Doctor Web, Ltd.

Dr.Web® Enterprise Suite

Administrator Manual

Version 4.44.3

Dr.Web® Enterprise Suite
Administrator Manual
25.09.2008.

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

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

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

Dr.Web®

Dr.Web® develops and distributes information security solutions under the Dr.Web trademark which provide efficient protection from malicious software and spam. Dr.Web® customers can be found among home users from all over the world and in government enterprises, small companies and nationwide corporations.

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

We thank all our customers for their support and trust in Dr.Web products!

Doctor Web, Ltd.

Table of Contents

Chapter 1: Welcome to Dr.Web® Enterprise Suite

1.1. Introduction

The Manual is meant for system administrators responsible for the organization of anti-virus protection.

This Manual is intended to introduce technical features and the functionality of the software and provide detailed information on the organization of the complex anti-virus protection of corporate computers using **Dr.Web® Enterprise Suite** (**Dr.Web® ES**).

The main part of the document explains how to organize a complex anti-virus protection of computers of your company, namely how to install the program, build an anti-virus network, configure and update **ES** components to assure the ultimate anti-virus protection in your company.

The second part of the document (Appendices) provides technical information, describes the parameters necessary for adjustment of the modules, explains the syntax and values of instructions.

The Manual does not include the description of **Dr.Web®** anti-virus packages for protected computers. For relevant information, please consult **"Dr.Web® Anti-Virus for Windows. User Manual"**.

Before reading this document make sure you have the latest version of the Administrator Manual. The Manual is constantly updated and the current version can always be found at the official web site of **Doctor Web, Ltd**. at http://download.drweb.com/esuite/.

1.2. Conventions and Abbreviations

The following conventions are used in the Manual.

Table 1-1. Conventions

Symbol	Comment
 Note, that	Marks important notes or instructions.
 Warning	Warns about possible errors.
Dr.Web® ES	Names of **Dr.Web®** products and components.
Anti-virus network	A term in the position of a definition or a link to a definition.
<IP-address>	Placeholders.
Cancel	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
`C:\Windows\`	Names of files and folders, code examples, input to the command line and application output.
Appendix A	Cross-references or Internal Hyperlinks to web pages.

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

- **Dr.Web® GUS** — **Dr.Web® Global Update System**,
- **ES** — **Enterprise Suite**,
- GUI — Graphical User Interface, a GUI version of a program — a version using a GUI,
- LAN — Local area network;
- OS — operating system,
- PC — personal computer.

1.3. About Dr.Web Enterprise Suite

Dr.Web® Enterprise Suite ensures complete anti-virus protection of your company's computers regardless of whether they are integrated in a local network or not.

Dr.Web® ES provides for

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

Dr.Web® ES allows both to grant the users of the protected computers with the permissions to set up and administer the anti-virus packages on their computers, or flexibly limit their rights, including absolute prohibition.

Dr.Web® ES has a *client-server* architecture. **ES** components are installed on the computers of users and administrators and the computer(s) to function as the anti-virus server(s), and exchange information through network protocols TCP/IP, IPX/SPX, NetBIOS. An aggregate of computers on which **Dr.Web® ES** cooperating components are installed is called an *anti-virus network*.

An anti-virus network includes the following components:

- *Anti-virus Server* stores distribution kits of anti-virus packages for different OS's of protected computers, updates of virus databa ses, anti-virus packages and anti-virus Agents, user keys and package settings of protected computers. The anti-virus Server sends necessary information to the correspondent computers on Agents' requests and keeps a general log of events of the whole anti-virus network.
- *Anti-virus Console* is used for the remote administration of the anti-virus network by means of editing the settings of the anti-virus Server and protected computers stored on the anti-virus Server and protected computers.

- *In-built Web Server* is automatically installed with the anti-virus Server. It is a certain extension of a standard web page of the Server and allows to
  - view general information about the **ES** Server,
  - read the documentation,
  - view the repository.
- *Anti-virus ES Agent* is installed on protected computers. It installs, updates and controls the anti-virus package as instructed by the anti-virus Server. The **ES** Agent reports virus events and other necessary information about the protected computer to the anti-virus Server.

The anti-virus Server can be installed on any computer of the local network, not only on that functioning as a local network server. It is crucial that this computer is connected to the Internet to communicate with other anti-virus network computers and Global Update System servers.

The anti-virus Console can be installed on a different computer than the Server, there should be a TCP/IP connection between the Console and the anti-virus Server (IPv6 is also supported).

The anti-virus network can incorporate several anti-virus Servers. The features of such configuration are described in the Manual in p. Peculiarities of a Network with Several Anti-Virus Servers below.

An anti-virus package installed on protected workstations includes the following components:

Core components:

- *Dr.Web Scanner for Windows* is a part of the common product **Dr.Web® for Windows**. Its executable file is drweb32w.exe. The Scanner is configured through group or personal settings for the workstation. It scans the PC upon user's demand or according to the user's local schedule. Additionally has an anti-rootkit module (not included in **Dr.Web® Enterprise Scanner**).

- *Dr.Web Enterprise Scanner for Windows* is one of **ES** Agent functions. It is also an anti-virus scanner and uses the same virus databases and search engine. But this functionality is 'built in' the **ES** Agent. **Dr.Web® Enterprise Scanner** is meant to scan for viruses on demand: either according to the schedule, or a direct task from the **ES** administration console. It has no special interface and no independent settings, it is configured only when run through the Console interface (when scanning is scheduled or initiated manually).

Optional components:

- *SpIDer Guard (a file monitor)* constantly resides in the main memory and checks all opened files on removable media and files opened for writing on hard drives on-access. Besides, the guard constantly monitors running processes for virus-like activity and, if they are detected, blocks these processes and informs the user about it.
- *SpIDer Mail (a mail monitor)* also constantly resides in the memory. The program intercepts all calls from your mail clients to mail servers via POP3/SMTPIMAP4/NNTP protocols and scans incoming (or out-going) mail messages before they are received (or sent) by the mail client.

1.4. Benefits

Dr.Web ES offers the following benefits:

- Cross-platform Server's software enables using both Microsoft® Windows® and UNIX® operated computers;
- Both Windows OS and UNIX OS computers are protected;
- Network traffic can be reduced to minimum, special compression algorithms are applicable;
- Data transferred between system components can be encrypted;
- Grouping of anti-virus stations facilitates administering of the anti-virus network;
- The administrator's workplace (anti-virus Console) can be installed almost on any computer under any OS;
- Remote installation and removal of the package software directly from the Console of the system administrator (for Microsoft® Windows NT OS, Microsoft® Windows® 2000 OS, Microsoft® Windows® XP Professional OS, Microsoft® Windows® 2003 OS, Windows® Vista OS);
- Centralized installation of anti-virus Agents, the Agents' software can be set up prior to the installation on client machines;
- Spam filters can be used on anti-virus stations (provided that it is authorized by the acquired license);
- Virus databases and program modules updates are promptly and efficiently distributed to client computers by the **Dr.Web® Enterprise Suite Server**;
- Server's critical data (databases, configuration files, etc.) is backed up.

In comparison to other anti-virus products, **Dr.Web® ES** can be installed on infected computers!

1.5. System Requirements

For Dr.Web ES to be installed and function the following is required

- the anti-virus Server should have access to the Internet to receive updates from **Dr.Web® GUS**;
- anti-virus network computers should have access to the Internet to connect to the Sever or be in the same local network as the Server;
- a TCP/IP connection between the Console and the anti-virus Server (IPv6 is also supported).

The anti-virus Server requires

- Intel® Pentium® III 667 MHz or faster;
- 128 MB RAM (256 MB in case a built-in database is used);
- up to 12 GB of free (available) disk space: up to 8 GB for a built-in database (installation catalog) and up to 4GB for the system temporary catalog (for work files);
- Windows NT4 SP6a OS or later, Linux® OS, FreeBSD® OS or Solaris™ OS (see Appendix A. The Complete List of Supported OS Versions);
- MS Installer 2.0 (for the installation of the anti-virus Server for Windows OS);
- Windows Script 5.6 WindowsXP-Windows2000-Script56-KB917344-x86-enu.exe (for installation on Windows NT4 OS, Windows XP OS and Windows 2000 OS);
- `libiconv` library v. 1.8.2 or later (for the installation of the anti-virus Server for FreeBSD OS and Solaris OS).

MS Installer 2.0 is included into Windows 2000 (with SP3) OS and later versions. If you use earlier versions of Windows OS, you should previously download and install MS Installer 2.0.

For details, please visit http://msdn2.microsoft.com/en-us/library/aa367449.aspx.

The Libiconv library can be downloaded from ftp://ftp.freebsd.org.

The anti-virus Console requires

- a computer under Windows OS or a UNIX system-based OS (see Appendix A. The Complete List of Supported OS Versions);
- Windows Script 5.6 `WindowsXP-Windows2000-Script56-KB917344-x86-enu.exe` (for installation on Windows XP OS and Windows 2000 OS).

The anti-virus ES Agent and the package require

- Intel® Pentium® II 400 MHz or faster;
- RAM not less than 32 MB;
- not less than 108 MB of available disk space (8 MB for executable files, the rest - for logs);
- Windows 98 SE OS, Windows Me OS , Windows NT4 (with SP6) OS or later
  - Notes: **SpIDer Guard** operates in 32bit systems only.

No other anti-virus software (including other versions of **Dr.Web®** anti-virus programs) should be installed on the workstations of an anti-virus network managed by **Dr.Web® ES**.

1.6. Distribution Kit

The program software is distributed in two variants subject to the OS of the selected anti-virus Server:

- as two bzip2 files or installation packages for UNIX system-based OS's - for the Server and the Console,
- as two executable files of the installation wizard for Windows NT OS, Windows 2000 OS, Windows XP OS, Windows 2003 OS, Windows Vista OS - for the Server and the Console.

The distribution kit contains the following components:

- anti-virus Server software for the respective OS,
- anti-virus Agents software and anti-virus packages software for supported OS's,
- anti-virus Console software and launch scripts for main OS's,
- Web Server software,
- virus databases,
- manuals, templates, and examples.

In addition to the distribution kit, serial numbers are also supplied. Having registered these serial numbers one can get files with a Server key and an Agent key.

1.7. Key Files

When purchasing a license for the **Dr.Web® ES** anti-virus, you receive registration keys or a registration card with a serial number. Mind that it is impossible to install the Server unless you have key files. These files are designed to regulate user rights to use the **Dr.Web® ES** anti-virus. Key file parameters are set in accordance with the license agreement. Such files also contain user data.

Key files have a write-protected format based on the mechanism of electronic signature. 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.

The **Dr.Web® ES** license parameters and price depend on the number of protected computers, which includes the servers protected by the **Dr.Web® ES** network.

Before purchasing a license for a **Dr.Web® ES** solution you should carefully consider this information and discuss all the details with your local distributor. You should state the exact number of anti-virus Servers to build the anti-virus network with. The number of independent Antivirus Servers (the servers which do not interact with each other) running the network does not affect the license price (see also p. Installing the Anti-Virus Server and the Anti-Virus Console).

Note that **Dr.Web® ES** is licensed per connection. When calculating the number of licensed needed for the network, count the number or connections between Antivirus Servers. Each connection requires an additional license. Furthermore, an additional license is required for each connection between Antivirus Servers regardless of its type (see...for details), that is a separate license for each connection is required for each Antivirus Servers. For example, in case of one connection between two server, you need two licenses.

License key files are generally sent to users by e-mail, after the product serial number has been registered at the special web site: http://buy.drweb.com/register/ unless otherwise specified in the registration card attached to the product. Visit the web site above, in the form enter your personal data and in the corresponding field type the registration serial number (it is written on the registration card). An archive with key files will be sent to the designated address. Or you will be allowed to download it directly from the web site.

As a rule, key files come in a zip-archive, which contains a key file for the Server (`enterprise.key`) and a key file for workstations (`agent.key`).

Users can receive key files in one of the following ways:

- by e-mail (usually after registration of the serial number at the web site, see above);
- with the anti-virus distribution kit if license files were included at kitting;
- as a file on a separate carrier.

Please keep key files until they expire. They are required during the installation and re-installation of the anti-virus, as well as to restore program components. In case a license key file is lost, you need to complete the registration form at the web site specified above so that you can restore it. Note that you will need to enter the same registration serial number and the same personal data as during the first registration, you can change the e-mail address only. In this case the license key file will be sent to the new address.

To try the **Dr.Web® ES** anti-virus and familiarize yourself with the software, you can order demo keys. Such key files provide for the full functionality of the main anti-virus components, but have a limited term of use. Demo key files are sent upon request made through the web form at http://download.drweb.com/demo/. Your request for demo keys will be examined and, if approved, an archive with key files will be sent to the designated address.

The use of obtained key files during the installation is described in p. Installing the Anti-Virus Server and the Anti-Virus Console below.

The use of key files after the program complex is installed is described in p. Replacing Old Key Files with New Ones below.

The number of requests for a key file is limited to 25 times. If more requests are sent, a key file will not be delivered.

1.8. Links

Some parameters of **Dr.Web® ES** are set as regular expressions. Regular expressions are processed by the PCRE program library, developed by Philip Hazel.

The library is distributed with open source codes; the copyright belongs to the University of Cambridge, Great Britain. All source texts of the library can be downloaded from http://www.pcre.org/.

The **Dr.Web® ES** software uses the Regina REXX interpreter legally protected by the GNU license. To download the source texts of the software or receive additional information, please visit the website of Regina at http://regina-rexx.sourceforge.net/.

The **Dr.Web® ES** software uses the JZlib library by JCraft, Inc. The library is legally protected by the BSD-based license. For more information, please visit http://www.jcraft.com/jzlib/LICENSE.txt.

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

The **Dr.Web® ES** software uses the Common Codec package derivative from Apache Jakarta Project distributed and protected by the Apache Software License. For details go to http://www.apache.org/licenses/LICENSE-1.1. The source text can be downloaded from http://jakarta.apache.org/.

The **Dr.Web® ES** software uses the JCIFS package distributed under the GNU Lesser license. The full source text can be downloaded from http://jcifs.samba.org.

Chapter 2: Installation and Removal of Dr.Web ES Components

This Chapter will guide you through the basic steps necessary to begin using the **Dr.Web® ES** anti-virus software.

Before installation, make sure that no other anti-virus software is installed on your computer.

2.1. Planning the Structure of an Anti-Virus Network

To create an anti-virus network

1. Make a plan of the anti-virus network structure taking including all protected computers and designating which ones are to function as the Servers.
2. Install the anti-virus Server software on the selected computer or computers.
3. Install anti-virus Consoles on the workplaces of the administrators of the anti-virus network. Mind that you do not need to install the anti-virus Console on each administrator computer. To make it accessible for use, you can share the Console's installation folder.
4. Through the Console, update the product software in the Server repository.
5. Configure the server(s) and workstations software.
6. Install the anti-virus Agent software on workstations and then register the anti-virus workstations at the anti-virus Server.
7. Through the Console set up and run the necessary modules.

When planning the structure of the anti-virus network, you should first of all select a computer to perform the functions of the anti-virus Server. Tip: the Server should be accessible on the network to all workstations connected to it during all the time of their operation.

To install the Server, the Console, and the anti-virus Agent, one-time access (physical or remote) to the correspondent computers is required. All further steps will be taken from the administrator's workplace (which can also be outside the local network) and will not require access to anti-virus Servers and workstations.

2.2. 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 **Dr.Web® ES** anti-virus. Unless and until it is successfully installed, no other **ES** components can be installed.

The installation procedure of the anti-virus Server depends on the Server version (for Windows OS or for UNIX system-based OS). Nevertheless, the parameters set during the installation and the structure of the installed software are the same for all versions.

All parameters set during the installation can be changed later by an anti-virus network administrator.

Together with the anti-virus Server the Web Server is installed, which like the Console serves to manage the anti-virus network and set up the Server. If you want your anti-virus network to be managed by other administrators, it is not necessary to install a Console on each administrator's computer. When an anti-virus Console is being installed, the **Dr.Web® Enterprise Console** folder is created on the local drive. You should share the folder, so that each administrator can run the Console's executable files.

It is not recommended to install the anti-virus software on computers on which it had previously been installed (even if unsuccessfully). It is necessary to remove all previously installed versions of the **Dr.Web®** anti-virus from the computers.

By default the anti-virus Server will run automatically after the installation.

2.2.1. Installing the Anti-Virus Server for Windows® OS

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

Before installing, please consider the following:

If Terminal Services are installed on Windows OS, you should install the software through the **Add or Remove Programs Wizard** only.

The distribution file and other files requested during the program's installation should reside on local drives of the computer on which the Server software is installed; these files should be made accessible for the LocalSystem user.

The anti-virus Server should be installed by a user with the administrator's rights to the computer.

After the anti-virus Server is installed it is necessary to update all **Dr.Web® ES** components (see p. Manual Updating of the Dr.Web ES Components).

In case an external database is to be used it is necessary to create the database first and set the ODBC driver (see Appendix B. The Description of the DBMS Settings. The Parameters of the DBMS Driver).

To install the anti-virus Server on a computer operated by Windows OS

1. Run the distribution file. A window for choosing the language of the **Installation Wizard** will open. Select the necessary language and click **Next**.
2. A window with information about the program to be installed will open. Click **Next**.

3. A window with the text of the license agreement will open. You should read and accept the agreement. To continue the installation, in the bottom part of the window select **I accept the terms of the license agreement** and click **Next**.

4. A window for selection of license key files will open.

   In the upper field click **Browse**, and then specify the `enterprise.key` license key file for the Server in the standard Windows OS window.

   At first installation of the Server, in the **This installation will** field select **Initialize new database**. In the **Initialize database with this Dr.Web® Enterprise Agent license key** field, specify the key file for the workstation software (`agent.key`).

   If you want to keep the Server database of the previous installation, select **Use existing database...**. You will be able to specify the database file later (see step **10**).

   Click **Next**.

5. A window for changing the default installation folder a window for changing the default installation folder (`C:\Program Files\DrWeb Enterprise Server`) will open. If necessary, change the installation folder.

6. Next you can choose the language of the notification templates, set the Agent's shared installation folder (hidden by default) and set up installation logging. If you want the Server to be started automatically after the installation, select the **Start service during setup** checkbox.

7. In the next window at first installation of the Server just click **Next**. Encryption keys will be automatically generated during setup.

   If you are installing the Server for an existing anti-virus network, select the **Use existing Dr.Web® Enterprise Server encryption keys** checkbox and specify the filenames of existing encryption keys for the Agents to identify the installed Server. Otherwise after the installation it will be necessary to copy the new encryption key to all workstations, on which **ES** Agents have been previously installed.

8. Next, if you have selected the existing database at step **4**, a window where you can specify a prearranged Server configuration file instead of that created by the installation program will appear.

9. In the next series of windows the main settings stored in the Server configuration file should be specified (see Appendix G. Server Configuration File).
10. In the dialog box dedicated to database parameters you can set up an internal or an external database of the Server. **IntDB** instructs to use built-in tools of the **Dr.Web® ES** anti-virus. In large networks with 100-200 computers or more, such configuration may slow down the operation. If you want to use an external DBMS, select **ODBC**. Setting the parameters for this variant is described in detail in Appendix B. The Description of the DBMS Settings. The Parameters of the DBMS Driver.
11. In the next dialog box dedicated to network configuration you can set up a network protocol for the Server (it is allowed to create only one protocol, more protocols can be set up later). To limit the local access to the Server, select the **Allow access to Dr.Web (R) Enterprise Console only** checkbox. The Installer, Agents and other Servers (in case of an existing anti-virus network built with **Enterprise Suite**) will not be able to access the Server. You can change these settings later through Console menu **Administration** -> **Dr.Web Enterprise Server** -> **Protocols**.

    Select the **Server detection service** checkbox, if you want the Server to answer broadcast and multicast queries of other Servers.

    To specify the default network settings click **Standard** in the bottom of the window. In case you want to limit the Server's operation only to the internal network interface – `127.0.0.1`, click **Restricted**. With such settings the Server can be administrated only from the Console launched on the same computer, and communicate only with the Agent launched on the same computer. In future after the Server settings have been checked out you will be able to change them.

    Click **Next**.
12. In the next window specify an administrator password. Click **Next**. (The window will not appear, if you are using an existing database).
13. Next you are recommended to instruct updating of the repository during the installation. To do this, select the **Update repository** checkbox. Click **Next**.
14. Click **Install**.

15. Further actions of the installation program do not require user intervention.
16. Once the installation is complete, click **Finish**.

Then install the anti-virus Console on the workplace of the anti-virus network administrator

1. Run the distribution file. A window for choosing the language of the **Installation Wizard** will open. Select the necessary language and click **Next**.
2. After a number of information messages a window with data about the program to be installed will open. Click **Next**.
3. A window with the text of the license agreement will open. You should read and accept the agreement. To continue the installation, in the bottom part of the window select **I accept the terms of the license agreement** and click **Next**.
4. Then confirm the installation catalog suggested by the program or select another one.
5. A window for choosing the installation mode will open. To install all components, select the **Complete** option button. To install only necessary components, select **Custom**. Click **Next**.
6. If you have chosen the custom type, a window to select components will open. In the list select the components to be installed. Click **Next**, when you are done.
7. The program will notify you when it is ready to install the Console. Click **Install**. After the installation is finished, click OK.

As a rule, the anti-virus Server is administrated by means of the anti-virus Console. Elements to facilitate adjusting and managing the Server are placed in the main Windows OS menu by the installation wizard.

On the **Programs menu**, the installation wizard creates a **Dr.Web®Enterprise Server** folder which contains the following items:

- `Console` — launches the anti-virus Console,
- `Documentation` — gives access to the documents of the anti-virus,
- `Server control` folder.

The Server control folder in its turn contains the commands to start, restart and shut down the Server, as well as the commands to set up the logging parameters and other Server's commands described in detail in Appendix H5. Dr.Web Enterprise Server.

The installation folder of the anti-virus Server (for OS Windows) has the following structure:

- `var` — contains the following subfolders:
  - `backup` — is meant for storing the backups of DBs and other critical data,
  - `extensions` — stores user scripts meant to automate the performance of certain tasks, all scripts are disabled by default,
  - `repository` – it is a so-called the updates folder; here updates of the virus databases, files of the anti-virus packages and files of the program's components can be found. It contains subfolders for the program components software which include subfolders for their versions depending on the OS. The folder should be accessible for writing to the **LocalSystem** user (under Windows OS) or the **drwcs** user (under UNIX OS) under which the Server is launched,
  - `templates` — contains a set of reports templates,
- `update-db` — contains scripts necessary to update the structure of Server's databases;
- `bin` — here reside executable files of the anti-virus Server;
- `webmin` —contains administrator's web-interface: documents, icons, modules;
- `etc` —contains the files where main program settings are stored;
- `Installer` — contains a program initializing the installation of the anti-virus Agent on a computer.

The content of the updates catalog `\var\repository` is automatically downloaded from the updates server through HTTP protocol according to the server's schedule, or the anti-virus network administrator can manually place the updates to the catalog.

2.2.2. Installing the Anti-Virus Server for UNIX® system-based Operating Systems

Installation should be carried out under Administrator account **(root).**

Package-based installation of the anti-virus Server on a UNIX system-based OS

1. To start installing the drweb-esuite package, use the following command:
   - for **FreeBSD** OS:
     `pkg_add` *<distribution_file_name.tbz>*
   - for **Solaris** OS:
     `bzip2 -d` *<distribution_file_name.bz2>* and then:
     `pkgadd -d` *<distribution_file_name>*
   - for **Linux** OS:
   - for **Debian** OS and **Ubuntu** OS:
     `dpkg -i` *<distribution_file_name.deb>*
   - for **rpm distribution kits**:
     `rpm -i` *<distribution_file_name.rpm>*

If the anti-virus Server is already installed on your computer, you can upgrade the software components. To do this, run the distribution kit with the command:

`rpm -U` *<distribution_file_name.rpm>*.

Also, there are so-called generic packages, which can be installed on any system including those which are not on the list of supported systems. They are installed by means of the installer included in the package:

```
tar -xjf <distribution_file_name.tar.bz2>
```

Then on behalf of the superuser run the following script - `./drweb-esuite-install.sh`

Installation can be cancelled at any time by sending any of the following signals — `SIGHUP`, `SIGINT`, `SIGTERM`, `SIGQUIT` and `SIGWINCH` (under **FreeBSD** OS changing the dimensions of the terminal window entails sending a `SIGWINCH` signal). When installation is cancelled, the changes to the file system roll back to the original state. When using an rpm package, installation can be interrupted by pressing CTRL + C.

Administrator name is **admin** by default.

2. Windows (the number and sequence of which can be different subject to the OS) containing information about the copyright and the text of the license agreement will open. To proceed with the installation, you should accept the license agreement.
3. If necessary, select the owner group and user. The same user will be the owner of the files of the anti-virus Server.
4. In the opened window select the key file for the Server (`enterprise.key`).
5. In the next window select the key file for the **ES** Agent (`agent.key`).
6. In case you are installing a Solaris system-compatible version, you will be asked to create a new database for the **ES** Server. If you are upgrading an already installed Server and you want to use the existing database, type **no**, press ENTER and select the path to the database. If you are installing the **ES** Server on your computer for the first time, press ENTER and specify the administrator (**admin**) password to access the Server (**root** is used by default).
7. Then (in case you are installing a Solaris system-compatible version) you will be asked to create new encryption keys. If you want to use existing keys (`drwcsd.pri` and `drwcsd.pub`), type **no**, press ENTER and specify the full path to the existing

keys. To create new encryption keys, press ENTER.

