/2000/XP/2003 it is determined by the OS authorization system. By default, it is disabled.

`-delay=`<number> — specifies in how many minutes after the load the welcome message should be displayed to the user. By default, it is 2 minutes; the `-1` value means to disable the welcome message.

`-help` — to display help in the format of commands. Under Windows 95/98/Me the help will be displayed in the window, in Windows NT/2000/XP/2003 it will be written into the Event Log (to view it use the Event Viewer).

G3. Agent

Constant settings of the agent (both the parameters and the list of servers the agent can connect to) are stored in the Windows registry in the `HKEY_LOCAL_MACHINE\SOFTWARE\IDAVLab\Enterprise Suite\Dr.Web® Enterprise Agent\Settings` string, and for the parameters set by the keys, the parameter name coincide with the key name.

When the agent is run and some parameters are explicitly specified, the specified settings are used not only in the current session, but are also written to the registry and become constant. Thus, if the agent is run for the first time with all necessary settings, at subsequent starts no parameters must be specified.

Under Windows NT/2000/XP/2003 the agent is run by the system as a service and is administrated through the Control panel. Under Windows 95/98/Me the agent is run as the Windows 95/98/Me service and it cannot be administrated.

Start instruction syntax:

`drwagntd [`parameters-keys`] [`servers`]`

The following keys are Possible:

`-home=`<directory> — directory, where the agent is installed. If the key is not set, the directory where the executable file of the agent resides is meant.

`-key=`<public_server_key> — a file of the server public key, by default, it is `drwcsd.pub` in the directory set by `-home`.

`-drweb-key=`<license_key> — user license key file. This key will be used by the client software, if it does not visit the server for a long time (more than 24 hours). If the connection with the server is supported, this key is not required. By default, arbitrary valid key in the directory set by the `–home` parameter.

`-crypt=`<mode> — server encryption mode. Possible values are `yes`, `no`, `possible`, the default value is `yes`.

`-compression=`<mode> — server traffic compression mode. Possible values are `yes`, `no`, `possible`, the default value is `possible`.

`-log=`<log_file> — agent's log file, by default, it is not logged.

Several `-log` keys are allowed with different file names, read below the description of the `verbosity` key.

`-rotate=`<quantity, size> — agent's log rotation. The default value is `10,10m` that means to store 10 files of 10 MB. If `m` is specified instead of `k`, the size will be set in KB, if no letter is specified; the size will be set in MB. A special `none (-rotate=none)` format can also be used — this means "do not use rotation, but write to one and the same file which can reach any size".

If rotation mode is used, the names of log files are generated as follows. Let log file name (see key above `-log`) be `file.log`. Then

- `file.log` — current file (log)
- `file.log.-1` — previous
- `file.log.-2` and so on — the greater the log is, the older is the version

`-verbosity=`<details_level> — log details level. By default, `INFO`, `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT` are also possible. The `ALL` and `DEBUG3` values are synonyms.

This key defines the log details level set by the `-log` key following after it (read above). Several keys of this type can be in one instruction.

`-retry=`<quantity> — the number of attempts to locate the server (if server search is used) before the failure is reported. 3 is set by default.

-timeout=<time> — search retry timeout in seconds. 5 is set by default.

-spiderstat=<interval> — interval in minutes the SpIDer Guard's statistics will be sent to the server, the default value is 30. The statistics will be sent to the server at such intervals if only the statistics have not been changed.

-help — generate help on command format and its parameters. The same is for -help of the interface module, read G2.

-control=<action> — administrating the state of the agent's service.
Possible actions:

install — install service

uninstall — uninstall service

start — run service (only Windows NT/2000/XP/2003)

stop — terminate service (only Windows NT/2000/XP/2003)

restart — restart service (only Windows NT/2000/XP/2003)

<servers> — list of servers. By default, drwcs@udp/231.0.0.1:2371, that means search the drwcs server using multicast requests for group 231.0.0.1 port 2371.

G4. Network installer

Start instruction format:

drwinst [keys] [variables] [servers]

Possible keys:

-key=drwcsd.pub — name and location of the server public key, it resides by default in the drwcsd.pub directory set by the -home key (read below).