8. At the next stage, in case you are installing a version for **Debian** OS or **FreeBSD** OS, you need to create a password for the anti-virus network administrator. Enter your password and retype it for verification. If combinations are different and verification fails you should start over. Follow the instructions in appearing messages. The password should not be less than 8 characters (in the version for **FreeBSD** OS).
9. Then the program components will be installed on your computer. In the course of the installation you can be asked to confirm some actions as the administrator.

In the course of the installation of the **ES** Server for **FreeBSD** OS an `rc` script `/usr/local/etc/rc.d/drwcsd.sh` will be created.

- To manually stop the Server, use the command: `/usr/local/etc/rc.d/drwcsd.sh stop`.
- To manually start the Server, use the command: `/usr/local/etc/rc.d/drwcsd.sh start`.

During the installation of the **ES** Server for **Linux** OS and **Solaris** OS, an `init` script (`/etc/init.d/drwcsd`) for the launching and termination of the Server using `/opt/drwcs/bin/drwcs.sh` will be created. The latter cannot be launched manually.

Then install the anti-virus Console on the workplace of the anti-virus network administrator

1. Use the following command:
   - for **FreeBSD** OS:
     `pkg_add` <*distribution_file_name.tbz*>
   - for **Solaris** OS:
     `bzip2 -d` <*distribution_file_name.bz2*> and then:
     `pkgadd -d` <*distribution_file_name*>
   - for **Linux** OS:
   - for **Debian** OS and **Ubuntu** OS:
     `dpkg -i` <*distribution_file_name.deb*>
   - for **rpm distribution kits**:

```
rpm -i <distribution_file_name.rpm>
```

Also, there are so-called generic packages, which can be installed on any system including those which are not on the list of supported systems. They are installed by means of the installer included in the package:

```
tar -xjf <distribution_file_name.tar.bz2>
```

2. Then the software will be installed on your computer. In the course of the installation you can be asked to confirm some actions as the administrator.

2.3. Installing the Anti-Virus Agent on Computers

The anti-virus Agent should be installed under Administrator account of the respective computer.

If there is any anti-virus software installed on the computer, the installer will attempt to remove it before starting the installation. In case of a failure you will have to uninstall the anti-virus software yourself.

To install the anti-virus Agent on a computer, access from this computer the Installer subfolder of the Server's installation folder and run the **drwinst** program. The anti-virus Agent software (but not the anti-virus package) will be installed on the computer. The anti-virus package will be automatically installed after the workstation has been registered at the Server (read p. Getting Started) and restarted.

The drwinst command allows additional parameters. To view the installation log in the real time mode, use the `-interactive` parameter.

If multicasting is not used to detect the Server, it is strongly recommended to specify a domain name for the **ES** Server in the DNS service and use this name when installing the Agent:

`drwinst -interactive` *<anti-virus_Server_DNS_name>*.

It is especially useful in case you would like to reinstall the **ES** Server on a different computer.

Or you can expressly specify the Server's address as follows:

```
drwinst -interactive 192.168.1.3
```

Using the `-regagent` switch during the installation will allow you to register the Agent in the Add or Remove Programs list.

The `-useolddlg` switch used together with the `-interactive` switch allows the dialog with the Agent installation log to be displayed.

By default the `drwinst` instruction launched without parameters will scan the network for **ES** Servers and try to install the Agent from the first found Server.

When the **drwinst** program is run with the `-config` switch a dialog box will open, which allows to change the default settings of the installer and some of the basic default settings of the Agent and to specify the components of the anti-virus package to be installed (the settings available in the interface of the network installer are expanded in p. Remote Installation of the Anti-Virus Agent).

You can also install the **ES** Agent remotely with the help of the anti-virus Console or the facilities of **Active Directory** (see p. Remote Installation of the Anti-Virus Agent).

2.4. Remote Installation of the Anti-Virus Agent (for Windows® OS)

The **Dr.Web® ES** anti-virus allows to detect the computers which are not yet protected by **Dr.Web® ES**, and in certain cases to install such protection remotely.

Remote installation of anti-virus Agents is only possible on workstations operated by Windows NT OS, Windows 2000 OS, Windows XP Professional OS, Windows 2003 OS, Windows Vista OS.

To install the anti-virus software on workstations, you must have administrator rights on the correspondent computers. The anti-virus Console should be launched under Windows 2000 OS, Windows XP Professional OS, Windows 2003 OS, Windows Vista OS.

Remote installation and removal of the Agent software is possible within a local network only and requires administrator's rights in the local network, and checkout of the anti-virus Server requires full access to its installation catalog.

It is necessary to share the location of the Agent Installer file `drwinst.exe` and the public encryption key `drwcsd.pub` on the network.

In case the Server is running under **UNIX** OS, for remote installation a Console under OS **Windows** and the **Samba** file server are required.

2.4.1. Installing the Agent Software through the Console

When the Console is launched, the catalog of the anti-virus network in its main window displays only those computers which are already included into the anti-virus network. The program allows also to discover computers which are not protected with **Dr.Web® Enterprise Suite** and to install anti-virus components remotely.

To quickly install the Agent's software on workstations, it is recommended to use Network Scanner which searches for computers by IP addresses. **To do this**

1. On the **Administration** menu of the Console, select **Network scanner**. A Network scanner window with no data loaded will open.
2. In the **Networks entry** field specify networks separated by spaces. If necessary, change the port and the timeout value.
3. Click  . The catalog (hierarchical list) of computers demonstrating where the **Dr.Web® ES** anti-virus software is installed will be loaded into this window.
4. Unfold the catalog elements corresponding to workgroups (domains).
   - The work groups containing inter alia computers on which the **Dr.Web® ES** anti-virus software can be installed are marked in the catalog with the icon  .

- Other groups containing protected or unavailable by network computers are designated with the icon  .
- The computers on which the anti-virus software is not installed are marked with a red icon  .
- The computers to which the administrator has no access rights are marked in the catalog with a grey icon  .
- Workstations with installed anti-virus software are marked with a green icon  .

You can also unfold catalog items corresponding to computers and check what program components are installed there.

5. Select an unprotected computer (or several unprotected computers) in the **Network scanner** window.
6. On the context menu of this computer, select **Install Dr.Web® Enterprise Agent**.
7. A window for a remote installation task will open.
8. In the **Dr.Web® Network Installer settings** section you can set up the installation parameters of the Agent's software.
9. If necessary, edit the target computer name in the **Computer names** entry field. By default in the **Server** field the IP address or the DNS name of the anti-virus Server to which the Console is connected are given. In the **Installer executable** field the full name of the network installer is specified. If necessary, edit it and reselect the public key in the **Public key** field.

When the Agent software is installed on several computers at the same time you can specify several IP addresses or computer names separated by spaces. You can also specify entire networks as `192.168.1.0/24` or ranges of IP addresses as `192.168.2.1-192.168.2.255`. Besides, you can enter computer domain names instead of the IP addresses.

10. By default the Agent's software will be installed to `C:\Program Files\DrWeb Enterprise Suite`. If necessary, specify another location in the **Install path** field.
11. If necessary, type the network installer command line parameters in the **Arguments** field (read more in Appendix H4. The Network Installer). In the **Log level** field specify the level of detail.

12. If you are going to install through **Windows Scheduler**, you need to enter authorization parameters.
13. Having set up all the necessary parameters of the **Dr.Web® Network Installer settings** section, click **Next**.
14. On the **Dr.Web® Enterprise Agent settings** tab you can select the components of the anti-virus package, specify the interface language, allow traffic encryption and compression, set the parameters of the log, etc.
15. After all necessary parameters have been specified, click **Install**.
16. The status of the installation will be displayed on the **Operation process** tab in accordance with the selected level of detail.
17. The anti-virus Agent will be installed on the selected workstations, then after the workstation has been authorized at the Server (read Getting Started) and restarted other anti-virus components will be installed.

You can also view the list of local network computers and install the anti-virus software on them through **Windows Network Browser**. In this case the actions are similar to the above, plus computers unavailable at the moment but information on which is stored in the **Windows Master Browser** service will be also displayed and marked with the icon  . Computers operated by Windows 98, Windows Me OS will be shown as unprotected if the **File and printer sharing for Microsoft Networks** and the **I want to be able to give others access to my files** modes are not enabled.

In case an anti-virus network is basically created and it is necessary to install the Agent's software on certain computers, it is recommended to use **installation via network**:

1. On the **Administration** menu, select **Network install**. A window **Dr.Web® Enterprise Agent Installation** will open.
2. Further steps are similar to **8-17** above.

2.4.2. Installing the Agent Software through Active Directory

If the **Active Directory** service is used in the LAN, you can remotely install the anti-virus Agent on workstations using this service. To do this

1. Download a copy of the anti-virus Agent installer for networks with **Active Directory** at http://www.drweb.com/.
2. Install the anti-virus Agent on the local network server supporting the **Active Directory** service. This can be made in the command line mode **(A)** or in the graphic mode of the installer **(B)**.

(A) To set all necessary installation parameters in the command line mode

Issue the following command with all necessary parameters and the obligatory parameter `/qn` which disables the graphic mode:

```
msiexec /a ES_Agent.msi /qn [parameters]
```

Obligatory parameters:

`/qn` – disable the graphic mode. With this switch the following parameters are to be specified:

- `ESSERVERADDRESS=`*<DNS_name>* - set the address of the anti-virus Server to which the Agent is to be connected. For the possible formats see Appendix E3. The Addresses of Dr.Web Enterprise Agent/ Installer.
- `ESSERVERPATH=`*<path_filename>* - specify the full path to the public encryption key of the Server and the file name (by default `drwcsd.pub` in the `Installer` subfolder of the Server installation folder).
- `TARGETDIR` – set the path to the Agent image (modified instalation package). The path should be given in the network addresses format even if the catalog is a locally accessible resource; the catalog should be accessible from the target stations.

Before administrative installation the target folder for the Agent image (see the `TARGETDIR` parameter) should not contain the anti-virus Agent Installer for networks with **Active Directory** (`ES_Agent.msi`).

Optional parameters

The **0** value of the parameters below orders to cancel the installation of the respective **Dr.Web®** anti-virus component, and **1** (default) enables the installation. For more about anti-virus components see p. About Dr.Web Enterprise Suite.

- `SPIDERML=0` – do not install **SpIDer Mail for Windows Workstations**.
- `SPIDERNT=0` - do not install **SpIDer Guard for Windows Workstations** NT/2000/XP/2003/Vista.
- `SPIDERMLS=0` - do not install **SpIDer Mail for Windows Servers**.
- `SPIDERNTS=0` - do not install **SpIDer Guard for Windows Servers**.
- `SCANNER=0` - do not install **Scanner for Windows**.

Examples:

```
msiexec /a ES_Agent.msi /qn
ESSERVERADDRESS=servername.net
ESSERVERPATH=\\win_serv\drwcs_inst\drwcsd.pub
TARGETDIR=\\comp\share SPIDERMLS=0 SPIDERNTS=0
```

```
msiexec /a ES_Agent.msi /qn
ESSERVERADDRESS=192.168.14.1
ESSERVERPATH="C:\Program Files\DrWeb Enterprise
Server\Installer\drwcsd.pub"
TARGETDIR=\\comp\share
```

These parameters can alternatively be set in the graphic mode of the installer.

(B) To set all necessary installation parameters in the graphic mode

Before administrative installation, make sure that the target folder for the Agent image does not contain the anti-virus Agent Installer for networks with **Active Directory** (`ES_Agent.msi`).

1. Issue the command `msiexec /a ES_Agent.msi`.
2. An **InstallShield Wizard** window with information on the program selected for installation will open. Click **Next**.

The Agent Installer uses the language specified in the language settings of the computer

3. In the next window, specify the DNS name (preferred form) or the IP address of the **ES** Server (see Appendix E3. The Addresses of Dr.Web Enterprise Agent/ Installer). Specify the location of the public key file of the Server (`drwcsd.pub`). Click **Next**.
4. In the next window the components of the **Dr.Web® Anti-Virus** are listed. **Dr.Web® Enterprise Scanner** is installed by default, the rest may be cancelled. For that, clear the respective checkboxes. Click **Next**.
5. In the next window type the name of a network catalog, to which the image of the Agent is planned to be written. The path should be specified in the network addresses format even if the catalog is a locally accessible resource; the catalog should be accessible from the target stations. Click **Install**.

Next on a local network server, where Active Directory administrative tools are installed, appoint installation of the package on selected workstations

1. In **Control Panel**, select **Administrative Tools** -> **Active Directory Users and Computers**.
2. In the domain containing the computers on which the anti-virus Agents are to be installed, create an organizational unit (hereinafter OU), name it, for example, **ES**, and include the computers, on which the Agent is to be installed, into this unit.

3. On the OU context menu, select **Properties**. An **ES Properties** window will open.
4. Go to the **Group Policy** tab. Click **Add** and create an element named **ES** policy. Double-click it.
5. A **Group Policy Object Edi**tor window will open. In the hierarchical tree, select **Computer Configuration** -> **Software Settings** -> **Software Installations**.
6. On the context menu of **Software Installations**, select **New**. In the opened submenu select **Package**.
7. Next specify the folder, in which the Agent image was created during the administrative installation above (the path should be specified in the network addresses format even if the catalog is a locally accessible resource). Click **OK**.
8. A Deploy Software window will open. Select the Assigned option. Click **OK**.
9. In the **Group Policy Object Editor** window, select the added package. On the context menu of this element, select **Properties**.
10. In the opened package properties window, select the **Deployment** tab. Click the **Advanced** button.
11. An **Advanced Deployment Options** window will open. Select the **Ignore language when deploying this package** checkbox. Click **OK**.
12. Click **OK**.
13. The anti-virus Agent will be installed on selected computers at their next registration in the domain.

2.5. Removing the Dr.Web ES Anti-Virus

2.5.1. Uninstalling the ES Software for Windows® OS Locally or through the Console

When uninstalling the program completely, do not remove the Server in the first place. First remove the **ES** Agent.

To remove the **ES** Agent software from a workstation, run the `drwinst` instruction with the `–uninstall` parameter (or with the `–uninstall –interactive` parameters, if you want to control the process) in the installation folder of the anti-virus Agent (by default `C:\Program Files\DrWeb Enterprise Suite`).

Example:

```
drwinst –uninstall –interactive
```

When the Agent is being uninstalled, the anti-virus package is also removed from your computer.

To successfully remove the Agent, make sure the `uninstall.rexx` file resides in the installation folder of the anti-virus Agent. The file is placed to the folder during the Agent's installation, but, if the installation had failures, it can be missing in the folder (you will be notified about it during the deinstallation in the above-specified mode). In this case, copy the file from the `var\repository\20-drwagntd\win` subfolder of the Server's installation folder.

To uninstall the anti-virus software of workstation through the Console (for Windows NT OS, Windows 2000 OS, Windows XP OS, Windows 2003 OS, Windows Vista OS only), in the catalog of the anti-virus network select the necessary group or certain anti-virus stations. On the context menu, select **Deinstall Dr.Web® Agent**. The Agent's software and the anti-virus package will be removed from the workstations selected.

Remote installation and removal of the Agent software is possible within a local network only and requires administrator's rights in the local network

In case the Agent's removal is instructed when there is no connection between the anti-virus Server and the anti-virus workstation, the Agent software will be uninstalled from the selected computer once the connection is recovered.

The Server and Console software is removed through standard Windows OS tools by means of the **Add or Remove Programs** element in **Control Panel**.

2.5.2. Uninstalling the ES Agent Software through Active Directory

1. In **Control Panel**, select **Administrative Tools** -> **Active Directory users and computers**.
2. Right-click your **ES** organizational unit in the domain. On the context menu, select **Properties**. An **ES Properties** window will open.
3. Go to the **Group Policy** tab. Select **ES policies**. Double-click the item. A **Group Policy Object Editor** window will open.
4. In the hierarchical list, select **Computer configuration** -> **Software settings** -> **Software installations** -> **Package**. Then on the context menu, select **All tasks** -> **Uninstall** -> **OK.**
5. On the **Group Policy** tab, click **OK.**
6. The anti-virus Agent will be removed from the stations at the next registration in the domain.

2.5.3. Uninstalling the Server Software for UNIX® system-based Operating Systems

Deinstallation should be carried out under the administrator account (**root**).

On Solaris OS before initializing deinstallation stop the **ES** Server through the following command: `/etc/init.d/drwcsd stop`.

To remove the Server installed from packages

1. To uninstall the **ES** Server software, enter the following command:
   - for **FreeBSD** OS: `pkg_delete drweb-esuite`
   - for **Solaris** OS: first stop the Server:
     - **Solaris10** OS: `svcadm disable system/drwcsd`

- **Solaris9** OS: `/etc/init.d/drwcsd stop`
- Then enter the command: `pkgrm DWEBesuit`

- for **Linux** OS:
- for **Debian** OS and **Ubuntu** OS: `dpkg -r drweb-esuite`
- to remove the Server software, installed from an **rpm distribution kit**: `rpm –e drweb-esuite`
- to remove the Server software, installed from a **generic package**: run the `drweb-esuite-uninstall.sh` script.

Deinstallation can be interrupted at any time by sending any of the following signals to the process: `SIGHUP`, `SIGINT`, `SIGTERM`, `SIGQUIT` and `SIGWINCH` (on **FreeBSD** OS, changing the dimensions of the terminal window entails sending a `SIGWINCH` signal). Deinstallation should not be interrupted without necessity or it should be done as early as possible.

2. On **Solaris** OS, you will be asked to confirm that you really want to uninstall the software and agree to run the deinstallation scripts on behalf of the administrator (**root**).

The **ES** Server software will be removed.

On **FreeBSD** OS and **Debian** OS, the Server operations will be immediately terminated, the database, key and configuration files will be copied to `${HOME}/drwcs/` (as a rule, it is `/root/drwcs/`) under **Debian** OS. Under **FreeBSD** OS, you will be requested to enter a path, by default it is `/var/tmp/drwcs`.

On the **Solaris** OS operating environment, after the Server has been removed, the database, key and configuration files will be copied to the `/var/tmp/DrWebES` folder.

Chapter 3: The Components of an Anti-Virus Network and Their Interface

3.1. The Anti-Virus Server

An anti-virus network built with **Dr.Web® ES** must have at least one anti-virus Server.

The anti-virus Server is a memory-resident component. You can shut it down from the Console or through the correspondent Server control command on Windows OS **Programs menu**. The anti-virus Server software is developed for various OS's – Windows NT OS, Windows 2000 OS, Windows XP OS, Windows 2003 OS, Windows Vista OS, Linux OS, FreeBSD OS and Solaris OS.

The anti-virus Server performs the following tasks:

- installs the Agent software and anti-virus packages on a selected computer or a group of computers;
- requests the version number of the anti-virus package and the creation dates and version numbers of the virus databases on all protected computers;
- updates the content of the centralized installation folder and the updates folder;
- updates virus databases and executable files of the anti-virus packages, as well as executable files of the program on protected computers.

Communicating with anti-virus Agents, the anti-virus Server collects and logs information on operation of the anti-virus packages. Information is logged in the general log file implemented as a database. In small networks (not more than 100-200 computers) an internal database can be used. In larger networks it is recommended to use an external database.

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

- versions of the anti-virus packages on protected computers,

- time and date of the software installation and update on workstations,
- versions and dates of virus databases updates,
- OS versions of protected computers, processor type, OS system catalogs location, etc.,
- configuration and settings of anti-virus packages,
- data on virus events, including names of detected viruses, detection dates, actions, results of curing, etc.

The anti-virus Server notifies the administrator on virus events occurring on protected computers by e-mail or through the Windows OS standard notification system. You can set the alerts as described in p. Setting Alerts.

To increase the reliability and productivity of an anti-virus network and distribute the computational load properly, the **Dr.Web® ES** anti-virus can also be used in the multiserver mode. In this case the Server software is installed on several computers.

The anti-virus Server as it is has no interface. Basic instructions necessary to manage the Server are listed in the Server control folder. As a rule, the anti-virus Server can be managed through the anti-virus Console, which acts as an interface for the Server.

3.2. The Anti-Virus Console and the In-Built Web Server

The *anti-virus Console* is an administration tool which is used to manage the anti-virus Server(s). Once connection to the anti-virus Server is established, the anti-virus Console allows to edit settings and launch tasks for every anti-virus workstation connected to this Server.

The anti-virus Console is a platform-independent application and can be installed on a computer with any OS supporting the Java virtual machine. The connection between the Console and the Server is provided via TCP/IP or IPv6.

For the Console to connect through the proxy-server, it is necessary to allow the proxy the `CONNECT` method to the corresponding port.

The anti-virus network is administrated via the Console's interface.

The Console main window includes the following elements (see Figure 3-1):

- Main menu bar;
- Toolbar;
- Hierarchical list (catalog) of the anti-virus stations and groups;
- Control panel (to enable/disable displaying this panel, use Console settings);
- Search panel;
- Traffic monitor (to enable/disable displaying this bar, use Console settings);
- Memory usage bar (to enable/disable displaying this bar, use Console settings);
- Status bar.

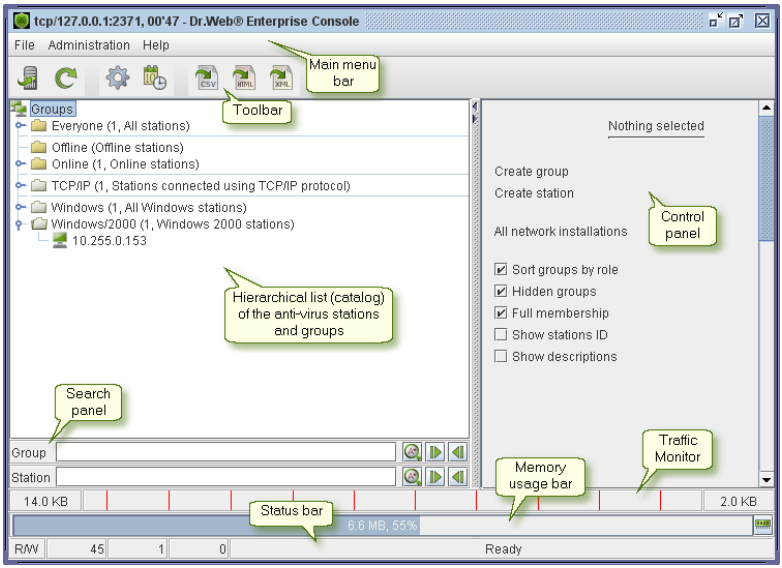

Figure 3-1. The Console's main window

Server parameters can be set both through the main menu bar and the toolbar.

Items on the anti-virus network catalog can be set up from the context menu of these elements and from the control panel, which duplicates the context menu of a selected item.

The Console operates in a standard graphical user interface, which is an analogue to that used in Windows OS and in the graphical environments of UNIX system-based OS's. The tasks solved with the help of this interface are described in the next Chapters. Below is given only a brief overview of the main menu bar elements and toolbar buttons used to administer the program.

The main menu bar includes the following menus:

- **File**,
- **Administration**,
- **Help**.

The File menu contains the following items:

- **Connect to Dr.Web® Enterprise Server** — instructs to connect the Console to the Server; if the Console is connected to a Server, it will be disconnected from the current Server before connecting to a new Server;
- **Dr.Web® Enterprise Console settings** — allows to specify the parameters of connection to the Server, the interface language, the level of detail of the Console's log, etc.;
- **Disconnect from Dr.Web® Enterprise Server** — instructs to disconnect from the current Server;
- **Exit** — instructs to disconnect from the Server and terminate the program.

The Administration menu contains the following items:

- **Administrator accounts** — allows to add, edit or delete administrator accounts of the anti-virus network (read p. Managing Administrator Accounts);
- **Configure Dr.Web® Enterprise Server** — opens a window with main Server's settings (read p. Setting the Server Configuration);
- **Configure repository** — allows to configure settings for each product in the repository (for more on the repository, read p. Administration of the Server Repository and further);

- **Dr.Web® Enterprise Server schedule** — opens a window for scheduling tasks for the Server (read p. Setting the Server Schedule);
- **Neighborhood** – opens a window for managing connections among the **ES** Servers in a multi-server anti-virus network (read p. Setting Connections Between the Servers of an Anti-Virus Network);
- **Edit templates** – opens a window of the editor of notifications templates (read p. Setting Alerts);
- **Database** — allows to remove the data about anti-virus workstations of a certain period of time and the anti-virus workstations themselves from the database;
- **Alerts** — allows to view Server's messages (read p. Receipt of Alerts);
- **Jobs execution log** — contains the list of scheduled tasks at the Server with comments and the completion marked;
- **Show unapproved stations** — opens a window with the list of unapproved stations (read p. New Stations Approval Policy);
- **Dr.Web® Enterprise Server Statistics** — viewing the statistics of the Server's operation (read p. Server Statistics);
- **Show Dr.Web® Enterprise Server log** — opens a window for modifying the Server's log (read p. Keeping the Log on the Server. Viewing the Log);
- **Remote data** — displays information on anti-virus network operation received from other Servers (read p. Using an Anti-Virus Network with Several Servers);
- **Dr.Web® Enterprise Server information** — opens a window with detailed information on the version of the anti-virus Server;
- **Check for updates** — opens a window to immediately check for software updates (read p. Scheduled Updates);
- **Restart Dr.Web® Enterprise Server** — reboots the current anti-virus Server (the connection between the Server and the Console will be interrupted and restored);
- **Shutdown Dr.Web® Enterprise Server** — stops the anti-virus Server to which the Console is connected;

- **Network browser** – this component scans the local network to define if and what **ES** anti-virus software for workstations is installed on the computers. Network browser allows to quickly install the Agent software in the local network and establish an anti-virus network;
- **Network scanner** — allows to set the list of networks, scan networks for installed anti-virus software and determine the state of protection of computers, as well as install the software (see p. Network Browser and Network Scanner);
- **Network install** — allows to simplify installing the Agent's software on certain workstations (see p. Network Browser and Network Scanner).

The Help menu contains the following items:

- **Documentation** – opens a window with the **Dr.Web Enterprise Suite Administrator Manual**;
- **Doctor Web, Ltd.** – leads to the home page of the official site of **Dr. Web, Ltd**: http://www.drweb.com;
- **Doctor Web, Ltd. news** – opens the web page with company's news: http://info.drweb.com/;
- **Customer Support Center** – opens the clients on-line support section: http://support.drweb.com/;
- **Ask Customer Support** – leads to the web form where you can ask a question or upload a suspicious file for analysis: http://support.drweb.com/request/;
- **About** – opens a window with information on the versions of the used anti-virus and system software, the license expiry date, the number of licensed stations, etc.

Under UNIX OS, to view the web resources from the Help menu, the user environment variable `$BROWSER` is applied, and if it is not set, the value `Firefox` is taken by default.

Toolbar buttons:

- Connect to another Dr.Web® Enterprise Server,
- Refresh shown data,
- Configure connected Dr.Web® Enterprise Server,

- Change connected Dr.Web® Enterprise Server schedule,
- Save shown data in CVS format,
- Save shown data in HTML format,
- Save shown data in XML format.

When the Console is started on Windows OS an icon appears in the notifica tion area of the Taskbar.

You can perform the following through the icon:

- Right-click the icon to open the context menu.
- Left-click it to minimize open windows of the Console if there are any open. Otherwise restores all windows.
- Left-click it twice to restore the minimized windows.
- Or middle-click it to do the same.

To ensure quicker access, some menu items were added to the context menu of the Console icon.

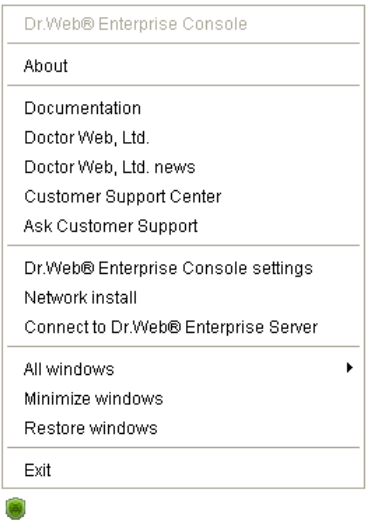

Figure 3-2. The icon and the context menu of the anti-virus Console

The anti-virus Console allows to set up not only the parameters of the Server, but also the parameters of connected workstations, which are stored on the Server, and the configuration of the whole network.

Select an element you need to configure in the list and view the available settings on its context menu.

The **search panel** facilitates searching necessary elements. The panel allows to find all groups or stations whose names coincide with the combination specified in the search line.

To quickly access most main menu items and subitems, use the hot keys listed in Table 3-1.

Table 3-1. The hot keys to manage the anti-virus Console

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® Enterprise Server
ALT-Y	Administration — Configure repository — Entire repository settings
ALT-S	Administration — Dr.Web® 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® Enterprise Server log
ALT-A	Administration — Unapproved stations

Hot key	Menu — submenu item
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
F5	Refresh displayed data

An additional instrument to manage the anti-virus network and set up the Server is the **in-built Web Server**. The Web Server functions as a web console. The following items are available on its menu:

- Information,
- Documentation,
- License,
- Repository,
- Help.

The Web Server is available on the computer on which the anti-virus Server is installed at port `9080` http and `9081` https.

For example,

```
http://IP address(or domain name):9080
```

or

```
https://IP address(or domain name):9081
```

If you connect through https protocol (secure SSL connection), the browser requests you to approve the server certificate. Warnings and indications of distrust to the certificate may display, because the certificate is unknown to your browser. You need to approve the certificate to connect to the web-server.

Some browsers (for example, **FireFox 3**) report errors when connecting through https and refuse connection to the web-server. To solve this problem, add the web-server to the list of exceptions by clicking Add site in the warning message. This allows connection to the web-server.

3.3. Network Browser and Network Scanner

The anti-virus Server comprises **Network Browser** and **Network Scanner** among other tools.

It is planned to exclude **Network Browser** from the next Dr.Web® ES versions.

Two similar tools are used because of the necessity to keep different versions of **Dr.Web® ES** compatible. At present the anti-virus Server comprises both tools **Network Browser** and **Network Scanner**, as it is possible that at the same time an anti-virus network can include workstations with the Agent **4.33** and workstations already upgraded to **4.44**.

These tools function as follows:

- Scan (browse) the network for workstations.
- Detect **Dr.Web® ES** Agents on stations.
- Install the anti-virus Agent on the detected stations as instructed by the administrator. **ES** Agent installation is described in detail in p. Installing the Agent Software through the Console (the same steps for **Network Browser** as for **Network Scanner**).

To scan (browse) the network

1. On **Dr.Web® ES** Console menu, select **Administration** and the respective item (**Network Scanner** or **Network Browser**).
2. In the settings window, set the necessary parameters (see below).
3. Click the **Refresh** button to launch network scanning.

4. When scanning is completed you will be shown a list of stations, with current **ES** Agent installations marked.

Network Browser and **Network Scanner** perform the above operations with certain functional difference.

Main difference:

- Parameters used at network scanning (browsing).
- Interaction with anti-virus Agents (Agent version, ways of detection of installed Agents).

See more detailed description below.

Network Browser

Scanning start parameters

When activating **Network Browser** you can specify the names of workgroups and domains to be ignored at browsing.

Interaction with anti-virus Agents

Network Browser is included in **Dr.Web® ES 4.44** and higher for reverse compatibility with **Dr.Web® ES 4.33**.

Network Browser can detect only Agents **4.33** and cannot interact with the Agents of version 4.44.

After Agent v. **4.33** has been installed on a protected station, it creates a resource, whose name contains respective identification data. This identification resource is created network-available, which enables the **Browser** to detect it when scanning the network. **Browser's** conclusion, whether there is an Agent on the station is based on the availability of the identification resource.

In case of absence of remote access tools or deletion of the identification resource by the station administrator, the **Browser** will not be able to find the necessary identification resource and therefore make a false conclusion that there is no Agent installed on the workstation.

Network Scanner

Scanning start parameters

The following search parameters can be set at start of **Network Scanner**:

- IP addresses of the networks to be scanned (see Appendix E. The Specification of Network Addresses);
- Port to call the Agent.

Interaction with anti-virus Agents

Network Scanner has been included in **Dr.Web® ES** starting from version **4.44**.

Network Scanner can detect the Agents of version **4.44** and cannot interact with Agents **4.33**.

Anti-virus Agents **4.44** installed on protected stations process respective calls of **Network Scanner** received at a certain port. By default it is port `udp/2372`. Correspondingly, it is the default port offered by the Scanner to call at. **Network Scanner** decides whether there is an Agent on the workstation based on the assumption of the possibility to exchange information with the station (request-response) through the specified port.

If the station is forbidden (for example, by a firewall) to accept packages at `udp/2372`, the Agent will not be detected and consequently **Network Scanner** considers that there is no Agent installed on the station.

3.4. The Anti-Virus ES Agent

Workstations are protected from virus threats by the **Dr.Web®** anti-virus packages designed for correspondent OS's.

The packages are installed and operated by anti-virus Agents. The Agents are usually installed by administrators (pp. Installing the Anti-Virus Agent on Computers and Remote Installation of the Anti-Virus Agent (for Windows OS)) and constantly reside in the memory of protected workstations. They maintain connection to the anti-virus Server(s), thus enabling administrators to configure anti-virus packages on workstations from the Console, schedule anti-virus checks, see the statistics of anti-virus components operation and other information, start and stop remotely anti-virus scanning, etc.

Anti-virus Servers opportunely download updates and distribute them to the Agents connected to them.Thus due to **ES** Agents anti-virus protection is implemented, maintained and adjusted automatically, without user intervention and irregardless of user's computer skills.

In case an anti-virus station is outside the anti-virus network the anti-virus Agent uses the local copy of the settings and the anti-virus protection on that computer retains its functionality (up to the expiry of the user's license), but virus databases and program files are not updated.

Updating of mobile Agents is described in p. Updating Mobile Agents.

The anti-virus Agent is designed to perform the following:

- to execute tasks set by the anti-virus Server (to install and update the anti-virus package, launch scanning, etc.), if necessary, anti-virus package files are run through a special interface;
- to send the results of performed tasks to the anti-virus Server;

- to send notifications to the anti-virus Server on preset events that occur during the operation of the anti-virus package.

Every anti-virus Agent is connected to an anti-virus Server and is included in one or several groups registered on this Server (for more, see p. Groups. Preinstalled Groups, Creating and Removing Groups). The Agent and the anti-virus Server communicate through the protocol used in the local network (TCP/IP, IPX or NetBIOS).

Hereinafter a computer on which the **ES** Agent is installed as per its functions in the anti-virus network will be called a *workstation*, while in the local network it can be functioning both as a server or a workstation.

When run in the Windows OS environment, the anti-virus Agent displays an icon in the Taskbar.

Some administrative functions over the anti-virus workstation are accessible through the context menu of this icon, which is shown in Figure 3-3.

Figure 3-3. The context menu of the anti-virus Agent

The range of settings accessible through the context menu of the Agent icon depends on the configuration of the workstation specified by the administrator.

You can find info about the set of Agents' parameters and description of corresponding administrative functions in the ES Agent's help.

Mind that by selecting **Exit** you only remove the icon from the notification area of the Taskbar. The Agent will remain running.

To terminate the program itself, type

```
net stop drwagntd
```

in the command line. It is not recommended to stop the Agent because in this case the anti-virus package software will not be updated and the Server will not receive any information on the status of the workstation, although the permanent protection will not be disabled.

The Agent will be launched automatically at computer restart. To launch the program back without restarting your computer, type

```
net start drwagntd
```

in the command line. The permanent protection will be restored.

The icon's visual representation listed in the Table 3-2.

Table 3-2. The icon's visual representation

Icon	Description	Action
	The black picture on the green background.	The Agent is operating normally and is connected to the Server.
	A crossed Server icon on the basic background.	The Server is unavailable.
	An exclamation mark in a yellow triangle over the icon.	The Agent requests to restart the computer.
	The background of the icon changes color from green to red.	An error occurred during updating of the package components.

Icon	Description	Action
	The background of the icon is constantly red.	The Agent is stopped or not running.
	The background of the icon is yellow.	The Agent is working in the mobile mode (for more, see p. Updating Mobile Agents).

About the settings of the anti-virus Agent read p. Editing the Parameters of the Anti-Virus Agent.

3.5. The Interaction Scheme of the Components of an Anti-Virus Network

The Figure 3-4 describes a general scheme of an anti-virus network built with **Dr.Web® ES.**

The scheme illustrates an anti-virus network built with only one Server. In large companies it is worthwhile installing several anti-virus Servers to distribute the load between them.

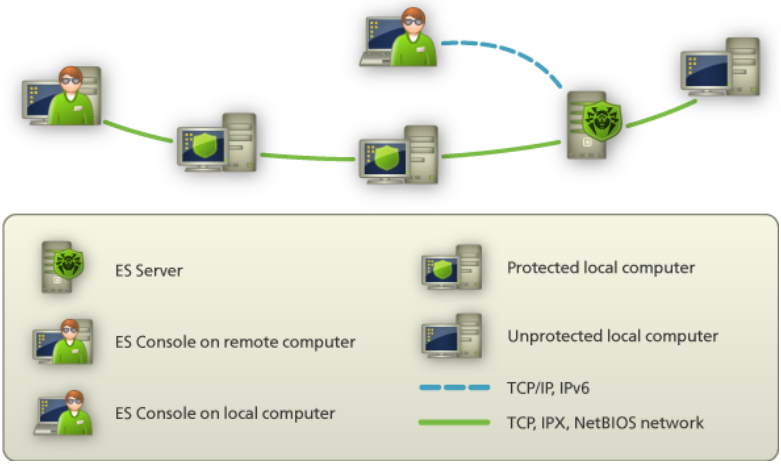

Figure 3-4. The physical structure of the anti-virus network

In this example the anti-virus network is implemented within a local network, but for the installation and operation of **ES** and anti-virus packages the computers need not be connected within any local network, Internet connection is enough.

When an anti-virus Server is launched the following sequence of commands is performed:

- anti-virus Server files are loaded from the bin catalog,
- the Server's Scheduler is loaded,
- the content of the centralized installation catalog and update catalog is loaded, notification system is initialized,
- Server database integrity is checked,
- Server Scheduler tasks are performed,
- the Server is waiting for information from anti-virus Agents and commands from Consoles.

The whole stream of instructions, data and statistics in the anti-virus network always goes through the anti-virus Server. Anti-virus Consoles exchange information only with Servers. Based on Console's commands, Servers transfer instructions to anti-virus Agents and change the configuration of workstations. Connection between a Console and a certain Server is established only after an anti-virus network administrator is authenticated by his login name and password on the given Server.

Thus, the logical structure of the fragment of the anti-virus network looks as in the Figure 3-5.

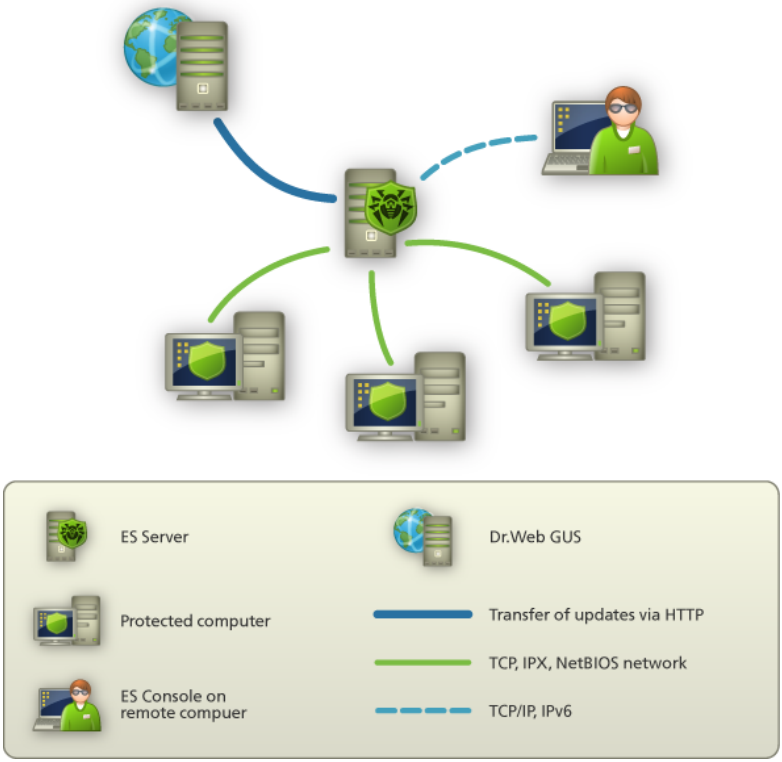

Figure 3-5. The logical structure of the anti-virus network

The Server sends to workstations and receives from them (a thin continuous line in the Figure 3-5) the following information through one of the supported network protocols (TCP, IPX or NetBIOS):

- Agents' requests for the centralized schedule and the centralized schedule of workstations,
- settings of the Agent and the anti-virus package,
- requests for scheduled tasks to be performed (scanning, updating of virus databases, etc.),
- files of anti-virus packages — when the Agent receives a task to install them,
- software and virus databases updates — when an updating task is performed,
- Agent's messages on the configuration of the workstation,
- statistics (to be added to the centralized log) on the operation of Agents and anti-virus packages,
- messages on virus events and other events which should be logged.

The volume of traffic between the workstations and the Server can be quite sizeable subject to the settings and the number of the workstations. Therefore the program complex **Dr.Web® ES** provides for the possibility to compress traffic. See the description of this optional mode in p. Traffic Encryption and Compression below.

Traffic between the Server and the anti-virus Agent can be encrypted. This allows to avoid disclosure of data transferred via the described channel as well as to avoid substitution of software downloaded onto workstations. By default traffic encryption is enabled (for more, please read p. Traffic Encryption and Compression).

From the update web server to the anti-virus Server (a grey thick continuous line in the Figure 3-5) files necessary for replication of centralized catalogs of installation and updates as well as overhead information on this process are sent via HTTP. The integrity of the information (**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 (a dashed line in Figure 3-5) data about the configuration of the Server (including information about the network layout) and workstations settings are passed via TCP/IP or IPv6. This information is visualized on the Console, and in case a user (an anti-virus network administrator) changes any settings, the information about the changes is transferred to the Server.

Connection between a Console and a Server is established only after an anti-virus network administrator enters his login and password.

Chapter 4: Getting Started. Launching the Anti-Virus Console and Establishing a Simple Anti-Virus Network

Before using the anti-virus software it is recommended to change the settings of the backup folder for the Server's critical data (see p. Setting the Server Schedule). It is advisable to keep the backup folder on another local disk in order to reduce the risk of losing Server's software files and backup copies at the same time.

The Server is started automatically once the installation of the Server is complete. To set up the Server and configure the anti-virus software, the anti-virus Console should be run on the computer of the administrator and a connection to the Server should be established. Examples below describe the launch of the anti-virus Console from the administrator computer operated by Windows OS. For other operating systems the actions are the same.

The program files of the Console as well as launching scripts for certain OS's reside in the Console's installation folder. This folder can be made network-accessible for other administrators.

The Console should not be placed to a folder the path to which contains an exclamation mark (!).

To launch the anti-virus Console:

1. If you work under a **UNIX** system-based OS, run the script `drwconsole.sh`.
2. If you work under OS **Windows**, run `drwconsole.exe`.
3. A window for logging in on the Server will open.

- If no Server address is specified in the **Server** entry field, type it or use the  button. A search window will open.

- In the entry fields in the bottom of the window a search template is specified. Edit it, if necessary (see Appendix Appendix E. The Specification of Network Addresses). Click **Search**. The list of found Servers will be displayed in the upper part of the window. Select the necessary Server in this list and click **Select**.
- Enter the login and the password of an anti-virus network administrator. The name **admin** and the password **root** are suggested by default during the installation; it is advisable to change the password, read p. Managing Administrator Accounts.
- Click **Login**.

Registration at the Server is impossible if the traffic encryption and compression settings of the Console and the Server are incompatible. If this is the cause of the registration failure, on the **File** menu, select **Dr.Web® Enterprise Console settings**. A window for editing Console settings will open. Go to the **Communication** tab. Select the same settings in the **Encryption mode** and the **Compression mode** drop-down lists as set for the Server and click **OK**. (To view the Server's configuration from a connected Console, on the **Administration** menu, select **Configure Dr.Web® Enterprise server**, then select the **General** tab). The default parameters of these settings for the Console and the Server are compatible; the original compatibility may be broken if you have changed one of these settings. Registration is also impossible if your Console version is incompatible with the Server's version.

If registration at the Server is successful, the main Console window will open. In this window information on the anti-virus network stored on the Server can be viewed.

Now you can administer the Server and the anti-virus network: create (p. Installing the Agent Software through the Console), edit, approve, configure, and remove (Administration of Anti-Virus Workstations) anti-virus workstations, view logs and other data. Main controls are the main menu, the toolbar and the context menu of the anti-virus catalog items as described in p. The Anti-Virus Console and the In-Built Web Server above.

After the Agent has been installed on a workstation it will try to establish a connection with the Server. With default Server settings new workstations should be approved by an administrator to be registered at the Server (for more about the policy of connecting new workstations, please refer to p. New Stations Approval Policy). In this mode new workstations are not connected automatically, but placed by the Server into the list of Unapproved stations.

To connect a new workstation to the Server, on the **Administration** menu of the Console, select **Show unapproved stations**. A list of detected but not approved workstations will open.

Select the station in the list, and on the context menu select **Approve and set Everyone**.

If you select **Approve and set group**, you can appoint another primary group for the given workstation(s). Read more about primary groups in p. Inheriting the Configuration from Groups by Workstations.

The workstation will be connected to the Server and the anti-virus network layout will be changed respectively.

The workstation will be placed to predefined groups of workstations **Everyone** and **Online**, and to other relevant groups according to the OS family and version installed on the anti-virus station.

To finish the installation of some components for anti-virus workstations you will need to restart the computer. In this case there will appear a red exclamation mark over the Agent's icon in the **Taskbar or** (in earlier Windows OS versions) the installer will display a notification.

By default, not all groups are displayed in the hierarchical list of the network elements (hidden groups are not displayed, if they are empty). To view all groups, on the context menu of any element of the catalog, select **Hidden groups**.

Chapter 5: Accounts and Groups

5.1. Anti-Virus Network Administrators

There are two types of administrator accounts:

- full-rights accounts,
- read-only accounts.

Administrators with full rights have exclusive rights to the administration of the anti-virus Server and of the whole network. They can view and edit the configuration of the anti-virus network and create new administrator accounts of both types. An administrator with full rights can configure the anti-virus software of a workstation, limit and disable user intervention into the administration of the anti-virus software on the workstation (see p. Setting Users' Permissions).

Administrators with read-only rights 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 current administrator accounts.

To manage the **Dr.Web® ES anti-virus**, it is not necessary to have administrator rights on computers included in the anti-virus network. However, remote installation and removal of the Agent software is possible within a local network only and requires administrator's rights in the local network, and checkout of the anti-virus Server requires full access to its installation catalog.

It is recommended to appoint a reliable, qualified employer experienced in the administration of a local network and competent in anti-virus protection as an administrator of the anti-virus network. Such employer should have full access to the installation folders of the anti-virus Server. Such employer should either be a local network administrator or work closely with such person.

5.2. Managing Administrator Accounts

The **Dr.Web® ES** anti-virus allows any administrator with full rights to edit settings (including administrator name and password), create new accounts and delete already existing ones.

By default, if not specified otherwise during the installation, the program is installed with a full-rights administrator account (name - `admin`, password - `root`). If the program is installed with the default settings, it is advisable to change the password as soon as you log in on the Server for the first time.

To edit administrator accounts

1. On the **Administration** menu of the Console, select **Administrator accounts**. A list with administrator accounts will open.
2. To edit an account, right-click it in the list, and on the context menu, select the correspondent item. A window for editing the account will open.
3. To add an account, right-click the list, and on the context menu, select **Add**. A similar window will open.
4. To delete an account, right-click it, and on the context menu, select **Delete**.

The **Edit administrator** window in steps 2 and 3 allows you to fill in or edit the necessary fields (the **Login**, **Password** and **Retype password** fields should be obligatorily filled in when a new account is added). When creating an administrator account with full rights, clear the **Read only** checkbox (set by default).

5.3. Groups. Preinstalled Groups, Creating and Removing Groups

Grouping is designed to make the administration of anti-virus workstations easier.

Grouping of anti-virus stations allows to set the same settings for all stations in a group with just one instruction, as well as to initialize certain tasks on all these stations. Groups can also be used to order (structure) the list of workstations.

At the installation of the program so-called preinstalled (system) groups are created.

System Groups

Dr.Web® ES has an initial set of system groups. These groups are created during the installation of **Dr.Web® Enterprise Server** and may neither be deleted, nor renamed. Still the administrator may disable their display in the administrator's Console, if necessary.

Everyone group

Group containing all stations known to the anti-virus Server. The **Everyone** group has default settings.

By workstation status

The two following groups reflect the current status of the station, that is if it is connected to the Server or not at the moment. These groups are completely virtual, may not have any settings or be primary groups.

- **Online** group. The group contains all workstations connected at the moment (reacting to Server requests).
- **Offline** group. The group contains all workstations not connected at the moment.

By network protocol

The three following groups elicit the protocol of workstations' connection to the Server. These groups are completely virtual, may not have any settings or be primary groups.

- **TCP/IP** group. The group contains workstations connected at the moment through the TCP/IP protocol.
- **IPX** group. The group contains workstations connected at the moment through the IPX protocol.

- **NetBIOS** group. The group contains workstations connected at the moment through the NetBIOS protocol.

By operation system

This category of groups represents the operation systems under which the stations are working at the moment. These groups are not virtual, may have station settings and be primary groups.

- **Windows** family groups. This family includes a large set of groups, which reflect the specific version of Windows operation system. All possible group names are nevertheless sufficiently unambiguous. For example, the **Windows** group includes all stations working under all versions of Windows OS. The **Windows/2000** group includes stations working under Windows 2000 OS, and the **Windows/2000/AS** group stations under Windows 2000 Advanced Server OS, etc.
- **Linux** group. Stations under Linux OS.
- **FreeBSD** group. Stations under FreeBSD OS.
- **Solaris** group Stations under Solaris OS.

By the state of the anti-virus SW on the station

- **Expired** group. For each station account at the Server, it is possible to set a validity period. After the account has expired, the station is transferred to the **Expired** group.
- **Deinstalled** group. Once anti-virus Agent SW has been deinstalled from a station, the staion is transferred to the **Deinstalled** group.

User Groups

These groups are assigned by the anti-virus network administrator for his/her own needs. The administrator may create own groups and include workstations in them. The contents and names of such groups are not restricted by **Dr.Web® Enterprise** in any manner.

In Table 5-1 all possible groups and group types are given for your reference, along with the specific parameters supported (+) or not supported (–) by the groups.

The following parameters are considered:

- **Automatic membership**. The parameter reflects whether stations may be automatically included in the group (automatic membership support) and group contents automatically adjusted during Server operation.
- **Membership administration**. The parameter reflects whether the administrator can manage group membership: add stations to or remove from the group.
- **Primary group**. The parameter reflects whether the group can be primary for a station.
- **Possibility to have own settings**. The parameter reflects whether the group can have own settings (to be propagated to its stations).