`-uninstall` — uninstallation of the package on a station with the help of the uninstall script. (By default the `uninstall.rexx` script name is located in the station's root directory, for other cases read about key `-script`). If such key is unavailable (equals to `-no-uninstall`), the installation occurs.

`-script=`<script_name> — sets a file with the executed script. The default value depends upon the key presence `-uninstall` (`uninstall.rexx` will be default; at installation `preinstall.rexx` is by default.

Absence of the `preinstall.rexx` file during the installation does not mean error.

`-override` — to try to install the software once again. The attempt will fail, if any components are run. It is advisable to use the sequence "uninstall — repeated normal installation ". Absence of this file equals to `-no-override`.

If the network installer is run in the normal installation mode (i.e. without `-uninstall` and `-override` keys) on stations where the installation was already done, this will not generate any actions. The installer program terminates with the flag indicating that a successful installation has been completed.

`-interactive` — interactive mode. Absence of key is equivalent to the `-no-interactive` task.

`-quiet` — in interactive mode not to use the dialogs (do not prompt to reboot, etc.)

-retry=<quantity> — similar to the agent.

-timeout=<time> — similar to the agent.

-compression=<mode> — server traffic compression mode. Possible values are yes, no, possible, the no value is set by default.

-home=<directory> — installation directory. By default, it is "Program Files\DrWeb Enterprise Suite" on the system drive.

-log=<log_directory> — the directory for the logs of installation and uninstallation. By default, it is the logs subdirectory of the directory set by -home for installation or user directory for storage of temporary files (determinied by the operating system).

Due to the usage of the log directory the administrator can create a directory in the shared resource. All stations' logs will be located in this directory, which is convenient for analysis. Log file names are generated automatically using GUID and the computer name.

-verbosity=<details_level> — details level of the log (similar to the agent). The default value is WARNING.

-platforms=p1,p2,p3... – platforms load order (it is standard by default, read Appendix I).

-help — generate a help. Similar to the agent's interface module.

The variables are set after the keys as the list, the format of elements is as follows:

<variable>=<value>

Two most important variables:

`spider.install=no` — do not install SpIDer Guard. If no variable is specified — then install.

`spiderml.install=no` — similar, do not install SpIDer Mail.

`agent.id`=<identifier> ,
`agent.password`=<password> — the identifier and the password of a workstation; if these parameters are set, the workstation is connected not as the a "newbie", but with the specified parameters.

The list of servers is absolutely similar to the one described for the agent.

G5. Dr.Web® Enterprise Server

There are several variants how to launch the server. These variants will be described separately.

G5.1.

`drwcsd [`keys`]` — run the server (the keys are described below).

G5.2.

`drwcsd [`keys`] initdb agent.key [`<DB_script>
`[`<ini_file> `[`<password>`]]]` — database initialization.

`agent.key` — Dr.Web license key file (must be obligatory specified).

<BD_script> — DB initialization script. A special value — ("minus") — means not to use such script.

<ini_file> — previously formed file in the `drweb32.ini` format, which will determine the configuration of the Dr.Web default components (i.e. for the Everyone group). A special value — ("minus") — means not to use such file.

<password> — original password of the server administrator (its name is `admin`). By default, it is `root`.

The "minus" symbol can be omitted, if next parameters are missing.

G5.3.

`drwcsd [`keys`] updatedb` <script> — perform any action with the database (for example, to update it at a version upgrade), having executed the SQL-instructor from the <script> file.

G5.4.

`drwcsd verifydb` – run the server to check the database (when the check is completed, the server terminates).

G5.5.

`drwcsd upgradedb` <directory> – run the server to update the structure of the database at a version upgrade (see the `var/update-db` directory)

G5.6.

`drwcsd exportdb` <file> – export of the database to the specified file

G5.7.

`drwcsd importdb` <file> – import of the database from the specified file (the previous content of the database is deleted)

G5.8.

`drwcsd backup [`<directory> `[`<quantity>`]]` – backup critical server data (database, server license key file, private encryption key) to the specified directory. Users of version 4.32 upgrading to version 4.33, who saved the public-private pair of the encryption key, can use the drwsign utility (read G7) to create the private key of the new format – a complex of the public-private key from which the public can always be derived. The maximum quantity of the stored backup copies can be specified.

G5.9.