Table 5-1. Groups and supported parameters

Parameter / Group/group type	Parameter			
	Automatic membership	**Membership administration**	**Primary group**	**Possibility to have own settings**
Everyone	+	–	+	+
By workstation status	+	–	–	–
By network protocol	+	–	–	–
By operation system	+	–	+	+
User groups	–	+	+	+
By the state of anti-virus SW on the station	+	–	–	–

To create a new group

1. On the context menu, select **Create group** (the item is available regardless of what elements of the anti-virus catalog are selected). A window for creating a group will open.
2. The **ID** entry field is filled in automatically. You can edit it, if necessary. The identifier should not contain blank spaces.
3. Type the group name in the **Name** entry field.

4. Type comments in the **Description** entry field (optional).
5. Click **OK**.

You can also delete the groups you created (preinstalled groups cannot be deleted). To do this, right-click the group, and on the context menu, select **Delete**.

The groups you create are initially empty. See below how to add workstations to groups.

All groups reside on the same hierarchy level of the anti-virus network catalog. Nesting of groups is impossible.

5.4. Adding a Workstation to a Group. Removing a Workstation from a Group

There are several ways how to add a workstation to a new (created) group.

Through the context menu of a group

1. Select the necessary group in the Console's catalog.
2. On the context menu, select **Stations**. A window for managing the content of the group will open.
3. In the Known field, highlight the stations you want to add to the group and click  .

To remove a station from the group, highlight it in the **Members** field and click  .

By dragging items in the Console catalog

To move a station to a different group, unfold the group folder, left-click the station's icon and drag it to the target group. To copy a station to a different group, follow the same procedure keeping the CTRL key pressed.

Moving a station from the **Everyone** preinstalled group is impossible. You can only copy it.

Through the context menu of a station

1. On the context menu of the necessary workstation, select **Properties**.
2. In the opened **Properties** window, select the **Groups** tab.
3. In the **Member** of field, there is a list of groups, which the station is included to. In the **Known group** field, there is a list of all existing groups. Select the necessary group you want to add the station to, and click the  button.

Removing a station from the group is similar. Select the correspondent group's radio button and click  .

You can also add a station to a group and set this group as the primary one. For more read p. Inheriting_the_Configuration_from_Groups_by Workstations.

You cannot change the set of preinstalled groups.

As a result of operations with the database or reinstallation of the software on anti-virus workstations, several stations with the same name may appear on the anti-virus network list (only one of them will be correlated with the respective workstation). To remove repeated workstation names, select all names of such workstation, and on the context menu, select **Unite workstations**. By default the name of the anti-virus station given to it the last time at its registration at the Server will be offered to use.

5.5. Setting a Group. Using Groups to Configure Workstations. Setting Users' Permissions

Each station is included in the Everyone group as well as the groups correspondent to the OS of the station and to the relevant OS family. Immediately after the installation, the settings of the **Everyone** group

are the default uniform settings for all workstations. These settings are inherited by all other groups and all workstations.

The **Dr.Web® ES** anti-virus allows to join workstations into groups. You can specify certain settings for each group, and these settings will be inherited by all workstations belonging to the group.

To change the default settings of a group

1. Select a group in the network catalog.
2. Right-click the object. On the context menu, select the necessary setting and edit it.

The group's settings include the configuration of the anti-virus programs (for more refer to p. Viewing and Editing the Configuration of a Workstation), the schedule and permissions settings, etc. Editing the configuration of anti-virus programs is completely analogous to editing the configuration of a workstation described in Administration of Anti-Virus Workstations. Setting the permissions is similar to setting the permissions of separate workstations described below (p. Setting Users' Permissions).

The Agent's settings are not included into the group's configuration and cannot be specified through a group.

You can run, view and terminate tasks for scanning for a separate group of stations as well as several selected groups. In the same way, you can view the statistics (on infections, viruses, start/shutdown, scanning and installation errors, etc.) and summary statistics for workstations of a group or several groups.

When viewing or editing workstation's configuration inherited from the primary group (for more read p. Inheriting the Configuration from Groups by Workstations), a notification that the settings are derived from the Everyone group will be displayed in correspondent windows.

If you modify the configuration of a workstation, this inscription will disappear and the  **Remove these settings** button will become enabled in the toolbar. You can restore the configuration inherited from the primary group; click this button to do this.

5.5.1. Inheriting the Configuration from Groups by Workstations

When a new workstation is connected to the Server, its configuration settings are adopted from one of the groups it belongs to (the primary group). If the settings of the primary group are modified, these changes are inherited by all workstations included into the group, unless the workstations have been customized. When creating a workstation, you can specify what group will be regarded as primary. By default, this is the **Everyone** group.

If **Everyone** is not the primary group, and a different primary group has no personal settings, the settings of the **Everyone** group are inherited by a new station.

There are several ways how to set a new primary group for a workstation or a group of workstations.

To view and change the primary group for a workstation

1. Select a station in the network catalog.
2. On the context menu, click **Properties**. In the opened window go to the **Groups** tab.
3. If necessary, reassign the primary group by clicking the **Primary option** button against the necessary group.
4. Click **OK**.

You can also make a group primary for all workstations included into it. To do this, select the necessary group in the catalog, and on the context menu, select **Become primary**.

You can also assign a certain group as primary for several selected workstations. To do this, select the necessary workstations in the catalog (you can also select groups – the action will be applied to all the included workstations, you can use the CTRL and SHIFT keys when selecting), then on the context menu, select **Assign primary group**. A window with the list of groups, which can be assigned as primary for these workstations will open. Select the necessary group and click **OK**.

By default the network structure is displayed in such a way as to show a station in all the groups it is included into. If you want workstations to be displayed in the network catalog in their primary groups only, on the context menu, clear the **Full membership** checkbox.

5.5.2. Setting Users' Permissions

New workstations inherit default permissions from the primary group. You can change default permissions for a whole group as well as for each workstation included into it.

To change users' default permissions to administrate the anti-virus package

1. Right-click the necessary group or unfold the group and right-click the necessary workstation in the catalog, and on the context menu, select **Permissions**. A window for editing permissions will open.
2. By default, a user is authorized to launch each component, but prohibited to edit components' configuration or stop the operation of components. To change (enable or disable) any permission, select or clear the correspondent checkbox.
3. To accept the changes in permissions, click **OK**; to reject the changes, click **Cancel**.

To cancel edited permissions and to restore the default ones (inherited from the preinstalled groups), click  **Remove these settings**.

You can also propagate these settings to another object by clicking  .

To export the settings to file, click  .

To import settings from a file, click  .

5.5.3. Propagation of Settings to Other Groups/Stations

Configuration settings of anti-virus programs, schedules and user permissions of a group or a workstation can be propagated to other groups and workstations. **To do this**

1. Right-click the necessary station or group whose configuration settings you want to propagate and select the necessary item. In the window for editing the configuration of the anti-virus component, the schedule or permissions click  ( or  subject to the window type) (**Propagate these settings**). A window of the network catalog will open.
2. Select necessary groups and stations to which you want to propagate the settings.
3. To enable changes in the configuration of these groups, click **OK,** to reject the action and close the window – click **Cancel**.

Chapter 6: Administration of Anti-Virus Workstations

Anti-virus networks operated by **Dr.Web® ES** provide for centralized configuring of anti-virus packages on workstations. The program complex allows:

- to set the configuration parameters of anti-virus programs,
- to schedule tasks and launch on-demand tasks on workstations,
- to update workstations, also after an updating error, in this case the error state will be reset.

The administrator of the anti-virus network can grant a user with the permissions to change the configuration of the workstation and launch tasks, as well as restrict or prohibit such actions.

The configuration of workstations can be modified even when they are temporarily disconnected from the Server. These changes will be accepted by the workstations as soon as they are reconnected to the Server.

6.1. New Stations Approval Policy

The procedure of approving new workstations manually was described in Getting Started. Launching the Anti-Virus Console and Establishing a Simple Anti-Virus Network. But you can change the approval policy by choosing a different mode of workstations' access to the Server.

To change the access mode of workstations to the Server

1. On the **Administration** menu of the Console, select **Configure Dr.Web® Enterprise Server**.
2. On the **General** tab, in the **Newbie** drop-down list select the necessary option:
   - Allow access automatically,
   - Approve access manually (the mode is specified by default unless changed at the Servers installation),
   - Always deny access.

It is recommended to set the **Approve access manually** mode. In this mode new stations are placed to the **Unapproved stations** list until approved by the administrator. The list is available on the **Administration** menu.

The **Allow access automatically** mode instructs to connect all new stations automatically to the Server without requesting the administrator.

When the **Always deny access** mode is set, new stations are not connected to the Server. The administrator should manually create an account for a new station.

To create an account for a new workstation manually

1. On the context menu of any element of the network catalog, select **Create station**. A window for creating a new workstation will open.
2. The **ID** field is filled in automatically. You can edit the parameter in the **ID** field, if necessary (it should not contain spaces and should be unique).
3. Enter the station name and password into appropriate fields. Retype the password.
4. If necessary, make comments in the **Description** field.
5. Click **OK**.

6.2. Viewing and Editing 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 catalog of the anti-virus Console's main window.
2. On the context menu, select **Installed components**. A window with the list of installed components will open.
3. To close the window, click **Close**.

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

To view what virus databases are installed on a workstation

1. On the context menu of a workstation, select **Virus bases**. A window with the list of the installed virus databases will open.
2. To close the window, click **Close**.

You can also edit the settings of any anti-virus component for the given workstation.

To view and edit the properties of a workstation

1. On the context menu, select **Properties**. In the opened window on the **General** tab you can specify a password to authorize the station at the Server, set the validity of the workstation's account in the **Expires** field and add comments in the **Description** field.
2. On the **Groups** tab you can change the primary group for this station.
3. On the **Configuration** tab you can change the configuration of the station. The configuration includes the permissions, the schedule, and the settings of the anti-virus components - **Dr.Web® Scanner for Windows**, **SpIDer Guard for Windows**, **SpIDer Mail for Windows Workstations**, etc.

The set of the components' parameters and recommendations to their configuring are described in the manual **Dr.Web® Anti-Virus for Windows. User Manual**.

Meanwhile the Console's interface is somewhat different from the interface of the anti-virus components:

- to change the parameters whose values can be either **Yes** or **No**, click the appropriate value,
- entry fields and drop-down lists are standard,

- to restore the value a parameter had before editing, click  in the toolbar (the upper part of most settings windows, e.g. **Schedule**, **Permissions**, **Dr.Web® Scanner for Windows**, **SpIDer Guard® for Windows** and **SpIDer Mail® for Windows Workstations**),
- to set the default value for a parameter, click  ,
- to restore the values all parameters had before editing, click  ,
- to restore the default values of all parameters, click  ,
- to export parameters to a file of a special format, click  ,
- to import parameters from such file, click  .

4. Click **OK** to confirm the changes made, or click **Cancel** to restore the state of the configuration before editing.
5. To delete the specific configuration of the given workstation, click  (**Remove these settings**). The configuration inherited from the preinstalled groups will be restored (see p. Setting a Group. Using Groups for Setting Workstations. Setting User's Permissions).

Other components of the anti-virus package are set up similarly.

You can create different groups of users subject to optimal permissions and settings for them. Setting main parameters of stations through groups will allow you to save time on handling the settings of each individual group.

To limit/ extend user's permissions on administering the anti-virus package, on the context menu of the station or group, select **Permissions**, and in the opened window, select the rights you want to grant the user with. And vice versa clear the respective checkboxes, if necessary.

If you have edited a workstation, when it was not connected to the Server, the new settings will be accepted, once the Agent has reconnected to the Server.

To remove personal settings of a workstation, on the context menu of the station, select  Remove personal settings. The list of this workstation's settings will open, checkboxes against altered personal settings will be selected. Clear the checkboxes as necessary and click **OK.** The workstation's settings inherited from the primary group will be restored.

Before editing the configuration of a workstation for **SpIDer Guard for Windows** and **Dr.Web® Scanner for Windows**, familiarize yourself with recommendations on using the anti-virus for computers on Windows Server 2003 OS, Windows 2000 OS, or Windows XP OS. An article with necessary information can be found at http://support.microsoft.com/kb/822158/en. The article is meant to help you increase system performance.

Provided that your Agent key (`agent.key`) allows to use a spam filter for the **SpIDer Mail** component, on the **Antispam** tab you can set up the filter (on the context menu of any group or workstation, select **SpIDer Mail® for Windows Workstations).** Spam filter settings are described in the manual **"Dr.Web® Anti-Virus for Windows. User Manual"**.

6.3. Editing the Parameters of the Anti-Virus Agent

To view and edit the configuration of the anti-virus Agent for the necessary station, select the station in the anti-virus network catalog. Then on the context menu, select **Configure** -> **Dr.Web® Enterprise Agent for Windows**. A window for editing the Agent's settings will open.

Any changes incompatible with the Server settings (for example, changes of the encryption and compression modes) 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. Click this button to accept changes in settings. To reject changes in settings and to close the window, click **Cancel**.

To instruct the Server to reconnect the station, click 

(make this station a newbie). All registration parameters of this station will be reset.

It is impossible to view and edit the settings of an Agent disconnected from the Server.

In case a critical error occurs during the operation of the Agent

1. Initiate a forced update of the workstation (see p. Manual Updating of the Dr.Web ES Components).
2. Through logs of the Agent and the updater stored on the workstation investigate the cause of the error. By default both log files (`drwagntd.log` and `drwupgrade.log`) reside in the **logs** subfolder of the Agent's installation folder.
3. Remove the cause of the error.
4. Run a forced update of the workstation again.

6.4. Scheduling Tasks on a Workstation

Schedule – a list of actions performed automatically at a preset time on workstations. Schedules are mostly used to scan stations for viruses at a time most convenient for users, without having to launch the Scanner manually. Besides **Dr.Web® Enterprise Agent** allows to perform certain other types of tasks as described below.

There are two types of schedules:

- *Centralized (Enterprise) schedule*. It is set by the anti-virus network administrator and complies with all the rules of configuration inheritance.
- *Local schedule* of a station. It is set by the user of the specific station (if the station has the permissions) and stored locally on this station; **Dr.Web® ES Server** does not control this schedule.

Centralized Schedule

Scheduling tasks through the Console

Using the Console you can schedule tasks for a certain workstation or a group of workstations. This service facilitates all basic operations necessary to assure anti-virus protection of your network in the automatic mode.

1. Select the necessary station or a group of stations. On the context menu, select **Schedule**. A window for editing the schedule will open. By default two tasks are available:
   - **Startup scan** (enabled by default),
   - **Daily scan** (disabled by default).
2. You can add new tasks and remove or edit the existing ones. You can also disable a task or enable a previously disabled task.
3. After editing click **OK** to save the task or **Cancel** to skip changes or delete a newly created task.

If, when edited, the schedule is empty (without any task), the Console will offer you to use either the schedule inherited from groups, or the empty schedule. Use empty schedule to override the schedule inherided from the groups.

To add a new task

1. On the context menu of the task list, select **Add**. A window for creating a new task will open.
2. Give a name to the task in the **Name** entry field.
3. In the **Action** drop-down list select the type of the task. After the selection is made, the bottom part of the window will look differently depending on the selected action.
   - If you want a certain program to be launched, select **Run**. Then type the full name (with the path) of the executable file to be launched in the **Path** entry field, and type command line parameters for the program to be run in the **Arguments** field.

- If you want the **Scanner** to be run, select **Dr.Web® Scanner for Windows** and type the Scanner's command line parameters in the **Parameters** field.
- If you want the **Enterprise Scanner** to be run, select **Dr.Web® Enterprise Scanner for Windows**.
- If you want this event to be logged, select **Log**, and in the **String** field type the text of the message to be added to the log.

4. In the Time drop-down list set the time mode of the task:
   - Daily,
   - Every N minutes,
   - Hourly,
   - Monthly,
   - Shutdown,
   - Startup,
   - Weekly.

   The parameters of different types of the time modes are described below.
5. When all parameters for the task are specified, click **OK** to accept changes, or click **Cancel** to close the window skipping the changes in the schedule.

Table 6-1. The parameters of different types of the time modes

Type	Description
Daily	Enter the hour and the minute, for the task to be launched at the time specified.
Every N minutes	The **N** value should be specified to set the time interval for the execution of the task. At **N** equal `60` or more the task will be run every **N** minutes. At **N** less than `60`, the task will be run every minute of the hour multiple of **N**.
Hourly	Enter a number from `0` to `59` to set the minute of every hour the task will be run.
Monthly	Enter the day of the month, the hour and the minute, for the task to be launched at the time specified.

Type	Description
Shutdown	Have no additional parameters. The task will be launched at shutdown. The **Shutdown** task is not executed for **Dr.Web® Enterprise Scanner** and **Dr.Web Scanner for Windows**.
Startup	Have no additional parameters. The task will be launched at startup.
Weekly	Enter a day of the week, the hour and the minute, for the task to be launched at the time specified.

To edit or delete an existing task, select it in the list, and then on the context menu, select the correspondent item.

Local schedule

Editing the local schedule on a workstation

1. On the Agent context menu, select **Schedule** and then **Local**.
2. A window for editing the local schedule of **Dr.Web® Enterprise Agent** will open.

On the Agent context menu, the **Schedule** item will contain the **Local** option provided that the **Create local schedule** checkbox has been selected in the station permissions from the Console.

Using the local schedule a user can plan scanning and set parameters of this task. Variants of setting objects for scanning as well as command line switches which specify the program settings are described in **"Dr.Web® Anti-Virus for Windows. User Manual"**.

3. When you are done, click **Close**.

Some scheduled tasks, namely launching the updating utility, cannot be successfully performed unless the **ES** Server is stopped. Otherwise an error message will be displayed and the task will not be executed.

With the default settings, the anti-virus Monitor runs on workstations, updating tasks and anti-virus scanning are launched from time to time – without the anti-virus network administrator's intervention.

6.5. Launching and Terminating Anti-Virus Scanning on Workstations

You can manually initiate anti-virus scanning and specify its parameters on every workstation.

Users can scan their workstations themselves using **Dr.Web® Scanner for Windows**. A Scanner's shortcut is created on the desktop during the installation of the anti-virus package. The Scanner can be launched and operate successfully even in case of Agent's malfunction or running Windows OS in the safe mode.

You can view the list of all scanning processes active at present (both run manually by you, or users, or scheduled).

You can also terminate tasks for scanning on workstations (both run manually by you, or users, or scheduled).

To launch a task for scanning

1. Select a station or a group of stations. On the context menu, select **Scan**. A window for arranging a task will open.
2. Specify the parameters of the scanning and the objects to be scanned.
3. Click **OK** to run the scanning process on the workstation.

Below are given recommendations on how to set scanning.

With the **Heuristic analyzer** checkbox selected by default, the Scanner makes attempts to detect unknown viruses. In this mode the Scanner may give false positives though.

The **Scan archives** checkbox is selected by default and instructs the Scanner to search for viruses in files within archives and containers of different types.

The **Scan mailboxes** checkbox is selected by default and instructs to scan mailboxes.

To specify objects for scanning, choose one of the two alternative modes:

- Scan system;
- Scan paths.

If **Scan system** is selected, specify what system volumes should be scanned (if **Fixed volumes** and **Removable volumes** checkboxes are selected, all volumes of these types are scanned). If **Scan paths** is selected, the list of scanned paths is to be formed, and, if necessary, the list of paths excluded from search (how to specify excluded paths 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 the boot sectors of the drives selected for scanning (or those drives where the files selected for scanning reside). Both boot sectors of logical drives and main boot sectors of physical drives are scanned.

The **Startup processes** checkbox is selected by default and instructs to scan the files automatically launched at startup.

The **Processes in memory** checkbox is selected by default and instructs to scan the processes run in the RAM.

The **BurstScan technology** checkbox is selected by default and instructs to use this technology, which considerably increases the scanning speed on modern systems.

The **Low priority** checkbox is selected by default and grants a lower priority to scanning processes compared to users' tasks.

If necessary, select the **Show progress** checkbox (mind, though, that this mode considerably increases the network traffic).

The Paths selected to scan and the Paths being excluded during scanning lists are formed as follows:

- To add an object to the list, on the context menu, select **Add**,

- To remove an object, select it in the list, and on the context menu, select **Delete**,
- To edit an object, double-click it.

The Paths selected to scan list contains in explicit form the paths (disks and catalogs) to be scanned.

The list of paths excluded from scanning can contain the following elements:

- A character `\` or `/` excludes the entire disc with the Windows OS installation folder,
- A character `\` at the end of a path excludes the folder from checking,
- A path without a character `\` at the end - all subfolders of the selected folder are excluded from checking,
- Regular expressions. Paths can be specified through regular expressions. Any file whose full name (with the path) corresponds to a regular expression is excluded from checking.

Before starting **Dr.Web® Scanner for Windows** familiarize yourself with recommendations on virus scanning for computers operated by Windows Server 2003 OS, Windows 2000, or Windows XP OS. The information can be found at http://support.microsoft.com/kb/822158/en. The article is meant to help you increase system performance.

The syntax of regular expressions used for excluding paths from scanning is as follows:

```
qr{expression}flags
```

As a flag mostly the character `i` is used. It instructs "to ignore letter case difference". For more details, see p. K1. Options Used in Regular Expressions.

Some examples of specifying excluded paths through regular expressions are given below:

- `qr{\\pagefile\.sys$}i` — skip scanning Windows NT swap files,

- `qr{\\notepad\.exe$}i` — skip scanning `notepad.exe` files,
- `qr{^C:}i` — skip scanning disk C,
- `qr{^.:\\WINNT\\}i` – skip scanning `WINNT` catalogs on all disks,
- `qr{(^C:)|(^.:\\WINNT\\)}i` – skip scanning disk `C` and `WINNT` catalogs on all disks,
- `qr{^C:\\dir1\\dir2\\file\.ext$}i` – skip scanning the `c:\dir1\dir2\file.ext` file,
- `qr{^C:\\dir1\\dir2\\(.+\\)?file\.ext$}i` – skip scanning `file.ext`, if it is located in the `c:\dir1\dir2` catalog and its subcatalogs,
- `qr{^C:\\dir1\dir2\\}i` – skip scanning `c:\dir1\dir2` and its subcatalogs,
- `qr{dir\\^\\+}i` – skip scanning the `dir` subcatalog located in any catalog, but scan its subcatalogs,
- `qr{dir\\}i` – skip scanning the `dir` subcatalog located in any catalog and its subcatalogs.

See links to detailed descriptions of the regular expressions syntax in p. Links or refer to the User Manual **"Dr.Web Anti-Virus for Windows"**, the section about the Scanner's arguments.

On the **Actions** tab, you can set the program's reaction to events.

In the Infected files drop-down list, set the Scanner's reaction to the detection of a file infected with a known virus:

- The **Cure** action (enabled by default) instructs the Scanner to restore the state of the infected file as it had been before the infection (full recovery is usually impossible; a functionally correct state is 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. Setting Alerts on how to configure alerts).
- The **Quarantine** action instructs to move infected files to the quarantine folder.
- The **Delete** action instructs to delete infected files.

The **Incurable files** drop-down list sets the Scanner's reaction to the detection of a file infected with a known incurable virus (and in case an attempt to cure a file failed). By default, the **Quarantine** action is specified; other variants described above are available too (except for **Cure**).

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

When scanning with the OS installation folder included to the list of objects, it is advisable to select the **Report** action for suspicious files instead of the default **Quarantine** action.

In the **Infected archives** drop-down list set the Scanner's reaction to the detection of an infected or suspicious file in a file archive or container. The reaction is to be applied to the whole archive. Possible actions are the same as for incurable files (by default, it is **Quarantine**, as well as **Delete**, **Report**).

In the **Infected boot sectors** drop-down list set the Scanner's reaction to the detection of an infected or suspicious boot sector. The **Cure** (by default; disabled for suspicious and incurable files) and **Report** actions are available.

In the **Adware** drop-down list set the Scanner's reaction to the detection of this type of unsolicited software. Possible actions are **Quarantine** (by default), **Ignore**, **Delete** and **Report**.

The Scanner's reaction to the detection of dialers and other types of unsolicited software is set in the same way.

To view the list of running components on a workstation and, if necessary, to terminate manually some of them

1. On the context menu, select **Running components**. The list of running components will open.
2. To terminate a process, select it in the list, and then on the context menu, select **Interrupt**. The task will remain in the list, but will be marked by an **X** in the first column.
3. To remove interrupted processes from the list, on the context menu of any item of the list, select **Clean**.

You can also interrupt all processes matching a certain criterion. This option is especially useful if such instruction is to be sent to numerous stations at once.

To interrupt all scanning processes of a certain type

1. On the context menu, select **Interrupt running components**. A window for choosing scanning types will open.
2. Select checkboxes against the necessary types.
3. Click **OK**.

As a rule, the software on a workstation is updated automatically. If necessary, you can update it manually, in particular in case of a failure in a previous automatic update.

6.6. Viewing the Statistics

You can view the results of operation of the station's components — the software updater, the anti-virus Scanner, the anti-virus Monitor.

The windows with the statistics for different components and the total statistics of workstations have the same interface, and the actions to set the information to be provided are similar. Below is given an example how to get statistics for anti-virus components operation on a certain workstation.

To view the statistics on operation of anti-virus programs on a workstation

1. In the anti-virus network catalog, select the necessary station.

If you want to view records for several stations, select these stations keeping the SHIFT or CTRL key pressed.

2. On the context menu, select **Tables**, and in the opened submenu, select **Statistics**. The Statistics window will open (with no data loaded).
3. In the drop-down lists in the left bottom part of the window select the time interval for which the data should be displayed (by default, all available data is displayed).

4. To load data into this window, click  . A table with the data on the operation of anti-virus components will be loaded into the window.
5. To sort the data displayed in a column, double-click its name.
6. To view any line of the table in a more suitable way, select the necessary line in the table and click  (or double-click the line). The data will be displayed in a separate window.

If several lines are selected in the table, the records will be displayed in a separate window for each selected line.

7. To save the table for printing or future processing, click  **save shown data in CSV format**,  **save shown data in HTML format**, or  **save shown data in XML format**.
8. To view the summary statistics not split in sessions, click  . A window of summary statistics will open.

A window with summary statistics can also be opened from the context menu of the workstation. To do this, select **Summary statistics**.

9. To view the statistics as a diagram, click  in the Statistics window. A statistics graph window will open.

To view the list of components launched on a workstation, on the context menu of the station, point to **Tables**. On the opened submenu, select **Start/Stop**.

To view information on detected viruses (virus names, infected objects, program actions, etc.), on the **Tables** menu above, select **Infections**.

To view information on scanning errors, on the **Tables** menu, select **Errors**.

To view information on detected viruses grouped according to their types, on the **Tables** menu, select **Viruses**.

To view the list of scanning errors on the selected workstation for a certain period, on the **Tables** menu, select **Errors**.

To view the list of installed software, on the context menu, select **All network installations**.

To view the data on an unusual state of workstations, which might need your attention, for a certain period

1. On the context menu, select **Tables**. On the opened submenu, select **Status**. A window to set up a request will open (with no data loaded).
2. Click  . Data about the state of workstations will open.
3. To view only data of certain severity, specify the severity level by selecting the respective option button in the lower part of the window. By default, the **Very low** gravity level is selected, all data being displayed.
4. The list will also include the stations disconnected for several days from the Server. Type this number of days in the entry field in the left bottom part of the window or select it in the drop-down list.
5. You can format the way the data are presented just like in the statistics window above.

6.7. Setting a Language of Anti-Virus Components Interface on a Workstation

Using the Console you can set a language to be used by the anti-virus components on a workstation:

1. On the context menu of a group of station, select **Configure** -> [necessary product] -> go to the **Miscellaneous** tab.
2. In the **Language resources** field, select the required language from a drop-down list.

Chapter 7: Configuring the Anti-Virus Server

7.1. Setting the Server Configuration

To set the configuration parameters of the anti-virus Server, on the **Administration** menu of the Console, select **Configure Dr.Web® Enterprise Server**. A window for setting the Server configuration will open.

General tab

The **Name** parameter sets the name of the Server. 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 set the interaction of the Server with the OS and the DBMS. Change the default settings only on advice of the technical support.

In the **Newbie** field the connection policy for new workstations can be set (for more, read p. New_Stations_Approval_Policy). The **Reset unauthorized to newbie** checkbox below instructs to reset the connection parameters of unauthorized workstations.

The **Statistics** checkbox when selected instructs to send statistics on the operation of the anti-virus Server for analysis to the Internet server athttp://stat.drweb.com/. If necessary, you can set up the connection parameters in the field below. It is not recommended to set the interval of sending less than 1 hour.

In the **Encryption** and **Compression** drop-down lists the policy of traffic encryption and compression between the anti-virus Server, the Agents and the Console(s) is selected (for more, read p. Traffic Encryption and Compression).

The **Show host name** checkbox when selected instructs the program to log not the workstations' IP addresses but their host names.

The **Replace NetBios name** checkbox when selected instructs to display not the names of the workstations but their host names in the catalog of the anti-virus network (when host names cannot be detected, IP addresses are displayed).

Show host name and **Replace NetBios name** checkboxes are cleared by default. If the DNS service is not set up properly, enabling these boxes may considerably slow down the Server's operation. When using any of these options, it is recommended to enable cashing names on the DNS server.

Security tab

On the **Security** tab, restrictions for network addresses from which Agents, Consoles, network installers and other ("neighboring") **ES** Servers will be able to access the given Server are set. The **Agents**, **Installations**, **Consoles** and **Neighbors** additional tabs are designed to set the restrictions for the correspondent types of connections.

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

By default all connections are allowed (the **Use this ACL** checkbox is cleared). To make the list of allowed or denied addresses, select the checkbox.

To allow any TCP address, include it into the **TCP:Allow** or **TCPv6:Allow** list. To do this, right-click this list, and on the dynamic menu, select **Add**. A window for editing the address will open.

Type the network address and click **OK**.

In the last field a prefix should be specified. It is a byte number, which denotes the range of IP addresses in a certain IP network/subnetwork.

Examples:

1. Prefix 24 stands for a network with a network mask: `255.255.255.0`

   Containing 254 addresses.

   Host addresses look like: `195.136.12.*`

2. Prefix 8 stands for a network with a network mask: `255.0.0.0`

   Containing up to 16387064 addresses (256*256*256).

   Host addresses look like: `125.*.*.*`

Besides, you can delete addresses from the list and edit the addresses included into the list.

To deny any TCP address, include it into the **TCP:Deny** or **TCPv6:Deny** list.

The addresses not included into any of the lists are allowed or denied depending on whether the **Deny priority** checkbox is selected. If the checkbox is selected, the addresses not included into any of the lists (or included into both of them) are denied; otherwise, such addresses are allowed.

Restrictions for IPX addresses can be set similarly.

Database tab

On the **Database** tab a DBMS for storage of the centralized log of the **Dr.Web® ES** anti-virus and for its setting is selected.

For more, read p. Setting the Mode of Operation with Databases.

Alerts tab

The parameters in the **Alerts** tab allow to set up the mode of notifying the anti-virus network administrators and other users on virus attacks and other events detected by the program.

For more, read p. Setting Alerts.

Transports tab

On the **Transports** tab, the parameters of the transport protocols used by the Server are set up.

For each protocol the name of the anti-virus Server can be specified in the **Name** field; if no name is specified, the name set on the **General** tab is used (see above, if no name is set on the tab, the computer name is used). If for a protocol a name other than the name on the **General** tab is specified, the name from the protocol's description will be used by the service detecting the Server of Agents, etc.

Protocols tab

On the **Protocols** tab, protocols for interaction of the Server with other **ES** components can be chosen.

By default, the interaction with anti-virus Agents, Console(s) and Agent installation programs is enabled; the interaction of the Server with other **ES** Servers is disabled.

For a multi-server network configuration (read p. Peculiarities of a Network with Several Anti-Virus Servers), enable this protocol by selecting the correspondent checkbox.

Location tab

On the **Location** tab, you can specify additional information about the computer on which the anti-virus Server is installed.

7.1.1. Traffic Encryption and Compression

The **Dr.Web® ES** anti-virus allows encrypting the traffic between the Server and anti-virus Agents, between the Server and the Console(s), and between **ES** Servers (in multi-server anti-virus networks). This mode is used to avoid leakage of user keys and other data during interaction.

The program uses reliable tools of encryption and digital signature based on the concept of pairs of public and private keys.

The encryption policy is set separately for each component of the **Dr.Web® ES** anti-virus. Settings of other components should be compatible with the settings of the Server.

To set the encryption policy on the Server, on the **Administration** menu of the Console, select **Configure Dr.Web® Enterprise Server**. On the **General** tab, select the necessary variant in the **Encryption** drop-down list:

- **Yes** — enables obligatory traffic encryption for all components,
- **Possible** — instructs to encrypt traffic with those components whose settings do not prohibit it (is set by default, if the parameter has not been modified during the Server's installation),
- **No** — encryption is not supported.

When coordinating the settings of the encryption policy on the Server and other components (the Agent or the Console), one should remember, that certain combinations are incompatible and, if selected, will result in disconnecting the corresponding component from the Server.

Table 7-1 describes what settings provide for encryption between the Server and the components (**+**), when the connection will be non-encrypted (—) and what combinations are incompatible (**Error**).

Table 7-1. Compatibility of the encryption policy settings on the Server and a connected component

Component's settings	Server's settings		
	Yes	Possible	No
Yes	+	+	Error
Possible	+	+	—
No	Error	—	—

Encryption of traffic creates a considerable load on computers whose capacities are close to the minimal system requirements for the components installed on them (read p.System Requirements). So, when traffic encryption is not needed, you can disable this mode. To do this, you should step by step switch the Server and other installed components to the **Possible** mode first, avoiding formation of incompatible Console-Server and Agent-Server pairs. If you do not follow this recommendation it may result in loss of connection with the component and the necessity to reinstall it.

By default, the Console and the anti-virus Agent are installed with the **Possible** encryption setting. This combination means that by default the traffic will be encrypted, but it can be disabled by editing the settings of the Server without editing the settings of the components.

As traffic between components, in particular the traffic between **ES** Servers, can be considerable, the **Dr.Web® ES** anti-virus provides for compression of this traffic. The setting of the compression policy and the compatibility of settings on different components are the same as those for encryption. The only difference is that the default parameter for compression is **No**.

With the compression mode enabled, traffic is reduced, but the computational load on computers is increased considerably (more than with encryption).

7.1.2. Setting the Mode of Operation with Databases

To specify the parameters of the centralized logging of events occurring in the anti-virus network, on the **Administration** menu of the Console, select **Configure Dr.Web® Enterprise Server**. Go to the **Database** tab and select the type of DB in the **Database** drop-down list:

- **IntDB** – internal DB (a component of the anti-virus Server),
- **ODBC** (for Servers running under Windows OS) or **PostgreSQL** (for Servers operated by UNIX system-based OS) – external DB.

For an internal DB, if necessary, enter the full path to the database file into the **Path** entry field and specify the cache size and the data log mode.

The parameters of an external DB are described in detail in Appendix B. The Description of the DBMS Settings. The Parameters of the DBMS Driver.

Using an internal DBMS is selected by default. This mode considerably increases the load on the Server. It is recommended to use an external DBMS in large anti-virus networks.

If an **Oracle external DBMS** is used, it is necessary to install the latest version of the **ODBC driver** delivered with this DBMS. It is strongly recommended not to use the **Oracle ODBC driver** supplied by **Microsoft**.

The program complex provides for the possibility to perform transactions connected with clearing the database used by the anti-virus Server, in particular to delete records of events and data about the workstations which have not visited the Server for a certain period of time. To clear the database, on the **Administration** menu, select **Databases** and perform the respective command.

7.1.3. Setting Alerts

To set the mode of sending alerts about the events connected with the operation of the **Dr.Web® ES** anti-virus, on the **Administration** menu of the Console, select **Configure Dr.Web® Enterprise Server**. Go to the **Alerts** tab and select the necessary mode of alerts in the **Alert sender** drop-down list:

- **None** — do not send messages (the default mode),
- **eMail** — send by e-mail,
- **Windows network message** — send through **Windows Messenger** (for Servers under Windows OS only).

To send notifications by e-mail, specify, if necessary, the address of the SMTP server, sender and recipient addresses and, if necessary, a user name and password for the SMTP server.

For messages in a Windows OS network, specify the list of names of the computers to receive the messages.

In the bottom of the tab, select checkboxes against the events on which the notifications should be sent.

The text of messages is determined by message templates. Message templates are stored in the `var/templates` subfolder of the Server installation folder. If necessary, you can edit the template to change the text of a message.

When a message is being generated, the program replaces the variables in the template (written in braces) with a certain text, which depends upon the current parameters of the anti-virus complex. Available variables are listed in Appendix D. The Parameters of the Notification Templates.

It is strongly recommended to use the Console's templates editor for editing the templates. To do this, on the **Administration** menu, select **Edit templates**. A window for editing templates will open.

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 text of the message can be edited.

If you use an external editor for editing templates remember that the text of the templates requires **UTF-8** encoding. We do not recommend you to use **Notepad** or other editors which insert a byte order mark (**BOM**) to indicate that the text is encoded in **UTF-8**, **UTF-16** or **UTF-32**.

7.1.4. Receipt of Alerts

By default, when a message is received from the Server an **Alerts** window appears. To open it at any time, on the **Administration** menu, select **Alerts**. A list with subjects of alerts will be displayed in the window. To view the full text of a message, select it in the list, and on the context menu, select **Show** or double-click the message.

To disable displaying messages of a certain type, select a message of the necessary type, and on the context menu, select **Filter out**. You can also cancel this filter and instruct to display all messages in future. To do this, click  in the toolbar.

By default, only those messages are displayed, which are not disabled for display in the settings.

To delete a message, on the context menu, select **Delete**.

To delete all messages, on the context menu, select **Clear**.

You can disable automatic opening of this window. To do this, select the **Do not disturb** checkbox in the bottom left corner of the window.

To display messages in the chronological order, select the **Old messages first** checkbox in the bottom left corner of the window.

7.2. Server Logging. Viewing the Log

The anti-virus Server logs the events connected with its operation. Under **UNIX** OS by default the syslogd service is used for logging; under OS **Windows** the log file resides by default in the var subfolder of the Server installation folder; its name is drwcsd.log. It is a plain text file.

The Server's log helps to detect the problem in case of an abnormal operation of the **Dr.Web® ES** anti-virus.

The administrator can view logging in the real time mode from the anti-virus Console. Before viewing logged data, the level of detail of the displayed data should be set up.

The log in the anti-virus Console records events only from its opening. It is impossible to view earlier data by means of this service.

To view the log in the Console's window

1. On the **Administration** menu of the anti-virus Console, select **Show Dr.Web® Enterprise Server log**. A **Select log level** window will open.
2. Select the correspondent radio button against the necessary log's level of detail. The following options are available:
   - **Fatal error** — instructs to inform only of the most severe errors,
   - **Error** — notify of operation errors,
   - **Warning** — warn about errors,
   - **Notice** — display important information messages,
   - **Info** — display information messages,
   - **Trace**, **Trace 1**, **Trace 2**, **Trace 3** — enable tracing events. The options are displayed in the ascending order according to the level of detail. Trace instructs to log in the minimum level of detail; **Trace 3** instructs to log in the maximum level of detail.

- **Debug**, **Debug 1**, **Debug 2**, **Debug 3** — instruct to log debugging events. The options are displayed in the ascending order according to the level of detail. Debug instructs to log in the minimum level of detail; **Debug 3** instructs to log in the maximum level of detail.

3. Click **OK**.
4. A **Dr.Web® Enterprise Server log** window with data of the specified level of detail will open.

7.3. Setting the Server Schedule

To schedule tasks for the Server

1. On the **Administration** menu, select **Dr.Web® Enterprise Server schedule**. A window for setting the list of tasks for the Server will open.
2. To remove a task from the list, right-click it in the list, and on the context menu, select **Delete**.
3. To edit the parameters of the task, right-click the necessary parameter in the list, and on the context menu, select **Edit**. A window for editing parameters will open.
4. To add a new task to the list, on the context menu, select **Add**. A window for editing the task will open.

Old data is automatically deleted from the database to save disk space. The default time span for **Purge old data** and **Purge old stations** tasks is 90 days.

5. You can also disable a task, or enable a previously disabled task. To do this, right-click the necessary task, and on the context menu, select the corresponding item.
6. To save changes in the settings, click **OK**. To reject changes, click **Cancel**.

The **Update all products** task is scheduled by default. If you delete the task, after clicking **OK** you will receive a prompt for the action.

7. To export the schedule into a file of a special format, click  .
8. To import parameters from such file, click  .

When a new task is created or an existing task is edited, a window for entering the parameters will open.

To edit the parameters of a task

1. In the **Name** entry field assign a name to the task, which will be displayed in the schedule.
2. Select the type of task in the **Action** drop-down list. The bottom part of the window containing the parameters of the selected task will change its look (the parameters of different types of tasks are described below).
3. Select time intervals at which the task is to be launched and set the time accordingly (it is similar to scheduling tasks for a workstation, as described in p. Scheduling Tasks on a Workstation above).
4. Click **OK**.

Table 7-2. Tasks types and settings

Type	Description
Run a procedure	For tasks of this type, you need to enter the procedure name in the Name filed.
Shutdown and Restart	There are no additional parameters for tasks of this type. Use these tasks to stop and restart the server.
Run	Specify the path to the executable file of the Server in the Path field, and the command line parameters at launch in the Arguments field. Select Execute synchronously option if you want the server to wait while task finishes.
License expiration reminder	Select the period till the license expiration when to execute the task.
Update	See paragraph Updating Mobile Agents for details.
Log	Specify the message to be logged.
Backup critical server data	Use these tasks to create backups of the server database, the license key file and private key.

Type	Description
	Specify the folder where to store the backup files (empty by default) and the maximum number of backup copies allowed (for unlimited number of copies, use 0). Appendix H5.8. for details.
Stations that nave not visited for a long time	Specify the absence period after which the station should be considered absent for too long. After this period, a reminder displays.
Purge non-activated stations	Specify the period of inactivity after which the station should be purged. **Note**: To view the list on inactive stations, in the menu select Administration and then select Unconfirmed stations.
Purge unsent IS events	Specify the period after which the event should be purged. This task affects only the event which the secondary servers fail to deliver to the main server. If the secondary server fails to send an event, the event is moved to the list of unsent events, which the server tries to resend periodically. When you execute the Purge unsent IS events task, the events older than the specified period are purged.
Purge expired stations	Specify the period after which the stations with expired access should be purged. Note: To view the date when the station expires, right-click the station, select Properties and then select the General tab. The Access field displays the expiration date.
Purge old records and Purge stations tasks	Specify a period after which the records or stations should be considered outdated and purged.

The period set for a **Purge records** task by default equals 90 days. If you decrease the value, the statistics on the operation of the anti-virus complex will be less representative. If you decrease the value, the Server may need more resources.

7.4. Administration of the Server Repository

7.4.1. Introduction

The *repository* of the anti-virus Server is designed to store benchmark copies of the anti-virus software and update them from **GUS** servers.

The repository deals with sets of files (*products*). Each product resides in a separate subfolder of the repository folder located in the `var` folder, which in case of installation with the default settings is lodged in the Server's root folder. In the repository each product is dealt with separately.

To administrate the updating in the repository product *revisions* are used. A revision is a correct state of product files at a certain time (including file names and checksums) and has its unique number. The repository synchronizes revisions of products as follows:

a) to the anti-virus Server from the product update site (via HTTP),

b) between different anti-virus Servers in a multi-server configuration according to a specified synchronization policy,

c) from the anti-virus Server to workstations.

The repository allows to set up the following parameters:

- the list of product update sites in **a)** operations,
- restrictions to the number of products requiring synchronization of **a)** type (thus, a user is enabled to track only necessary changes of certain files or categories of files),
- restrictions to product's components requiring synchronization of **c)** type (a user can choose what should be installed on the workstation),
- control of switching to new revisions (independent testing of products before installation is possible),
- adding one's own components to products,
- independent creation of new products which will be synchronized too.

The Server's repository deals with the following products:

- the anti-virus Server,

- the anti-virus Console,
- the anti-virus **ES** Agent (the Agent's software and the Scheduler, the anti-virus package for workstations),
- the Web Server,
- virus databases.

For more about the repository, please refer to Appendix F. Administration of the Repository.

You can configure the repository for each product separately or jointly for all products. How to configure separate products is described below. Configuring the entire repository (a simple editor of the repository configuration) is described in p. A Simple Editor of the Configuration of the Repository.

7.4.2. General Parameters of the Repository

To configure the Server's repository, on the **Administration** menu of the Console, select **Configure repository**. On the opened submenu, select the product.

Further actions are described on the example of the anti-virus Agent.

Once settings of the repository have been changed, you should update the **Dr.Web® ES** anti-virus software to change the state of the repository according to the settings configured.

A window for configuring the repository for the selected product will open. Go to the **General** tab.

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. To do this, select the correspondent checkbox.

To reload the product (for example, to reset an error state), select the **Reload product** checkbox.

If the product's synchronization was interrupted (see p. Setting Synchronization below), a group of radio buttons in the left part of the tab becomes accessible. You can specify the reaction of the repository to incomplete synchronization:

- **Leave revision as is** — synchronization is prohibited,
- **Approve new revision** – allows switching to a new revision (for this purpose it is necessary to edit the settings which had provoked the termination of the synchronization, read p. Setting Synchronization below),
- **Stay with current revision** — instructs to use the current revision.

You can also specify the list of notifications to be sent by the Server at synchronization of the repository. To do this, select (or keep) checkboxes against the names of events upon which notifications should be sent. Additional settings of notifications can be customized on the **Notifications** tab, read p. Setting Notifications.

7.4.3. Setting the Dr.Web Global Update System (GUS)

On the **Administration** menu of the Console, select **Configure repository**. On the opened submenu, select the product. Open the **Dr.Web® GUS** tab.

On this tab, a list of known updates servers is displayed. You can

- remove a server from the list (right-click the necessary object, and on the context menu, select **Remove** object);
- change access priority (right-click the necessary object, and on the context menu, select **Move down** or **Move up**);
- add a new server to the list (on the context menu of the root element, select **Create server** or **Create proxy server**);
- change the server address and user authorization parameters (right-click the necessary object, and on the context menu, select **Tune server**).

When editing or adding a server, a window for editing updates server's settings appears.

Fill in the **Server** and the **Path** entry fields with the server address, the port and path to the server; fill in the **User** and the **Password** entry fields (if authorization on the server is not required, leave these fields empty). To save changes in the settings, click **OK**.

If a proxy server is used to access all or certain update servers:

- add the proxy server to the hierarchical list (the procedure for adding and setting a proxy server is the same).
- Then ascribe the update server to this proxy server: on its context menu, select **Move server to**.
- A submenu with the list of accessible proxy servers will open. Select the necessary one on the list.

If it is necessary to disconnect the update server from the proxy server, on the context menu, select **Move server to**, and then select the name of the root element of the list.

7.4.4. Setting Synchronization

On the **Administration** menu of the Console, select **Configure repository**. On the opened submenu, select the product. Go to the **Synchronization** tab.

On this tab, 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 a set of files to be synchronized. No file outside this set will be synchronized.

Do not enable to use an empty **Only** list! Synchronization will be blocked.

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

The **Delay** list specifies the set of files which when being synchronized terminate synchronization. Further actions in this case are prescribed on the **General** tab.

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

- first the files given in the **Only** list are selected,
- from the selected files (or all files, if **Only** is disabled) the files specified in the **Ignore** list are deleted;
- the **Delay** list is applied to the rest.

To edit any list, enable it first. To do this, select the **Use this list** checkbox. To add a file, on the context menu, select **Add**. An element containing a regular expression will be added to the list. Double-click it and edit the expression.

To delete an element, select **Delete** on the context menu of this element. For more about the syntax of regular expressions on this list, please refer to Appendix F. Administration of the Repository.

7.4.5. Setting Propagation

On the **Administration** menu of the Console, select **Configure repository**. On the opened submenu, select the product. On the **Distribution** tab, the set of files which should be distributed to workstations is specified. To do this, the **Only** and the **Ignore** lists are used. The procedure for setting distribution lists is similar to those for synchronization described above.

7.4.6. Setting Notifications

On the **Administration** menu of the Console, select **Configure repository**. On the opened submenu, select the product. On the **Notifications** tab, additional settings for notifications on the events connected with synchronization are specified. The permission to send notifications on events of different types is specified on the **General** tab (see p. General Parameters of the Repository). On this tab, you can specify the set of files which when updated trigger messages like - **Product has been updated successfully**.

To specify the set of files the **Only** and the **Ignore** lists are used. The procedure for setting notifications lists is similar to those described in p. Setting Synchronization above.

7.4.7. A Simple Editor of the Configuration of the Repository

A simple repository configuration editor allows to specify the repository configuration parameters common to 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

1. On the **Administration** menu, select **Configure repository**; on the opened submenu, select **Entire repository settings**. A window of the simple repository editor will open. Go to the **Dr.Web® GUS** tab.

   The setting of parameters of the **Dr.Web® Global Update System** is similar to that for separate products (read in p. Setting the Dr.Web GUS above). If it is necessary to set a non-standard URI to an updates server, select the **Edit URI** checkbox and edit the entry in the **Base URI** field.

2. Go to the **Dr.Web® Enterprise Agent** tab.

   In the group of radio buttons specify whether all files or only virus databases should be updated.

3. Go to the **Dr.Web® Enterprise Server** tab.

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

The parameters on the **Dr.Web® Enterprise Console** tab are similar to those for the Server in item 3 above.

7.5. Server Statistics

To view the Server statistics, on the **Administration** menu of the Console, select **Dr.Web® Enterprise Server Statistics**. A statistics window will open. Go to the **Counters** tab.

On this tab, the following data is displayed in numerical form:

- use of system resources,
- network traffic,
- activity of clients (total number, clients active at the moment, data on newbies and installers, neighboring servers),
- use of the database,
- use of file cache,
- external interaction (messages, web statistics, operation of the repository).

To turn on the graph representation of a counter, click the counter name. If a counter can be displayed as a graph on the **Graphs** tab, it will become underlined. Then go to the **Graphs** tab.

7.6. Peculiarities of a Network with Several Anti-Virus Servers

Dr.Web® ES allows to build an anti-virus network with several anti-virus Servers. In such networks each workstation is ascribed to one Server, which allows to distribute the load between them.

The connections between the Servers can have a hierarchical structure, which allows to optimally distribute the load between the Servers.

When you beginning to plan structure of your antivirus network, take into account the peculiarities of licensing multi-server environments. For details, refer to Key Files.

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

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

- the updates are distributed as soon as received,

- the scheduling of updates on Servers becomes unnecessary (except for those Servers which receive updates from the **Dr.Web® GUS** servers via HTTP).

7.6.1. Building a Network with Several ES Servers

Several **ES** Servers can be installed in an anti-virus network. Each anti-virus Agent connects to one of them; each Server with connected anti-virus workstations functions as a separate anti-virus network as described in previous Chapters.

Dr.Web® ES allows to connect such anti-virus networks by transferring data between the anti-virus Servers.

A Server can send to another Server

- software and virus database updates (only one of them is to receive updates from the **Dr.Web® GUS** servers);

It is recommended to schedule a task for updating from the GUS on subordinate **ES** Servers in case the parent **ES** Server is inaccessible. This will allow the Agents connected to a subordinate **ES** Server to receive updated virus databases and program modules. For more, read p. Setting the Dr.Web GUS.