`drwcsd syncrepository` – synchronize the repository with GUS. It is not advisable to use this instruction if the automatic updating is enabled for the server. In this case, the server should better be terminated.

G5.10. Instructions' formats, for Windows only

`drwcsd [`keys`] install` — install the server service in a system.

`drwcsd uninstall` — uninstall the server service from a system.

`drwcsd start` — run the server service.

`drwcsd stop` — stop the server service.

`drwcsd kill` — emergency shutdown of the server service (if normal termination failed). This instruction should be used in case of absolute necessity.

`drwcsd restart` — restart the server service (it is executed as the `stop` and then `start` pair).

`drwcsd reconfigure` — reconfigure the file and reboot (this makes the start faster for no new process is created).

`drwcsd rerepository` – reread the repository from the drive.

`drwcsd retepmlates` – reread notification templates from the drive.

G5.11. Description of keys

`-home=`<root> — installation server directory (root directory). The structure of this directory is described in p. 2.1.1. By default, it is the current directory at start.

`-exe-root=`<directory_for_executables> — the path to executable files. By default, it is the `bin` subdirectory of the root directory.

`-var-root=`< directory_for _modified> — path to a directory to which the server has a write access and which is designed to store modified files (for example, logs and the repository files). By default, it is the `var` subdirectory of the root directory.

`-conf=`<configuration_file> — name and location of the server configuration file. By default, it is the `drwcsd.conf` file in the `etc` subdirectory of the root directory.

`-activation-key=`<license_key> — server license key. By default, it is the `enterprise.key` file located in the `etc` subdirectory of the root directory.

`-id=`<номер> — if `enterprise.key` allows to use more than one server, sets the position of this server in the list. By default, it is 1, i.e. the first in the list.

`-private-key=`<private_key> — private server key. It resides, by default, in the `drwcsd.pri` directory of the `etc` subdirectory of the root directory.

-log=<log> — server log filename. A minus can be used instead of the filename (for servers under UNIX only). It means output the log to the standard output. By default: for Windows platform it is drwcsd.log in the directory specified by the key -var-root, for UNIX platforms it is set by the -syslog=user key (read below).

-syslog=<mode> — possible for UNIX only. It means logging to the system log. Possible modes are auth, cron, daemon, kern, lpr, mail, news, syslog, user, uucp, local0 — local7 and for some platforms — ftp, authpriv and console.

-rotate=<quantity, size> — log rotation mode, similar to that of the agent.

-pid=<file> —for UNIX only, a file to which the server writes the identifier of its process.

-user=<user>

-group=<group> — available for UNIX only, if run by root user; means to change the user or the group of process and to be executed with the privileges of the specified user (or group).

-verbosity=<details_level> — log details level (similar to the agent's). The default value is WARNING.

-db-verify=on – check database integrity when the server is run. This is the default value. It is NOT recommended to run if the opposite value is explicitly specified, except if run immediately after the database is checked by the drwcsd verifydb instruction, see above.

-help — displays the help. Similar to the programs described above.

-daemon — for Windows platforms it means to launch as a service; for UNIX platforms: "daemonization of the process" (go to the root

directory, disconnect from the terminal and operate in the background).

`-minimized` — (for Windows only, if not run as a service, but in the interactive mode) — minimize a window.

`-screen-size=`<size> — (for Windows only, if not run as a service, but in the interactive mode) — log size in strings seen in the server screen, the default value is `1000`.

G6. Internal database administrating utility

Run format:

```
drwidbsh
```

The program operates in the text dialog mode, it waits for instructions from a user (the instructions begin with the "full stop" symbol). To receive help on other instructions, input `.help`

A text of a help will be displayed (a variant for the server under UNIX platforms).

```
./drwidbsh ../var1/dbinternal.dbs
DrwIntDB version 2.8.13
Enter ".help" for instructions
drwidbsh> .help
.databases List names and files of attached
                                                databases
.dump ?TABLE? ... Dump the database in a text
                                                    format
.echo ON|OFF Turn command echo on or off
.exit Exit this program
.explain ON|OFF Turn output mode suitable for
                                        EXPLAIN on or off.
.header(s) ON|OFF Turn display of headers on or off
.help Show this message
.indices TABLE Show names of all indices on TABLE
.mode MODE Set mode to one of "line(s)",
            "column(s)", "insert", "list", or "html"
.mode insert TABLE Generate SQL insert statements
                                                for TABLE
```

```
.nullvalue STRING Print STRING instead of nothing
                                          for NULL data
.output FILENAME Send output to FILENAME
.output stdout Send output to the screen
.prompt MAIN CONTINUE Replace the standard prompts
.quit Exit this program
.read FILENAME Execute SQL in FILENAME
.schema ?TABLE? Show the CREATE statements
.separator STRING Change separator string for
                                            "list" mode
.show Show the current values for various settings
.tables ?PATTERN? List names of tables matching a
                                                attern
.timeout MS Try opening locked tables for MS
                                           milliseconds
.width NUM NUM ... Set column widths for "column"
                                                 mode
```

To receive additional information, use reference manuals on SQL language.

G7. The utility of generation of key pairs and digital signature

Variants of the command fromat:

`drwsign genkey [<private> [public]]` — generation of the public-private pair of keys and their record to correspondent files.

The utility version for Windows platforms (in contrast to UNIX versions) does not protect a private key from copying.

`drwsign sign [-private-key=<private>] <file>` — sign the `<file>` file using this private key.

`drwsign check [-public-key=<public>] <file>` — check the file's signature using <public> as a public key of a person who signed this file.

`drwsign join432 [-public-key=<public>] [-private-key=<private>] <new_private>` — combines the public and private keys, format of version 4.32, into new complex format of the private key, version 4.33.

`drwsign extract [-private-key=<private>] <public>` - derives the public file from the private key file of the complex format (version 4.33 or higher).

`drwsign help [instruction]` — brief help on the program and on the command line format.

G8. Administrating the UNIX-version of the server by the kill instruction

The UNIX-version of the server is administrated by the alerts, sent to the server processor by the `kill` utility.

Use the `man kill` instruction to receive help on the `kill` utility.

Below are listed the utility alerts and the actions performed by them:

- `SIGWINCH` – log statistics to a file (CPU time, memory usage, etc.)
- `SIGUSR1` – reading the repository from the drive
- `SIGUSR2` – reading templates from the drive
- `SIGHUP` – server restart
- `SIGTERM` – server shutdown
- `SIGQUIT` - server shutdown
- `SIGINT` - server shutdown

Similar actions are performed by the keys of the `drwcsd` instruction for Windows version of the server, read p. G5.4.

G9. Dr.Web® scanner for Windows

This component of the workstation software has the command line parameters described in " Dr.Web for Windows User manual"). The only difference is that when the scanner is run by the agent, the `/go /st` parameters are sent to the server automatically and without fail.

Appendix H. Environment variables exported by the server

To easier set the processes run by the ES server on schedule, the data on location of directories of the server is required. For this, the server exports the following variables of the run processes into environment:

`DRWCSD_HOME` – path to the root directory (installation directory). The key value is `-home`, if it was set at the server launch; otherwise, current directory at launch.

`DRWCSD_EXE` – path to the directory with executable files. The key value is `-exe-root`, if it was set at the server launch; otherwise, it is the `bin` subdirectory of the root directory.

`DRWCSD_VAR` — path to the directory, to which a server has a write access, and which is designed to store volatile files (for example, logs and repository files). The key value is `-var-root`, if it was not set at the server launch; otherwise, it is the `var` subdirectory of the root directory.

Appendix I. Agent installation script

The installation routine of the agents onto workstations using the network installer (`drwinst.exe`) is set by `install.script`. These files reside in the products root directory in the repository. In standard distributions they are located in `10-drwupgrade` and `20-drwagntd` directories and describe the default installation.

If the `.custom.install.script` file is present in the directory, it is used instead of the standard scenario.

Files with other names beginning with a full stop are not updated when the product is updated and do not influence the operation of the repository.

Sequence of operations during the installation:

1. The network installer requests from the server the platforms' set: win-setup, common, win, win-nt and win-9x – this is the list of standard platforms in the default order. The order of usage of platforms can be changed by the `–platforms=p1,p2,p3...` key when calling `drwinst`. The win-setup platform is not included into a standard distribution and is meant for creation of its own installation routines, if necessary.
2. The server forms a list of files according to the list of platforms, viewing step by step all products in alphabetical order and lists of files set by the `files{ }` constructions for the given platform in the `install.script` installation routine (read below). At the same time, the summary script is built on the basis of the `scripts{ }` constructions.
3. The server receives the general list of files and the summary script.