- information on virus events, statistics, etc.

The program provides for two types of connections between the Servers:

- a *parent-child* type of connection, where the principle Server transfers updates to the subordinate one and receives information about events,
- a *peer to peer* connection, where data types and transfer directions are set up individually.

An example of a multi-server structure is presented in Figure 7-1.

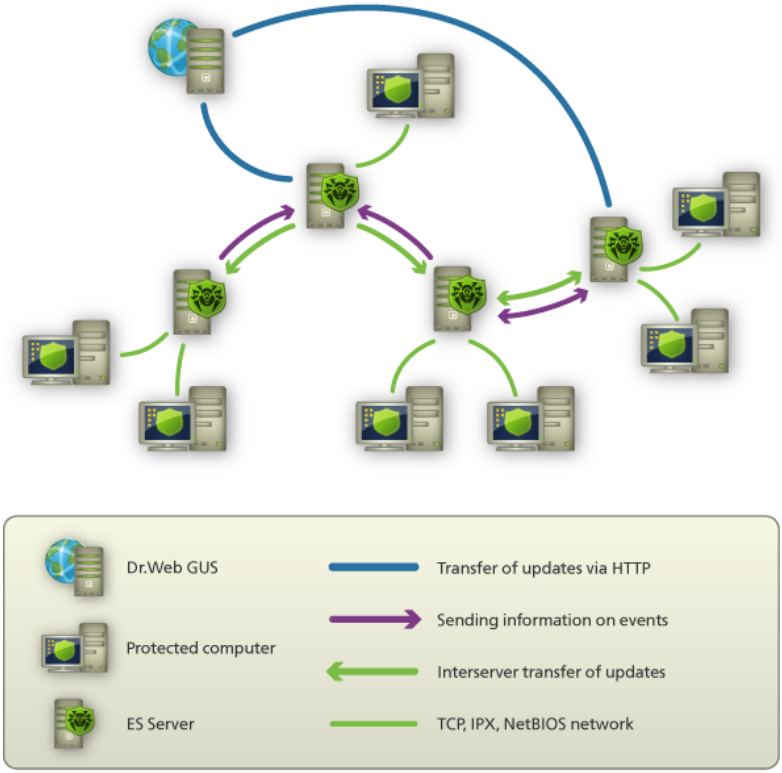

Figure 7-1. A multi-server network

Here are some advantages of a multi-server anti-virus network:

- receipt of updates from the **Dr.Web® GUS** servers by one principle anti-virus Server and their subsequent distribution to the other Servers directly or through intermediates;
- distribution of workstations between several Servers, decreasing the load on each of them;
- consolidation of data from several Servers on one Server; the possibility to view all the data through the Console connected to such Server.

The **Dr.Web® ES** anti-virus monitors and prevents the creation of cyclic data flows.

7.6.2. Setting Connections between the Servers of an Anti-Virus Network

To use several Servers in an anti-virus network, 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. All data flows, connections of the "peer to peer" and "parent-child" types should be indicated. Then, for each Server included into the network connections with any "neighboring" Servers ("neighbors" have at least one dataflow between them) should be set up.

Example: Configure a connection between Parent and Child Servers

1. Make sure that both **ES** Servers operate normally.
2. Make sure that each of the **ES** Servers uses different keys `enterprise.key`.
3. Connect to each of the **ES** Servers by means of the Console and give them "meaningful" names, as it will help prevent mistakes while connecting and administering the **ES** Servers. You can change the names through the **ES** Console menu: **Administration** -> **Configure Dr.Web® Enterprise Server** on the **General** tab in the **Name** entry field. In this example we name the Parent Server `MAIN`, and the Child Server - `AUXILIARY`.
4. On both **ES** Servers, enable the server protocol. To do this, on the **ES** Console **Administration** menu, select **Configure Dr.Web® Enterprise Server**. On the **Protocols** tab, select the **Dr.Web® Enterprise Server** checkbox (see p. Setting the Server Configuration).
5. Restart both **ES** Servers.

6. Connect the **ES** Console to the Child Server (AUXILIARY) and add the Parent Server (MAIN) to the list of neighbor Servers of the Child Server. To do this, on the **Administration** menu, select **Neighborhood**. A window with the hierarchical list of the anti-virus network Servers "neighboring" with the given Server will open. To add a Server to the list, on the context menu of any element (or group of elements), select **Add** (see Figure 7-2).

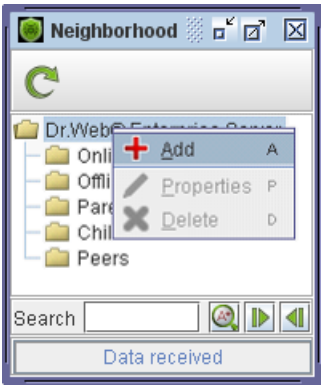

Figure 7-2.

A window to describe the connection between the current Server and the new Server will open (see Figure 7-3). Select the **Parent** type. In the **Name** entry field type the name of the Parent Server (MAIN), in the **Password** field type an arbitrary password to access the Parent Server. To the right of the **Key** field click the **«...»** button and specify the drwcsd.pub key of the Parent Server. In the **Address** field type the address of the Parent Server. Click **OK**.

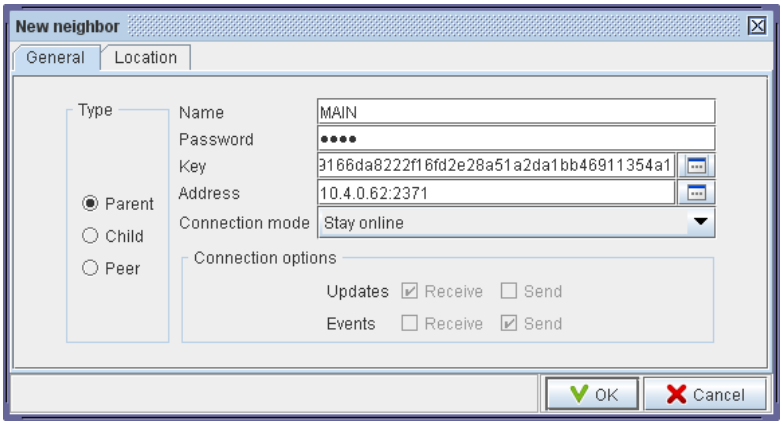

Figure 7-3.

As a result, the Parent Server (MAIN) will be included to the **Parents** and **Offline** folders (see Figure 7-4).

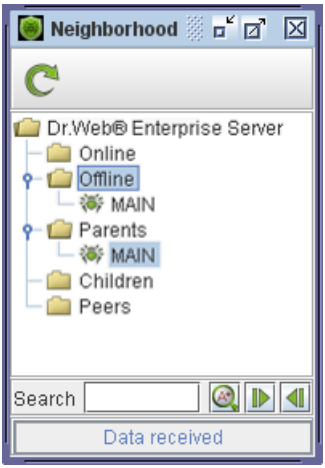

Figure 7-4.

7. Connect the **ES** Console to the Parent Server (MAIN) and add the Child Server (AUXILIARY) to the list of neighbor Servers of the Parent Server. To do this, on the **Administration** menu, select **Neighborhood**. A window with the hierarchical list of the anti-virus network Servers "neighboring" with the given Server will open. To add a Server to the list, on the context menu of any element (or group of elements), select **Add**. In the opened

window (see Figure 7-5) select the **Child** type. In the **Name** entry field type the name of the Child Server (`AUXILIARY`), in the **Password** field type the same password as at step **6**. To the right of the **Key** field click the **«...»** button and specify the `drwcsd.pub` key of the Child Server. Click **OK**.

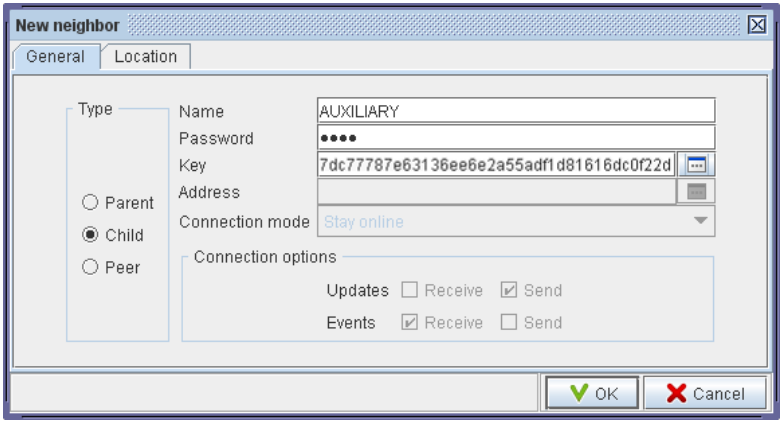

Figure 7-5.

As a result, the Child Server (`AUXILIARY`) will be included to the **Children** and **Offline** folders (see Figure 7-6).

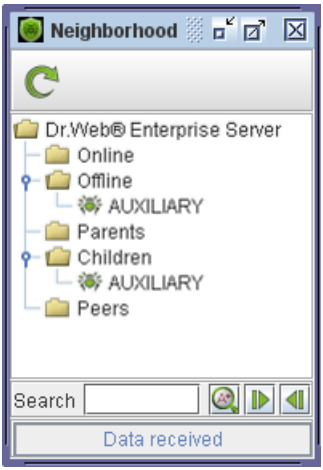

Figure 7-6.

8. Wait until the connection between the Servers has been established (usually it takes not more than a minute). Click the **Refresh** button from time to time to check this. After the Servers have been connected, the Child Server (AUXILIARY) will move from the **Offline** folder to the **Online** folder (see Figure 7-7).

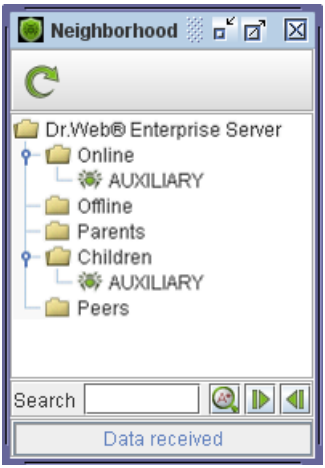

Figure 7-7.

9. Connect the Console to the Child Server (AUXILIARY) to make sure that the Parent Server (MAIN) is connected to the Child Server (AUXILIARY) (see Figure 7-8).

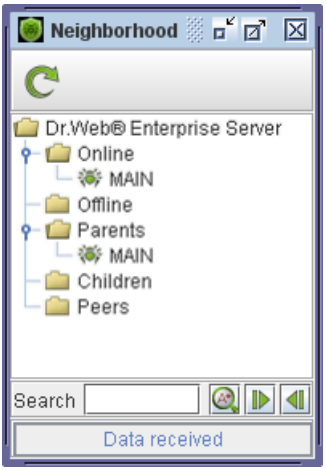

Figure 7-8.

You may not connect two Servers installed with the same license key (`enterprise.key`).

7.6.3. Using an Anti-Virus Network with Several Servers

The peculiarity of a multi-server network is that updates from the **Dr.Web® GUS** servers can be received by a part of the anti-virus Servers (as a rule, one or several parent Servers) and update tasks should be scheduled on these Servers only (for information on how to set Servers' schedule, read p. Setting the Server Schedule). Any Server which has received updates from the **Dr.Web® GUS** servers or some other Servers distributes them immediately to all connected child Servers and those peer Servers for which this option is enabled.

The **Dr.Web® ES** anti-virus automatically monitors the situations when due to an imperfect structure of the network or incorrect Server configuration an update already received is sent again to the same Server, and cancels the updating.

The administrator can receive consolidated data about important events on the anti-virus stations linked to any Server via intersever connections.

To view information on virus events on all Servers linked to the current Server

1. On the **Administration** menu, select **Remote data**. A window with accessible Servers will open (with no data loaded).
2. Click  , to load data into the table.
3. Each line contains data on the total number of entries on the status (the **Status** column), on detected infections (the Infections column), on scanning errors (the **Errors** column), on statistics (the **Statistics** column), on network installations (the **All network installations** column), on the launch and termination of tasks (the **Start/Stop** column) available on this Server. To view any line of the summary statistics in a more suitable form, select it in the table and click  (or double-click the necessary line). A window with a detailed description of this line will open.

If several lines are selected in the table, a detailed description of each of them will be displayed in separate windows.

4. To save the table for printing or further processing, click  **save shown data in CSV format**, or  **save shown data in HTML format**, or  **save shown data in XML format**.
5. To open the summary window with information on the status, detected infections, scanning errors, network installations, the launches and terminations of tasks, as well as the statistics on stations, select the necessary Server or several Servers, and then on the context menu, select an item with necessary information. A window with the table similar to that described in p. Viewing the Statistics will open. The only difference of this table is the presence of the **Server** column.

Chapter 8: Updating the Dr.Web ES Software and Virus Databases

Before updating **Dr.Web® ES** and its components, ensure availability of your Internet connection. Check that the Internet Protocol is properly configured and DNS server settings are specified correctly.

The anti-virus software and virus databases can be updated either manually or through the schedule of a Server or an Agent.

Before updating the anti-virus software and virus databases you should set the configuration of the repository (including access to the **Dr.Web® Global Update System** as described in p. Setting the Dr.Web GUS).

Action which you need to perform in order to upgrade the Server and Console differ depending on the version which you want to install:

1. Update from version **4.44 - 4.44.2** to version **4.44.3**;
2. Update from version **4.33.x** to version **4.44.3**.

For the **1** option, upgrade without uninstall is not supported. You will have to uninstall previous version of the Server and Console and reinstall the new one.

For the **2** option, the upgrade without uninstall is supported.

8.1. Upgrading Dr.Web ES 4.44-4.44.2 to Version 4.44.3

To upgrade to **4.44.3**, it is necessary to remove the Server and Console software **4.44** - **4.44.2** and install the version **4.44.3**.

For Windows OS

After the Server **4.44** - **4.44.2** has been removed, the following files will remain:

- the internal DB `dbinternal.dbs`,
- Server configuration file `drwcsd.conf` and Web Server configuration file `webmin.conf`,
- encryption keys `drwcsd.pri` and `drwcsd.pub`,
- license keys `enterprise.key` and `agent.key`,
- the SSL certificate `certificate.pem`.

When necessary, save other files that you are planning to use in the sequel in another location. For example, report templates in the `\var\templates` catalog.After the installation the new files can be replaced by the backups.

After you uninstall ES Server version 4.44—4.44.2, do the following to install ES Server version 4.44.3:

1. Run the distribution file. A window for choosing the language of the **Installation Wizard** will open. Select the necessary language and click **Next**.
2. A window with information about the program to be installed will open. Click **Next**.
3. A window with the text of the license agreement will open. You should read and accept the agreement. To continue the installation, in the bottom part of the window select **I accept the terms of the license agreement** and click **Next**.
4. A window for selection of license key files will open.
   In the upper field click **Browse**, and then specify the `enterprise.key` license key file for the Server in the standard Windows OS window.

If you want to keep the Server's database of the previous installation, select **Use existing database...**. You will be able to specify the database file later (see step **10**).

Click **Next**.

5. A window for changing the default installation folder a window for changing the default installation folder `C:\Program Files\DrWeb Enterprise Server` will open. If necessary, change the installation folder.
6. Next you can choose the language of the notification templates, set the Agent's shared installation folder (hidden by default) and set up installation logging. If you want the Server to be started automatically after the installation, select the **Start service during setup** checkbox.
7. In the next window select the **Use existing Dr.Web® Enterprise Server encryption keys** checkbox and specify the filenames of existing encryption keys for the Agents to identify the installed Server. Otherwise after the installation it will be necessary to copy the new encryption key to all workstations, on which **ES** Agents have been previously installed.
8. Next you can specify a prearranged Server configuration file instead of that created by the installation program.
9. In the next series of windows the main settings stored in the Server configuration file should be specified (see Appendix G. Server Configuration File).
10. In the dialog box dedicated to database parameters you can set up an internal or an external database of the Server. **IntDB** instructs to use built-in tools of the **Dr.Web® ES** anti-virus. In large networks with 100-200 computers or more, such configuration may slow down the operation. If you want to use an external DBMS, select **ODBC**. Setting the parameters for this variant is described in detail in Appendix B. The Description of the DBMS Settings. The Parameters of the DBMS Driver. After the respective type of the database is selected, click the **Browse** button to the right to specify the database file.
11. In the next dialog box dedicated to network configuration you can set up a network protocol for the Server (it is allowed to create only one protocol, more protocols can be set up later). To limit the local access to the Server, select the **Allow access to Dr.Web (R) Enterprise Console only** checkbox. The Installer, Agents and other Servers (in case of an existing anti-virus network built with **Enterprise Suite**) will not be able

to access the Server. You can change these settings later through Console: **Administration** -> **Dr.Web® Enterprise Server** -> **Protocols**.

Select the **Server detection service** checkbox, if you want the Server to answer broadcast and multicast queries of other Servers.

To specify the default network settings click **Standard** in the bottom of the window. In case you want to limit Server operation only to the internal network interface – `127.0.0.1`, click **Restricted**. With such settings the Server can be administrated only from the Console launched on the same computer, and communicate only with the Agent launched on the same computer. In future after the Server settings have been checked out you will be able to change them.

Click **Next**.

12. In the next window specify an administrator password. Click **Next**. (The window will not appear, if you are using an existing database).
13. Next you are recommended to instruct updating of the repository during the installation. To do this, select the **Update repository** checkbox. Click **Next**.
14. Click **Install**.
15. Further actions of the installation program do not require user intervention.
16. Once the installation is complete, click **Finish**.

Then install the anti-virus Console (see the installation steps in p. Installing the Anti-Virus Server for Windows OS).

After the installation of the Server is completed, run the Console and connect to the anti-virus Server. Update all the components. To do this, on the **Administration** menu, select **Check for updates**. **All Dr.Web® Enterprise Products** is selected by default. Click **OK**. The upgraded anti-virus program is ready for operation.

For UNIX OS

The procedure is the same as that in p. Upgrading Dr.Web ES 4.33.x to Version 4.44.3.

8.2. Upgrading Dr.Web ES 4.33.x to Version 4.44.3

Dr.Web® ES version **4.33** and **4.33.1** can be upgraded to version **4.44.3.** The database of the anti-virus Server and encryption keys will remain the same, so you will not need to reinstall the anti-virus Agents on workstations.

Dr.Web® ES 4.33.x is upgraded to **4.44.3** by installing the new version over the old one. If there are several **ES** Servers in the anti-virus network you can either reinstall all the **ES** Servers as described below, or reinstall only the master Server, the slave Servers will automatically download the repository and upgrade through it.

For Windows OS

After **Enterprise Server 4.44.3** has been installed over **4.33.x**, the following files will remain:

- the internal DB `dbinternal.dbs`,
- Server configuration file `drwcsd.conf` and Web Server configuration file `webmin.conf`,
- encryption keys `drwcsd.pri` and `drwcsd.pub`,
- license keys `enterprise.key` and `agent.key`,
- the SSL certificate `certificate.pem`.

Server and Console **4.33.x** software is removed during the installation automatically. When necessary, save other files that you are planning to use in the sequel in another location. For example, report templates in the `\var\templates` catalog. After the installation the new files can be replaced by the backups.

1. Before starting the installer **4.44.3** disable the Agent and installer protocols through the Console: **Administration** -> **Dr.Web® Enterprise Server** -> **Protocols**.
2. Install the Server software version **4.44.3**. To do this, run the file from the distribution kit. A window for selecting the language of the installation wizard will open. Select the necessary one and click **Next**.

3. An **InstallShield Wizard** window with information on the program selected for installation will open. Click **Next**.
4. A window will open to notify you that the new software is ready to be installed. Click **Install**.

   Then install the anti-virus Console (see the installation steps in the end of p. Installing the Anti-Virus Server for Windows OS).

After the installation is completed, run the Console and connect to the anti-virus Server. Update all the components. To do this, on the **Administration** menu, select **Check for updates**. **All Dr.Web® Enterprise Products** is selected by default. Click **OK**. Enable the Agent and installer protocols (**Administration** menu -> **Dr.Web® Enterprise Server** -> **Protocols**). The upgraded anti-virus program is ready for operation.

If you initially installed Server version 4.32, then you'll need to convert the private encryption key `drwcsd.pri` to the new format. Consult FAQ.

For UNIX system-based systems

All actions must be performed under the **root** administrator account.

If using an internal database:

1. Stop the **ES** Server.
2. Back up the internal DB `dbinternal.dbs`, Server configuration file `drwcsd.conf` and Web Server configuration file `webmin.conf`, encryption keys `drwcsd.pri` and `drwcsd.pub`, license keys `enterprise.key` and `agent.key`, the SSL certificate `certificate.pem` and other files that you are planning to use in the sequel, for example, report templates.
3. Remove **ES** Server software (see p. Uninstalling the Server Software for UNIX system-based Operating Systems).

4. Install the **ES** Server version **4.44.3** (see p. Installing the Anti-Virus Server for UNIX system-based Operating Systems).
5. Put the files specified in step **2** above and the Server configuration file (`drwcsd.conf`) to:
   - for **Debian** OS:
     `/var/opt/drwcs/etc`, except for the public key. Put the latter to `/opt/drwcs/Installer/`
   - for **FreeBSD** OS:
     `/var/drwcs/etc`, except for the public key. Put the latter to `/usr/local/drwcs/Installer/`
   - for **Solaris** OS:
     `/var/drwcs/etc`, except for the public key. Put the latter to `/opt/drwcs/Installer/`
6. Replace the new database file with the file saved at step 2:
   - for **Debian** OS:
     `/var/opt/drwcs/dbinternal.dbs`
   - for **FreeBSD** OS and **Solaris** OS:
     `/var/drwcs/dbinternal.dbs`

For all backup files from the previous Server version (see step 5 and 6) assign the same permissions as those set at the installation of the new Server version.

7. To upgrade the databases, execute the following commands:
   - for **Debian** OS and **Solaris** OS:
     `/etc/init.d/drwcsd upgradedb`
   - for **FreeBSD** OS:
     `/usr/local/etc/rc.d/drwcsd.sh upgradedb`
   - for **other** supported versions:
     ```
     /opt/drwcs/bin/drwcsd
     -var-root=/var/drwcs
     -log=/var/drwcs/log/drwcsd.log
     upgradedb update-db
     ```
8. Generate a new SSL certificate:
   - for **Debian** OS and **Solaris** OS:
     `/etc/init.d/drwcsd selfcert`
   - for **FreeBSD** OS:
     `/usr/local/etc/rc.d/drwcsd.sh selfcert`

- for **other** supported versions:
  `/opt/drwcs/bin/drwcsd -var-root=/var/drwcs -log=/var/drwcs/log/drwcsd.log selfcert`

9. Launch the **ES** Server.

If using an external database:

1. Stop the **ES** Server.
2. Back up the Server configuration file `drwcsd.conf` and Web Server configuration file `webmin.conf`, encryption keys `drwcsd.pri` and `drwcsd.pub`, license keys `enterprise.key` and `agent.key`, the SSL certificate `certificate.pem`.
3. Remove the **ES** Server software (see p. Uninstalling the Server Software for UNIX system-based Operating Systems).
4. Install the **ES** Server version **4.44.3** (see p. Installing the Anti-Virus Server for UNIX system-based Operating Systems).
5. Move the files specified in step 2 above to:
   - for **Debian** OS: to `/var/opt/drwcs/etc`, except for the public key. The latter must be saved to `/opt/drwcs/Installer/`
   - for **FreeBSD** OS: to `/var/drwcs/etc`, except for the public key. The latter must be saved to `/usr/local/drwcs/Installer/`
   - for **Solaris** OS: to `/var/drwcs/etc`, except for the public key. The latter must be saved to `/opt/drwcs/Installer/`

To all backup files from the previous Server version (see step 5) assign the same permissions as those set at the installation of the new Server version.

6. To upgrade the databases, execute the following commands:
   - for **Debian** OS and **Solaris** OS:
     `/etc/init.d/drwcsd upgradedb`
   - for **FreeBSD** OS:
     `/usr/local/etc/rc.d/drwcsd.sh upgradedb`

- for **other** supported versions:

```
/opt/drwcs/bin/drwcsd
-var-root=/var/drwcs
-log=/var/drwcs/log/drwcsd.log
upgradedb update-db
```

7. Generate a new SSL certificate:
   - for **Debian** OS and **Solaris** OS:

```
/etc/init.d/drwcsd selfcert
```

   - for **FreeBSD** OS:

```
/usr/local/etc/rc.d/drwcsd.sh selfcert
```

   - for **other** supported versions:

```
/opt/drwcs/bin/drwcsd
-var-root=/var/drwcs
-log=/var/drwcs/log/drwcsd.log selfcert
```

8. Launch the **ES** Server.

If you installed the Server version 4.32, you need to convert the private key to the new format. See Converting the Private Encryption Key drwcsd.pri of Version 4.32 to the New Format for details.

8.3. Updating Dr.Web ES through the Repository

Server's repository is updated according to the schedule (see schedule settings in p. Scheduled Updates). Software and virus database updates are transferred to the Agents automatically. To update the Server's software, you can use either the installer of a newer version (if available) or the repository, from which you can take the latest updates of the Server's software received from **Dr.Web® GUS** servers.

Updating Server

To update the Server software

1. Disable the use of communication protocols with the anti-virus Agent and the network installer. To do this, on the **Administration** menu of the Console, select **Configure Dr.Web® Enterprise Server**. In the opened window go to the

Protocols tab and clear the **Dr.Web® Enterprise Agent** and the **Dr.Web® Network Installer** checkboxes. Click **OK**. A dialog box requesting to restart the Server will open. Click **Yes**.

2. On the **Administration** menu, point to Configure repository and then select **Entire repository settings**. Make sure that on the **Dr.Web® Enterprise Agent** tab the **Update everything mode** is specified. On the **Dr.Web® Enterprise Console** tab, select for which OS's you want to receive updates. Click **OK**.
3. On the **Administration** menu, point to **Configure repository** and select **Dr.Web® Enterprise Server**. An **Edit Dr.Web® Enterprise Server** window will open. Go to the **Synchronization** tab.
4. The settings specified in this tab disable the Server updating. If you want to receive updates for all platforms, clear the **Use this list** checkbox in the **Only** field.
   - If you want to receive updates for OS **Windows**, the Expression list will look as follows:
     `^common/`
     `^win/`
   - If you want to receive updates for **Linux** OS, the Expression list should look like this:
     `^common/`
     `^unix/`
     `^unix-Linux-`*<Distribution kit>*`/`
     where *<Distribution kit>* stands for a certain OS modification of the Linux family.
   - For **FreeBSD** OS the last line looks as follows: `^unix-FreeBSDxx.x/`.
   - And for **Solaris**: `^unix-SunOSxx.x/`, where `xx.x` stands for your OS version (for more details, read Appendix A. The Complete List of Supported OS Versions).
5. Click **OK**.
6. On the **Administration** menu, select **Check for updates**. By default, it is offered to check for updates for all products. Click **OK**.
7. Stop the Server (on the **Administration** menu, select **Shutdown Dr.Web® Enterprise Server**). The Console will report the Server is disconnected.
8. Go to the Server's installation catalog and make a backup copy of Server configuration files from the `\etc` folder:
   `\etc\*.key`

```
\etc\*.pem
\etc\*.conf
\etc\*.pri
\etc\*.ini
```

9. It is recommended to back up the folders:

```
\bin
\etc
\Installer
\webmin
\var\extensions
\var\templates
\var\update-db
```

10. Then copy the content of the repository to the following folders:

Repository folder	Destination folder
\var\repository\20-drwcs\windows-nt-x86\bin	\bin
\var\repository\20-drwcs\common\Installer	\Installer
\var\repository\20-drwcs\common\webmin	\webmin
\var\repository\20-drwcs\common\etc	\etc
\var\repository\20-drwcs\common\extensions	\var\extensions
\var\repository\20-drwcs\common\templates	\var\templates
\var\repository\20-drwcs\common\update-db	\var\update-db

11. Copy the files backed up at step **8** to the `\etc` folder.

12. Update the database with the following instruction:

- for **Windows** OS:

```
"C:\Program Files\DrWeb Enterprise
Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb  Enterprise Server" upgradedb
"C:\Program Files\DrWeb Enterprise
Server\var\update-db"
```

- for **UNIX** OS:

```
bin/drwcsd -var-root=./var upgradedb
```

`var/repository/20-drwcs/common/update-db`

13.Launch the **ES** Server.

Once the software is successfully updated, the Console of the old version will not be able to connect to the Server. Use the new version of the Console to establish connection to the Server.

Updating Console

To update the Console software

1. Close the active Console.
2. Delete all files and folders from the installation folder.
3. Then copy the content of the repository to the following folders:

Repository folder		Destination folder
For Unix OS		
unix/bin/drwconsole.sh		Installation folder
common/jars		Create `jars` folder in the installation folder
For Windows OS		
Depends on the Windows OS version	\20-drwconsole\windows-nt-x64	Installation folder
	\20-drwconsole\windows-nt-x86	
\20-drwconsole\common\jars\		Create the `\lib\DrWeb` folder in the installation folder

4. Launch the Console.

8.4. Updating the Repository of a Server not Connected to the Internet

If the anti-virus Server is not connected to the Internet, its repository can be updated manually. Copy the repository of another **ES** Server, which has been updated normally. This way is not meant for upgrading.

1. Install the anti-virus Server software on another computer connected to the Internet as described in p. Installing the Anti-Virus Server and the Anti-Virus Console.
2. Stop the two Servers.
3. Start the Server connected to the Internet with the syncrepository switch to update the anti-virus software.

   Example for **Windows** OS:

   ```
   "C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Enterprise Server" syncrepository
   ```
4. Copy the content of the repository catalog of the Server connected to the Internet to the correspondent catalog on the main (working) Server. Usually it is:
   - `var\repository` under **Windows** OS,
   - `/var/drwcs/repository` under **FreeBSD** OS,
   - `/var/opt/drwcs/repository` under **Linux** OS.
5. If the main Server is working under UNIX OS, it is necessary to set the rights of the user created/selected at the installation of the Server to the copied repository.
6. On the main Server execute the command `drwcsd rerepository`.

   Under **Windows** OS the command can be performed both from the *command line*:

   ```
   "C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Enterprise Server" rerepository
   ```

   or from the *Start menu*:

   ```
   Start -> All Programs-> DrWeb Enterprise Server -> Server control -> Reload repository
   ```

7. Start the main Server.

8.5. Manual Updating of the Dr.Web ES Components

Before updating **Dr.Web® ES** and its components, ensure availability of your Internet connection. Check that the Internet Protocol is properly configured and DNS server settings are specified correctly.

To check for updates of Dr.Web ES products on the updates server

1. On the **Administration** menu, select **Check for updates**.
2. In the opened window, **All Dr.Web® Enterprise Suite Products** is selected by default. If you want to update a certain **ES** component, select the necessary one and click **OK**. If the checked component is outdated, it will be updated automatically during the check. Products are updated according to the settings of the repository (read p. Introduction and further).
3. After the check a window with results will appear. To close the window, click **Close**.

To update the software of an anti-virus station through the Console

1. On the context menu of the workstation or a group, select **Force stations update**.
2. On the opened submenu, select the necessary forced update mode
   - **Update failed components** instructs to reset the error state and update only those components that failed at the previous update;
   - **Speed up normal update** instruct to update only those components for which there is a new update on the server.
   - **Update all components** instructs to force the update of all components, including those updated successfully.

The same operation can be carried out with the help of the anti-virus Agent.

To update the software of an anti-virus station through the ES Agent

1. Permit the user of the given workstation to change the local policy (for information on how to do it, read p. Setting Users' Permissions).
2. On the context menu of the Agent icon, select **Re-sync now**.
3. On the opened submenu, select
   - **Only failed components**, if you want to update only those components the updating of which was failed and to reset the error state,
   - **All components**, if you want to launch updating of the failed components as well as other components.

8.6. Scheduled Updates

You can make a schedule on a certain anti-virus Server to regularly check for software updates and synchronize products in the repository with new versions on another anti-virus Server or the **GUS** server.

For more details on the schedule, see p. Setting the Server Schedule.

To schedule product updates on the Server

1. On the **Administration** menu, select **Dr.Web® Enterprise Server schedule**.
2. To add a task, on the context menu of the list of tasks, select **Add**.
3. Assign a name to the task in the **Name** field.
4. In the opened window, in the **Action** field select **Update**.
5. In the **Time** drop-down list, set the time span of running the task and specify time according to the time span selected (similarly to setting the time in the schedule of a workstation, read p. Scheduling Tasks on a Workstation above).
6. In the **Product** drop-down list, select the type of product to be updated by this task:

- **Dr.Web® Enterprise Agent**
  Dr.Web® Enterprise Server
  Dr.Web® Enterprise Updater
  Dr.Web® for Unix
  Dr.Web® Virus Bases
  Dr.Web® Enterprise Console
- **All Dr.Web® Enterprise Products**, if you want to set a task for updating all **Dr.Web® ES** components.

7. Click **OK** to accept the changes or **Cancel** to abort the changes.

8.7. Updating Mobile Agents

If your computer (laptop) has no connection to the **ES** Server(s) for a long time, to receive updates opportunely from the **Dr.Web® GUS**, you are well advised to set the Agent in the mobile mode of operation. To do this, on the context menu of the Agent icon in the notification area of the **Taskbar**, select **Mobile mode** -> **Active**. The icon will turn yellow.

In the mobile mode the Agent tries to connect to the Server three times and, if unsuccessful, performs an HTTP update. The Agent tries continuously to find the Server at interval of about a minute.

The option **Mobile mode** will be available on the context menu provided that the mobile mode of using the **Dr.Web® GUS** has been allowed in the station's permissions (for more, read p. Setting Users' Permissions).

To adjust the settings of the mobile mode, select **Mobile mode** -> **Settings**. In the **Update period** field set the frequency of checking the availability of updates on the **GUS**. If necessary, select the **Only when connected to Internet** checkbox.

When using a proxy server, select the **Use proxy to transfer updates** checkbox and below specify the address and the port of the proxy server, and the parameters of authorization.

In the mobile mode, to initiate updating immediately, select **Mobile mode** -> **Start update**.

When the Agent is functioning in the mobile mode, the Agent is not connected to the anti-virus **ES** Server. All changes made for this workstation at the Server, will take effect once the Agent's mobile mode is switched off and the connection with the Server is re-established. In the mobile mode only virus databases are updated.

To switch off the mobile mode, on the context menu of the Agent icon, select **Mobile mode** and clear the **Active checkbox**. The color of the icon will change from yellow to green and the Agent will be reconnected to the Server.

8.8. Replacing Old Key Files with New Ones

During the installation of the **Dr.Web® ES** anti-virus you will be asked to provide files containing the Server key and the key for workstations (read p. Installing the Anti-Virus Server and the Anti-Virus Console; for more information on key files read p. Key Files). Once your keys expire, some components of the program will not operate. To restore the full functionality of the **Dr.Web® ES** anti-virus, you should obtain and import new key files.

To install new key files in Dr.Web ES

1. Replace `enterprise.key` in the `etc` subfolder of the installation folder of the Server.
2. Restart the Server using standard Windows OS tools or the corresponding command from the **Start menu** (you can also use the Console).
3. By means of the Console import the new Agent key for the **Everyone** group. To do this, in the catalog of the anti-virus network in the Console window select the **Everyone** group, and on its context menu, select **Import key**.
4. In the next window select the new key file for workstations (`agent.key`) and click **OK**.

Appendices

Appendix A. The Complete List of Supported OS Versions

For the ES Server

Unix-FreeBSD-5.1
Unix-FreeBSD-5.2
Unix-FreeBSD-5.3
Unix-FreeBSD-5.4
Unix-FreeBSD-5.5
Unix-FreeBSD-6.0
Unix-FreeBSD-6.1
Unix-FreeBSD-6.2
Unix-FreeBSD-6.3
Unix-FreeBSD-7.0
Unix-FreeBSD-amd64-6.2
Unix-FreeBSD-amd64-6.3
Unix-FreeBSD-amd64-7.0
Unix-Linux-ALT-3.0
Unix-Linux-ALT-Server-4.0
Unix-Linux-ASP-10
Unix-Linux-ASP-11
Unix-Linux-ASP-12
Unix-Linux-Debian-etch
Unix-Linux-Debian-sarge
Unix-Linux-Debian-sid
Unix-Linux-Debian-woody
Unix-Linux-generic-glibc2.2
Unix-Linux-generic-glibc2.3

Unix-Linux-generic-glibc2.4
Unix-Linux-generic-glibc2.5
Unix-Linux-generic-glibc2.6
Unix-Linux-generic-glibc2.7
Unix-Linux-Mandrake-10.1
Unix-Linux-Mandriva-2006
Unix-Linux-Mandriva-2008
Unix-Linux-Mandriva-Corporate Server-4
Unix-Linux-RedHat-Enterprise Linux-4
Unix-Linux-RedHat-Enterprise Linux-5
Unix-Linux-RedHat-FedoraCore-5
Unix-Linux-RedHat-FedoraCore-6
Unix-Linux-RedHat-FedoraCore-7
Unix-Linux-RedHat-FedoraCore-8
Unix-Linux-SuSe-9.3
Unix-Linux-SuSe-10
Unix-Linux-SuSe-Enterprise Server-10
Unix-Linux-Ubuntu-6.06
Unix-Linux-Ubuntu-7.04
Unix-Linux-Ubuntu-8.04
Unix-Linux-x86_64-Debian-etch
Unix-Linux-x86_64-generic-glibc2.3
Unix-Linux-x86_64-generic-glibc2.4
Unix-Linux-x86_64-generic-glibc2.5
Unix-Linux-x86_64-generic-glibc2.6
Unix-Linux-x86_64-generic-glibc2.7
Unix-Linux-x86_64-generic-glibc2.8
Unix-Linux-x86_64-Mandriva-2008
Unix-Linux-x86_64-RedHat-Enterprise Linux-5
Unix-Linux-x86_64-RedHat-FedoraCore-8
Unix-Linux-x86_64-SuSe-ES-10
Unix-Linux-x86_64-Ubuntu-8.04

Unix-Solaris-9

Unix-Solaris-10

Unix-Solaris-10-sparc32 (Sparc V9 processor; UltraSparc or later)

Unix-Solaris-10-sparc64 (Sparc V9 processor; UltraSparc or later)

Windows:

- 32 bit:

Windows NT4 (SP6a)

Windows 2000 Professional (SP4)

Windows 2000 Server (SP4)

Windows XP Professional (SP3)

Windows XP Home (SP3)

Windows Server 2003 (SP2)

Windows Vista (SP1)

- 64 bit:

Windows Server 2003 (SP2)

Windows Vista (SP1)

For the ES-agent and anti-virus package

- 32 bit:

Windows 98

Windows Millennium Edition

Windows NT4 (SP6a)

Windows 2000 Professional (SP4)

Windows 2000 Server (SP4)

Windows XP Professional (SP3)

Windows XP Home (SP3)

Windows Server 2003 (SP2)

Windows Vista (SP1)

- 64 bit:

Windows Server 2003 (SP2)

Windows Vista (SP1)

SpIDer Guard

- 32 bit:

Windows 98
Windows Millennium Edition
Windows NT4 (SP6a)
Windows 2000 Professional (SP4)
Windows 2000 Server (SP4)
Windows XP Professional (SP3)
Windows XP Home (SP3)
Windows Server 2003 (SP2)
Windows Vista (SP1)

For the Console

Unix-like (JRE not included, download from java.sun.com):
solaris x86/ sparc
linux .rpm x86/x86_64
linux .deb x86/x86_64
generic unix / MacOS X (in tar.bz2 and .zip for manual installation)

Windows (JRE included):

- 32 bit:

Windows 2000 Professional (SP4)
Windows 2000 Server (SP4)
Windows XP Professional (SP3)
Windows XP Home (SP3)
Windows Server 2003 (SP2)
Windows Vista (SP1)

- 64 bit:

Windows Server 2003 (SP2)
Windows Vista (SP1)

Appendix B. The Description of the DBMS Settings. The Parameters of the DBMS Driver

When setting access to DBMS for storage and processing of data, use the parameters described below for various DBMS types.

Table B-1. Built-in DBMS (IntDB) parameters

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

Table B-2. ODBC parameters (only in the version for Windows OS)

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 value means "use default of the SQL server". More information can be found at http://www.oracle.com/technology/oramag/oracle/05-nov/o65asktom.html.

The database is initially created on the SQL server with the above mentioned parameters. It is also necessary to set the ODBC driver parameters on the computer where the anti-virus Server is installed. **To do this**

1. In Windows OS **Control Panel**, select **Administrative tools**; in the opened window click **Data Sources (ODBC)**. The **ODBC Data Source Administrator** window will open. Go to the **System DSN** tab.
2. Click **Add**. A window for selecting a driver will open.
3. Select the SQL Server item in the list and click **Finish**. The first window for setting access to the DB server will open.
4. Enter access parameters to the data source (the same as in the settings of the anti-virus Server). If the DB server is not installed on the same computer as the anti-virus Server, in the Server field specify its IP address or name. Click **Next**. The next window will open.
5. Specify the necessary DB access settings in this window. Click **Client configuration**. A window for selecting and setting the network protocol will open.
6. In the Network libraries field select a network library for TCP/IP or Named Pipes (recommended). If the DB server is not installed on a local computer, specify its name or IP address in the **Server alias** and **Server name** fields. Click **OK**. This window will close and the previous window for setting the driver will be available again. Click **Next**. The next window will open.
7. Check that the **Only when you disconnect** option, the **Use ANSI quoted identifiers** and the **Use ANSI nulls**, **paddings** and **warnings** checkboxes are selected. Click **Next.** The last window for setting access will open.

If ODBC driver settings allow you to change the language of SQL server system messages, select **English**.

8. Select the necessary parameters. When you are done, click **Finish**. A window with the summary of the specified parameters will open.
9. To test the specified settings, click **Test Data Source**. After you see a notification of a successful test, click **OK**.

As an external database of the anti-virus Server for Windows OS you can use Oracle DBMS. In this case you should install the ODBC driver supplied with the DBMS. We strongly advise you not to use Oracle ODBC driver, distributed by Microsoft. The procedure of setting this driver is the same as setting the driver for SQL.

When using Microsoft SQL Server 2005 deploy the ODBC driver supplied with this DBMS.

In large anti-virus networks (over 100 stations), it is recommended to use the **PostgreSQL** external database, which is more fault-resistant than internal databases. Please download the latest available version of this free product, otherwise do not use the **PostgreSQL** client earlier than **7.4.**

For more information about conversion to the external database see p. Changing the Type of the DBMS for Dr.Web Enterprise Suite.

For more information about installation of the anti-virus Server using external database see step 10 in p. Installing the Anti-Virus Server for Windows® OS.

Please mind that the ANSI version of the ODBC driver can be used starting from PostgreSQL 8.2.4 version only. The Unicode ODBC driver will work fine in all versions.

Table B-3. PostgreSQL parameters (only in the version for UNIX OS)

Name	Default value	Description
`host`	*<UNIX domain socket>*	PostgreSQL server host

Name	Default value	Description
port		PostgreSQL server port or name extension of the socket file
dbname	drwcs	Database name
user	drwcs	User name
password	drwcs	Password
options		Debug /trace options for sending to the Server
tty		File or tty to output at debug
requiressl		1 instructs to request a SSL connection; 0 does not instruct to make the request
max_expr_depth		Set a 2 or 2.5 times greater value than the number of workstations expected in the anti-virus network.

More information can be found at http://www.postgresql.org/docs/7.4/static/libpq.html.

Appendix C. The Description of the Notification System Parameters

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

Table C-1. E-mail notifications (the drwemail driver):

Parameter	Default value	Description
HOST	127.0.0.1	SMTP host
PORT	25	SMTP port
USER		SMPT user
PASS		SMTP password
DEBUG	NO	Debug mode
FROM	drwcsd@localhost	Sender address
TO	root@localhost	Recipient address

Table C-2. Notifications through Windows Messenger (the drwwnetm driver), for Windows OS version only:

Parameter	Default value	Description
TO	Admin	Computer network name

Appendix D. The Parameters of the Notification System Templates

The text for messages (sent by e-mail or Windows Messenger) is generated by a Server's component named the templates processor on the basis of the templates files.

A template file consists of text and variables enclosed in braces. When editing a template file, the variables listed below can be used.

The templates processor does not perform recursive substitutions.

The variables are written as follows:

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

Table D-1. Notation of variables

Variable	Value	Expression	Value
SYS.TIME	10:35:17:456	{SYS.TIME:5}	10:35:17:456
SYS.TIME	10:35:17:456	{SYS.TIME:3:5}	35:17
SYS.TIME	10:35:17:456	{SYS.TIME:3:-12}	35:17:456
SYS.TIME	10:35:17:456	{SYS.TIME:3:12}	35:17:456
SYS.TIME/10/99	99:35:17.456	{SYS.TIME/10/99/35/77}	99:77:17.456

In case a substitution is used (see the last row), there is no limitation for the number of substitution pairs.

System variables (allowed in Subject, Headers):

- `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,
- `SYS.BRANCH` — system version (Server and Agents).

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

Shared variables of messages (the Agent):

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

Shared variables of messages (Server's updating subsystem):

- `GEN.CurrentRevision` — current version identifier,
- `GEN.NextRevision` — updated version identifier,
- `GEN.Folder` — product location folder,
- `GEN.Product` — product description.

Message variables united according to message types (for the Agent):

Administrator_Authorization_Failed:

- MSG.Login — login,
- MSG.Address — Console network address;

Approved_Newbie:

- MSG.AdminName — administrator name,
- MSG.AdminAddress — administrator Console address;

AutoApproved_Newbie: no variables are available;

Awaiting_Approval: no variables are available;

Cannot_Add_Station:

- MSG.ID — station UUID;

Connection_Terminated_Abnormally:

- MSG.Reason — reason for the termination;

Infection:

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

Installation_Bad:

- MSG.Error — error message;

Installation_OK: no variables are available;

License_Limit:

- MSG.Used — number of stations in the base,

- `MSG.Licensed` — permitted by license,

  is sent when the number of registered stations is approaching the license limit, namely less than 5% of the license limit or less than two stations is unused;

Near_Max_Stations:

- `MSG.Used` — number of stations in the base,
- `MSG.Licensed` — permitted by license,
- `MSG.Percent` — the percentage of free licenses,

is sent at every Server launch in case the Server is launched with a key allowing a lesser number of stations than it already has;

Newbie_Not_Allowed: no variables are available;

Not_Seen_For_A_Long_Time:

- `MSG.StationName` — station name,
- `MSG.StationID` — station UUID,
- `MSG.DaysAgo` — number of days since the last visit,
- `MSG.LastSeenFrom` — address the station was seen at last time;

Processing_Error:

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

Rejected_Newbie:

- `MSG.AdminName` — administrator name,
- `MSG.AdminAddress` — administrator Console address;

Station_Already_Logged_In:

- `MSG.ID` — station UUID,

- MSG.Server — ID of the Server at which the station is registered,

is sent, if the station is already currently registered at this or another Server;

Station_Authorization_Failed:

- MSG.ID — station UUID,
- MSG.Rejected — values: rejected — access to a station is denied, newbie — there was an attempt to assign the "newbie" status to a station;

Statistics:

- MSG.Component — component name,
- MSG.ServerTime — event receipt 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;

Too_Many_Stations:

- MSG.ID — station UUID,

is sent when a new station cannot log in on the Server due to the license limitations;

Unknown_Administrator:

- MSG.Login — login,
- MSG.Address — network Console address;

Unknown_Station:

- MSG.ID — UUID of unknown station,

- `MSG.Rejected` — values: `rejected` — access for a station is denied; `newbie` — there was an attempt to assign the "newbie" status to a station;

`Update_Failed`:

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

`Update_Wants_Reboot`:

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

Message variables, according to messages (for Server's updating subsystem):

`Srv_Repository_Cannot_flush`: no variables are available;

`Srv_Repository_Frozen`: no variables are available;

`Srv_Repository_Load_failure`:

- `MSG.Reason` — message on the cause of the 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 name in a separate line),
- `MSG.Replaced` — list of replaced files (each name in a separate line),
- `MSG.Deleted` — list of deleted files (each name in a separate line);

`Srv_Repository_UpdateFailed`:

- `MSG.Error` — error message,
- `MSG.ExtendedError` — detailed description of the error;

Srv_Repository_UpToDate: no variables are available.

The variables of the last template do not include the files marked as "**not to be notified of**" in the product configuration file, read F1. The Syntax of the Configuration File .config.

The variables of the Server messages about the coming license expiration.

Key_Expiration:

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

Appendix E. The Specification of Network Addresses

In the specification the following conventions are taken:

- variables (the fields to be substituted by concrete values) are enclosed in angle brackets and written in italic,
- permanent text (remains after substitutions) is written in bold,
- optional elements are enclosed in brackets,
- the defined notion is placed on the left of the `::=` character string, and the definition is placed on the right (as in the Backus-Naur form).

E1. The General Format of Address

The network address looks as follows:

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

By default, *<protocol>* has the TCP value, IPX and NetBIOS are also possible. The default values of *<protocol-specific-part>* are determined by the application.

IP addresses:

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

  <ip-address> can be either a DNS name or an IP address separated by periods (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 hexadecimal numbers, *<mac-address>* must contain 12 hexadecimal numbers.

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

<*socket-number*> must contain 4 hexadecimal numbers.

Connection-oriented protocol:

<*protocol*>/ <*socket-address*>

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

NetBIOS addresses:

- Datagram-oriented protocol:
  `nbd/NAME[:PORT[:LANA]]`
- Connection-oriented protocol:

  `nbs/NAME[:PORT[:LANA]]`

  where `NAME` — NetBIOS computer name, `PORT` — port (by default 23), `LANA` — number of the network adapter (important for NetBEUI).

Examples:

1. `tcp/127.0.0.1:2371`
   means a TCP protocol, port `2371` on an interface `127.0.0.1`.
2. `tcp/[::]:2371`
   means a TCP protocol, port `2371` on an IPv6 interface `0000.0000.0000.0000`
3. `localhost:2371`
   the same.
4. `tcp/:9999`
   value for the Server: the default interface depending on the application (usually all available interfaces), port `9999`; value for client: the default connection to the host depending on the application (usually localhost), port `9999`.
5. `tcp/`
   TCP protocol, default port.
6. `spx/00000000.000000000001:2371`

   means socket SPX loopback `0x2371`.

Datagram-oriented protocol:

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

Examples:

1. `udp/231.0.0.1:2371`
   means using a multicast group `231.0.0.1:2371` on an interface depending on the application by default.
2. `udp/[ff18::231.0.0.1]:2371`
   means using a multicast group `[ff18::231.0.0.1]` on an interface depending on the application by default.
3. `udp/`
   application-dependent interface and endpoint.
4. `udp/255.255.255.255:9999-myhost1`
   using broadcasting messages on port `9999` on `myhost1` interface.