4. The server sends the files and the script which will be performed by the network installer.

Now, let us examine `install.script` on the example of the `20-drwagntd` directory.

```
; master part of installation: agent & its stuff.
; drwscr.dll goes with upgrader, so unlisted here.

platform{              ; win - for all Windows OS
                       ; `name: XXX' MUST go first!

  name:   win           ; (mandatory stanza)
                        ; this platform name

              ; include, scripts{ }, files{ }
              ; can go in any order

  scripts{              ; (optional)
              ; script being merged with all others
win.inst.rexx ; and executed after transfer all
              ; files for all platforms requested
              ; by installer
              ; Windows installer request order:
              ; - win-setup (optional! for
              ;                      customization)
              ;   - common
              ;   - win
              ;   - win-nt OR win-9x
  }

  files{      ; (optional)
              ; this platform files being
              ; transfered to installer
    win/uninstall.rexx
    win/drwinst.exe
    win/drwagntd.exe
    win/drwagnui.exe
    win/drwhard.dll
  }
}
```

```
platform{      ; win-9x - for Windows 95-ME
  name:   win-9x
  scripts{ win-9x.inst.rexx }
}

platform{      ; win-nt - for Windows NT-2003
  name:   win-nt
  scripts{ win-nt.inst.rexx }
}

platform{      ; common - for any OS including UNICES
  name:   common
  scripts{ common.inst.rexx }
}

; include file.name ; (optional)
        ; this stanza tells to include other file.
        ; including file will be searched in the
        ; same directory where current file are
        ; located if `file.name' does not include
        ; directory specificator
-----------------------------------------
```

The script contains a list of the `platform{ }` constructions and allows to include determinations from other files with the help of the `include` construction (`include` is admissible on the upper level only and is inadmissible inside `platform{ }`). If `file.name` in `include` does not contain paths, but the filename only, it is looked for in the same directory as the current one. The usage of `include` constructions in the included files is allowed.

The description of a platform begins with the `name: XXX` construction. Then, the pair of `files{ }` and `scripts{ }` lists follows, the order of these lists is inessential, the lists may contain any number of elements. The order of elements in the list is essential as it defines the order of files transfer to the station and the construction of the formed script.

The order of the `platform{ }` constructions is also inessential.

Below are listed the variables of the installation scripts (the values for these variables can be specified from the command line of the network installer) with their default values.

Components to be installed:

```
spider.install   = 'yes'
spiderml.install = 'yes'
scanner.install  = 'yes'
```

`install.home` – installation directory

```
agent.logfile = install.home'\logs\drwagntd.log'
agent.loglevel = 'trace'
agent.logrotate = '10,10m'
agent.servers = install.servers
agent.serverkey = install.home'\drwcsd.pub'
agent.compression = 'possible'
agent.encryption = 'yes'
agent.findretry = '3'
agent.findtimeout = '5'
agent.spiderstatistics = '30'
agent.importantmsg = '2'
```

The `agent.importantmsg` parameter defines the form of the messages on the updating error, on the reboot request, etc. displayed to a user. `0` — do not display, `1` — display as a pop-up dialog over all windows, `2` — display as a tooltip of the icon in the Windows Explorer (if the current Explorer version does not support this option, then mode `1 is used`).

Let us create nonstandard installation scenario in which SpIDer Guard is not installed and maximum detailed logging is set:

1. Create the `.win-setup.inst.rexx` file in the `20-drwagntd` directory and write to it

```
---------------
spider.install = 'no'
agent.compression = 'no'
agent.loglevel = 'all'
---------------
```

2. Create the `.custom.install.script` file in the `20-drwagntd` directory and write to it

```
---------------------------------
include install.script

platform{
 name: win-setup
 scripts{ .win-setup.inst.rexx }
}
-----------------------------------
```

3. Reboot the server or give a signal to reboot the repository:

- For Unix: `kill -USR1 cat `drwcsd.pid``
- For Windows: `drwcsd.exe rerepository`