E2. The Addresses of Dr.Web Enterprise Server

Receipt of connections:

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

By default, depending on *<connection-protocol>*:

- `tcp/0.0.0.0:2371`
  which means "all interfaces (excluding those with IPv6 addresses), port `2371`";
- `tcp/[::]:2371`
  which means "all IPv6 addresses, port 2371";
- `spx/00000000.000000000001:2371`
  which means "all interfaces, port `0x2371`";
- `nbs/drwcs:23:0`
  which means using NetBIOS stream protocol, port `23`, computer `drwcs`.

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
  which means using a multicast group 231.0.0.1:2371 for all interfaces;
- udp/[ff18::231.0.0.1]:2371-[::]:0
  which means using a multicast group [ff18::231.0.0.1:2371] on all interfaces;
- ipx/00000000.FFFFFFFFFFFF:2371-00000000.000000000000
  which means receipt of broadcasting messages on socket 0x2371 for all interfaces.
- nbd/drwcs:23:0
  which means using NetBIOS datagram protocol, port 23, computer drwcs.

E3. The Addresses of Dr.Web Enterprise Agent/ Installer

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,
- tcp/[::]:2371
  means loopback port 2371 for IPv6;
- spx/00000000.000000000001:2371
  means loopback socket 0x2371.

<drwcs-name> Server location 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 a TCP connection using a multicast group `231.0.0.1:2371` for all interfaces,

- `drwcs@ipx/00000000.FFFFFFFFFFFF:2371-00000000.000000000000`

  location of a Server with the `drwcs` name for an SPX connection using broadcasting messages on socket `0x2371` for all interfaces.

Appendix F. Administration of the Repository

To administrate the functions of the repository, the following files located in the program root folder are used:

- Configuration file `.config` specifies the set of files and the parameters of the updates server. The file has a text format, its structure is described below in Appendices F1. The Syntax of the Configuration File .config and F2. The Meaning of .config File Instructions.
- Status file `.id` displays the generalized state of a product (revision number and incremental number of transaction). The format is described below in Appendix F3. .id Files.

When setting up interserver links for product mirroring (read p. Peculiarities of a Network with Several Anti-Virus Servers), 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, use identical configuration,
- for subordinate Servers, disable synchronizing of components through HTTP protocol or keep the configuration identical.

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

F1. The Syntax of the Configuration File .config

The configuration file is a sequence of words separated by separators. A separator is any sequence of the following characters: space, tab, carriage return, line feed.

A word beginning with a semicolon (*;*) 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 a number sign (#) means the beginning of a stream comment; the rest of the word is specified by the end-of-comment marker.

Example:

```
123 456 #COMM from here there is a comment COMM here it is already ended
```

To include a character into a word, a ' prefix (apostrophe) is used — it is a special separating character for the given word (in other words, this character 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 characters: apostrophe, semicolon, number sign (' , ; , #) , it must be separated by special separator characters, as described above.

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

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

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

The meaning of instructions is explained in Appendix F2. The Meaning of .config File Instructions.

The format of instructions is described by the following conventions:

- [...] — a fragment of the configuration file (the 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, etc. times.
- `<...>` — a value specified by the user.

Example:

```
[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-only{   []0+ }]1-
[notify-ignore{ []0+ }]1-
[notify-off{    [update]1- [delay]1-
                [flushfail]1- [loadfail]1- }]1-
```

F2. The Meaning of .config File Instructions

The description instruction

The `description` instruction sets a product name which is displayed in the Console. If this instruction is unavailable, the name of the respective folder of the product is used as the product name.

Example:

```
description '"Dr.Web® Enterprise Agent"
```

The sync-with instruction

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 regarded the port number for the HTTP server and 3128 for the 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 and proxy-HTTP authentication.

Constant HTTP redirects (code 301) are cached in memory till server reboot.

Example:

```
 sync-with{
 http{ esuite.msk3.drweb.com /update }
 http{ esuite.msk4.drweb.com /update }
 http{ esuite.msk.drweb.com  /update }
 http{ esuite.us.drweb.com   /update }
 http{ esuite.jp.drweb.com   /update }
}
```

The sync-only instruction

The `sync-only` instruction explicitly specifies the sets of filenames (specified both by regular expressions in a simple form as shown in this section, and in full form `qr{}`, as shown in p. Launching and Terminating Anti-Virus Scanning on Workstations) which are subject to synchronization. If the instruction is absent, by default, the whole content of the folder will be synchronized (excluding files whose names begin with a period).

Example:

`sync-only{^common/drw.*vdb$}`

instructs to update only virus databases.

The sync-ignore instruction

The `sync-ignore` instruction explicitly specifies the set of files, which are not subject to synchronization.

If some files have been locally added to a product (which were 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 synchronization.

The sync-delay instruction

The `sync-delay` instruction sets the list of files which, if changed, disable the product's transition to a new revision. 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 Appendix F3. .id Files).

Examples:

- The 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

The `state-only` and `state-ignore` instructions set (limit) the list of files for distribution.

Example:

For the anti-virus Agent:

- no interface language, except for Russian, should be received,
- no components designed for Windows 98 OS, Windows Me OS should be received.

```
sync-ignore{
```

```
    ; As soon as the listed files are in the
    ; repository, they are to be propagated.
    ; Therefore, they should be deleted or
    ; listed in state-ignore{ } or full
    ; synchronization in this
    ; configuration should be made

;^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

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. Setting Alerts).

The repository generates the following types of notifications:

- `update` — when a product is successfully updated,
- `delay` — when a transaction is frozen,
- `flushfail` — when a flush error occurs,
- `loadfail` — when a load error occurs.

By default, all the types are allowed.

The `notify-off` instruction allows to disable certain 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 present in a file, the following rule is used:

- `sync-only` is applied first. Files not specified 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 rule is applied to the application order of `state-only` and `state-ignore`.

F3. .id Files

The *product's status file* is a text file in which the Server logs the revisions numbers of the product. Usually, the file contains a single number (the current revision number). The product will be synchronized if only the revision number on the **GUS** server is more than the current number. 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 subcatalogs with files of the following type:
   <original file name>.<new_revision>.
3) The result of the transaction is written to the `.id` file.
   This can be a normal state but with a new number, or a "frozen" state (frozen), if the `sync-delay` rule has worked:
   <new_revision> *<previous_revision>* `frozen`
4) If the state is not "frozen", new files replace the original files.

When the Server is rebooted after the `.id` file is analyzed, incomplete transactions "roll back", otherwise, step **4)** is performed.

F4. Examples of Administrating the Repository with a Modification of the Status File

Full synchronization of a product:

- stop the Server,
- delete the content of the product's folder, except for the `.id` and the `.config` files,
- write `0` to the `.id` file,
- launch the Server,
- update the product.

`0` revision has a special meaning, as it disables propagation, therefore the "`empty`" status 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,
- update the product.

Shift from the "frozen" status to a new version:

- replace the content of the `.id` file
  <new_revision> *<previous_revision>* `frozen`
  with
  <new_revision>,
- restart the Server,
- update the product.

Roll back from the "frozen" status to the previous version:

- replace the content of the `.id` file
  <new_revision> *<previous_revision>* `frozen`
  with
  <new_revision previous_revision>,
- restart the Server,
- update the product.

At future attempts to synchronize with the previous configuration and to the same *<new revision>*, the repository will go into the "`frozen`" status again. A roll back is reasonable when a suitable revision is available (for example, after successful tests in the lab) to download it or when changing the configuration.

Appendix G. Server Configuration File

The `drwcsd.conf` Server configuration file resides by default in the `etc` subfolder of the Server root folder. If the Server is run with a command line parameter, a non-standard location and name of the configuration file can be set (for more read Appendix H5. Dr.Web Enterprise Server).

The configuration file has a text format. The main structural elements of this file are words, separated by separators — spaces, tabs, carriage returns, line feeds, and format characters. In addition, a sequence of characters included in straight quotation marks `"..."` is considered a word.

Special sequences of two characters beginning with an ampersand (`&`) can be included in a word, not breaking it. They are interpreted as follows:

- `&&` — as an ampersand itself,
- `&r` — carriage return,
- `&t` — tab,
- `&n` — line feed,
- `&v` — vertical tab,
- `&f` — format character,
- `&b` — backspace character,
- `&e` — equal sign (=),
- `&l` — vertical bar (|),
- `&s` — space.

An ampersand (`&`) at the end of a line is equal to `&n`.

Thus, a usual ampersand (which is not used to set a special sequence) should be doubled.

Comments begin with a semicolon 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. Instructions can be followed by instructions parameters (one or several words).

Possible instructions and their parameters are described below. The sequence of instructions in a file is inessential. The parameters (fragments of parameters) set by a user are in angle brackets.

- `Name` *<name>*

  Defines the name of the Server it will respond to when the Server is being searched for by the Agent or the administrator Console. The default value — an empty line ("") — means using the computer name.

- `Threads` *<number>*

  Number of Server threads which are serving clients. By default it is set to 5. It is not advisable to change this parameter unless recommended by the customer support.

- `DBPool` *<number>*

  Number of database connections with the Server. For Windows OS and UNIX OS servers the parameter is set to 2 by default. It is not advisable to change this parameter unless recommended by the customer support.

- `Newbie` *<mode>*

  Access mode of new stations, can have the `Open`, `Close` or `Approval` values (by default, it is Approval. Read more in p. New Stations Approval Policy).

- `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=`*<catalog>*
  `ID=`*<client_identifier>*
  `User=`*<user>*
  `Password=`*<password>*
  `Proxy=`*<proxy_server>*
  `ProxyUser=`*<proxy_user>*

ProxyPassword=*<proxy_password>*"

Above is described a web server where **ES** will publish its statistics on detected viruses. The upload span is set in minutes, the default value is 30. It is not recommended to set the upload span to more than one hour.

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 Server key file (`enterprise.key`).

The User and the Password fields describe the authorization on the web server, other fields determine the proxy server and the authorization on it. By default, the fields are empty (no authorization required).

To get access to data collected on the statistics server, contact the customer support at support@drweb.com.

- `Encryption` *<mode>*

  Traffic encryption mode. Possible values: Yes, No, Possible (by default Possible). For more read p. Traffic_Encryption_and Compression.

- `Compression` *<mode>*

  Traffic compression mode. Possible values: Yes, No, Possible (by default No). For more read p. Traffic_Encryption_and Compression.

- `ConsoleAccess`, `InstallAccess`, `AgentAccess` and `LinksAccess` parameters are not displayed in the configuration file unless the **Use this ACL** checkbox is selected (for more see p. Setting_the_Server_Configuration). If this checkbox is selected, the displayed value for disabled parameters is "none". For enabled parameters the specified addresses will be displayed.

- `Database` *<DRIVER>* `from` *<PATH>* `using` *<PARAMETERS>*

  Determination of the database. <*DRIVER*> — database driver name, <PATH> — path where the driver is to be loaded from, <*PARAMETERS*>— connection parameters between the Server and the database. Read more in p. Setting_the_Mode_of Operation with Databases.

This instruction can be used only once in the configuration file.

- `Alert` *<DRIVER>* `from` *<PATH>* `using` *<PARAMETERS>*

  Determination of the "annunciator". *<DRIVER>* — annunciator driver name, *<PATH>* — path where the driver is to be loaded from, *<PARAMETERS>*— annunciator parameters. Read more in p. Setting Alerts.

This instruction can be used only once in the configuration file.

In this and in the next instruction the parameters in the using field are separated by spaces. The parameter name is separated from the value by an equal sign (=) (should not be surrounded by spaces). If the parameter can have more than one value, they are separated from each other by the vertical bars (|). If the parameter value contains equal signs, vertical bars or spaces, they are replaced with the `&&e`, `&&l`, `&&s` sequences accordingly.

- `Transport` *<NAME>* *<STREAM>* *<DATAGRAM>*

  It determines the transport protocols and assigns them to network interfaces. *<NAME>* — Server name set as in the name instruction above, if an empty line is specified, the name is taken from name. *<STREAM>* (for example, `tcp/`), *<DATAGRAM>* (for example, `udp/`) have the format described in Appendix D. The Parameters of the Notification System Templates.

- `Disable Message` *<message>*

  To disable sending messages of a specific type; possible parameter values: message type; the full list of message types is in the `var/templates` folder.

- `Disable Protocol` *<protocol>*

  Disable using of one of the Server protocols; possible values are AGENT, SERVER, INSTALL, CONSOLE. The SERVER protocol is disabled by default. Read more in p. Setting the Server Configuration.

Disabling unnecessary protocols saves system resources.

- `ShowHostNames=<value>`

  Enable computer domain names in the log instead of the TCP address. Possible values: `Yes` or `No`.

- `ReplaceNetBIOSNames=<value>`

  Enable replacing computer NetBIOS names with the DNS name. Possible values: `Yes` or `No`.

Appendix H. Command Line Parameters of the Programs Included in ES

H1. Introduction

Command line parameters have a higher priority than the default settings, or other constant settings (set in the Server configuration file, Windows OS registry, etc.). In some cases, the parameters specified at launch also predetermine the constant parameters. Such cases are described below.

Some command line parameters have a form of a switch — they begin with a hyphen. Such parameters are also called switches, or options.

Many switches can be expressed in various equivalent forms. Thus, the switches which imply a logical value (`yes/no`, `disable/enable`) have a negative variant, for example, the `-admin-rights` switch has a pair `-no-admin-rights` with the opposite meaning. They can also be specified with an explicit 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 a switch value contains spaces or tabs, the whole parameter should be put in quotation marks, for example:

```
"-home=c:\Program Files\DrWeb Enterprise Suite"
```

When describing the syntax of parameters of separate programs optional parts are enclosed in brackets `[...]`.

The names of switches can be abbreviated (by omitting the last letters), unless the abbreviated name is to coincide with the beginning of any other switch.

H2. The ES Agent Interface Module

The Agent's interface module is run for each user who logs in to a computer on-line. On computers operated by Windows NT OS, Windows 2000 OS, Windows XP OS, Windows 2003 OS, Windows Vista OS it is run with specified user permissions. For proper operation, the Agent requires standard **Windows Explorer** as a user shell or any other program fully compatible with it.

The syntax of the start instruction of the interface module:

```
drwagnui [parameters_switches]
```

The following switches are allowed:

- `-admin-rights or -no-admin-rights` — enable or disable the administration mode in Windows 98 OS, Windows ME OS (that is, to consider the user working in these environments as an administrator or not). The administrator can, for example, change the Agent's settings. For Windows NT OS, Windows 2000 OS, Windows XP OS, Windows 2003 OS, Windows Vista OS it is determined by the OS permissions 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 disables the welcome message.
- `-help` — to display help on the format of commands.
- `-trace` — to log in detail the location of error origin.

H3. The ES Agent

Settings of the Agent are stored in the Windows OS registry in the `HKEY_LOCAL_MACHINE\SOFTWARE\IDAVLab\Enterprise Suite\Dr.Web Enterprise Agent\Settings` branch. For the parameters set by switches, the parameter name coincides with the switch name.

The list of **GUS** servers the Agent can connect to is stored in `.config` files in repository subfolders (for Windows OS - `DrWeb Enterprise Server\var\repository\`).

When the Agent is started with explicitly specified parameters, 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 it is unnecessary to specify any parameters.

Under Windows NT OS, Windows 2000 OS, Windows XP OS, Windows 2003 OS, Windows Vista OS the Agent is run by the system as a service and is administrated through **Control Panel**. Under Windows OS 98/Windows OS Me the Agent is run as a Windows 98 OS, Windows Me OS service and cannot be administrated.

The start instruction syntax:

```
drwagntd [parameters_switches] [servers]
```

The following switches are possible:

- `-home=`*<folder>* — the folder to which the Agent is installed. If the switch is not set, the folder 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 folder 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 and in case the key received from the Server has expired. When the Agent is connected to the Server, this key is not required. By default, it is an arbitrary valid key in the folder set by the `-home` parameter.
- `-crypt=`*<mode>* — the encryption mode of the traffic with the Server. Possible values are yes, no, possible, the default value is yes.
- `-compression=`*<mode>* — the compression mode of the traffic with the Server. Possible values are yes, no, possible, the default value is possible.
- `-log=`*<log_file>* — Agent's log file. By default it resides in the logs subfolder of the Agent's installation folder. When uninstalling the Agent's software, the deinstallation log is saved to the system temporary folder.
- `-rotate=Nf,Mu` — rotation mode of the Agent log.

Conventions: `N` - number of files; `M` - file size; `u` - unit of measurement,possible values: `k`, `m`, `g`; `f` specifies in which format to store the log files, possible values: `z` (zip) - compress rotated logs with a gzip-compatible packer, is used by default, or `p` (plain) - do not compress.

The default is 10,10m, which means storing 10 files 10 megabites each, use compression. A special none format (`-rotate=none`) can also be used, it means "do not rotate, always write to the same file, which can reach any size".

If the rotation mode is used, the names of log files are generated as follows. Assume the log file name (see the `-log` switch above) is `file.log`, then

- `file.log` — current log file,
- `file.log-1` — previous log file,
- `file.log-2` and so on — the greater the number, the older the version of the log.

- `-verbosity=<details_level>` — log level of detail. By default, INFO is specified; `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `NOTICE`, `WARNING`, `ERROR`, and `CRIT` are also possible. The `ALL` and `DEBUG3` values are synonyms.
- `-trace` — to log in detail the location of error origin.

This switch defines the log level of detail set by the subsequent `-log` switch (read above). One instruction can contain several switches of this type.

- `-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 for the **SpIDer Guard**'s statistics to be sent to the Server; the default value is **30**. The statistics will be sent to the Server at such intervals provided that the statistics has been changed during the interval.

- `-help` — generate help on the format of the instruction and its parameters. The same is for -help of the interface module, read Appendix H2. The ES Agent Interface Module.
- `-control=`*<action>* — administrating the state of the Agent's service.
  Possible actions:
  - `install` — install the service,
  - `uninstall` — uninstall the service,
  - `start` — run the service (only Windows NT OS, Windows 2000 OS, Windows XP OS, Windows 2003 OS, Windows Vista OS),
  - `stop` — terminate the service (only Windows NT OS, Windows 2000 OS, Windows XP OS, Windows 2003 OS, Windows Vista OS),
  - `restart` — restart the service (only Windows NT OS, Windows 2000 OS, Windows XP OS, Windows 2003 OS, Windows Vista OS).
  - *<servers>* — list of Servers. By default - `drwcs@udp/231.0.0.1:2371`, which instructs to search the drwcs Server using multicast requests for group `231.0.0.1 port 2371`.

H4. The Network Installer

The start instruction format:
`drwinst [switches] [variables] [servers]`

Possible switches:

- `-key=drwcsd.pub` — name and location of the Server public key. It resides by default in the Installer subfolder of the Server installation folder.
- `-uninstall` — deinstallation 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 folder, for other cases read about the `-script` switch). If such switch is missing (equals to `-no-uninstall`), installation is performed.

- `-script=<script_name>` — sets a file with the executable script. The default value depends upon the presence of the switch `-uninstall` (`uninstall.rexx` will be by default; at installation `preinstall.rexx` is the default value).

The absence of the `preinstall.rexx` file during the installation does not mean an error.

- `-override` — to try to install the software once again.

  This switch allows variables. Mind that the variables (except for the list of servers) should coincide with those specified at previous launch.

  The switch may also be used together with other switches when starting the Installer via the command line.

  The attempt will fail, if any components are run. It is advisable to use the sequence "uninstall — repeated normal installation.

  The absence of this switch equals to `-no-override`.

If the network installer is run in the normal installation mode (i.e. without `-uninstall` and `-override` switches) on stations where the installation has already been performed, this will not incur any actions. The installer program terminates with a flag indicating that a successful installation has been completed.

- `-interactive` — in the interactive mode after the installation or removal is completed, the user may be requested to restart the computer, if necessary. If the parameter is not set, after the installation or removal is completed, the program closes automatically. The absence of the switch is equivalent to the `-no-interactive switch`.

When installing the Agent's software remotely through the Console, this key will not work.

- `-quiet` — not to use dialogs in the interactive mode (do not prompt to reboot, etc.).
- `-retry=<quantity>` — similar to the Agent.

- `-timeout=<time>` — similar to the Agent.
- `-compression=<mode>` — the compression mode of the traffic with the Server. Possible values are `yes`, `no`, `possible`, the `no` value is set by default.
- `-home=<folder>` — installation folder. By default, it is "`Program Files\DrWeb Enterprise Suite`" on the system drive.
- `-log=<logs_folder>` — the folder for the installation and deinstallation logs. By default, installation logs are saved to the `logs` subfolder set by `-home` for installation. Deinstallation logs are saved to the folder selected by the user for storage of temporary files.

Due to the use of the log folder the administrator can create a folder in the shared resource. All stations' logs will be located in this folder, which is convenient for analysis. Log file names are generated automatically using the GUID and the computer name.

- `-verbosity=<details_level>` — level of detail of the log (similar to the Agent). The default value is `ALL`.

This key defines the log level of detail set by the subsequent `-log` key (read above). One instruction can contain several switches of this type.

- `-regagent` — register the Agent in the list **Add or Remove Programs**.
- `-configure` — show configuration dialog, where the user can set various options of the installer and the Agent.
- `-useolddlg` — use the old dialog with the installation log. If the parameter is not set, the new dialog is displayed with the installation progress indicator and information bar, where the current operation is described.
- `-platforms=p1,p2,p3...` – platforms load order (it is standard by default, read Appendix J. Using the Script of ES Agent Initial Installation).
- `-help` — offer help. Similar to the Agent's interface module.

- `-trace` — to log in detail the location of error origin.

The variables are listed after switches. The format of the elements is as follows:

<variable>=<value>

Some most important variables:

- `agent.language="C:\Program Files\DrWeb Enterprise Suite\RU-ESAUI.DWL"` *<IP-address or DNS name of the ES Server>*
  this parameter switches the language of the Agent context menu to **Russian**. You should specify the full path to the language resources. By default, **English** is used.
- `spider.install=no` — do not install **SpIDer Guard**. Install if no variable is specified.
- `spiderml.install=no` — similarly; do not install **SpIDer Mail**.
- `scanner.install=no` — similarly; do not install **Dr.Web® Scanner for Windows**.
- `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.

H5. Dr.Web Enterprise Server

There are several variants as how to launch the Server. These variants will be described separately.

H5.1. Running the Server

`drwcsd [switches]` — run the Server (the switches are described in more detail below).

H5.2. Database Initialization

`drwcsd [keys] initdb agent.key [` *<DB_script>* `[` *<ini_file>* `[` *<password>*`]]` — database initialization.

- `agent.key` — **Dr.Web®** license key file (must be specified).
- *<DB_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 (his name is **admin**). By default, it is **root**.

A minus can be omitted, if the next parameters are missing.

H5.3. Database Updating

`drwcsd [switches] updatedb` *<script>* — perform any action with the database (for example, update to a new version) by executing SQL instructors from the *<script>* file.

H5.4. Database Verification

`drwcsd verifydb` – run the Server to check the database. Upon completion the Server saves the verification results in the log file (`drwcsd.log` by default).

H5.5. Database Upgrading

`drwcsd upgradedb` *<folder>* – run the Server to update the structure of the database at a version upgrade (see the `var/update-db` folder).

H5.6. Database Export

`drwcsd exportdb` *<file>* – export the database to the specified file.

Example for Windows:

```
C:\Program Files\DrWeb Enterprise
Server\bin\drwcsd.exe -home="C:\Program
Files\DrWeb Enterprise Server" -var-root="C:
\Program Files\DrWeb Enterprise Server\var" -
verbosity=all exportdb "C:\Program Files\DrWeb
Enterprise Server\esbase.es"
```

Under **UNIX** OS the action is performed on behalf of the drwcs:drwcs user to the directory `$DRWCS_VAR` (except for **FreeBSD** OS, which by default saves the file to the directory from which the script was run; if the path is specified explicitly, then the directory should have the recording right for the *<user>*: *<group>* that had been created at installation, by default it is `drwcs:drwcs`).

H5.7. Database Import

`drwcsd importdb` *<file>* – import the database from the specified file (the previous content of the database is deleted).

H5.8. Critical Server Data Backup

The following command creates backup copies of critical Server data (database contents, Server license key, private encryption key, Server configuration key, and Web Server configuration key):

`drwcsd -home=`*<path>* `backup [` *<directory>* `[` *<quantity>*`]]` – copy critical Server data to the specified folder. `-home` sets the Server installation catalog. *<quantity>* is the number of copies of each file.

Example for Windows:

```
C:\Program Files\DrWeb Enterprise
Server\bin>drwcsd -home="C:\Program Files\DrWeb
Enterprise Server" backup C:\a
```

The copies are stored in the `.dz` format unpackable with `gzip` and other archivers. After unpacking all the files, except for the database contents, are ready to use. To restore the data, the database contents can be imported from the backup to another database of the Server by means of the importdb switch (see p. Restoring the Database of Dr.Web Enterprise Suite).

Starting from the **4.33** version, **ES** regularly stores backups of critical information to `\var\Backup` of the Server installation catalog. For that purpose a daily task is included to the Server schedule, which performs this function. If such task is missing, it is strongly recommended to create it. Particularly there will be no backup critical data task, if the initially installed (and then consequently upgraded) Server version is **4.32**.

H5.9. Repository Synchronization

`drwcsd syncrepository` – synchronize the repository with the **GUS.** Stop the Server before initiating this instruction!

H5.10. Command Formats for Windows® OS Only

- `drwcsd [switches] install` — install the Server service in the system.
- `drwcsd uninstall` — uninstall the Server service from a system.
- `drwcsd start` — run the Server service.
- `drwcsd stop` — stop the Server service.
- `drwcsd kill` — perform emergency shutdown of the Server service (if normal termination failed). This instruction should not be used without extreme necessity.
- `drwcsd restart` — restart the Server service (it is executed as the `stop` and then `start` pair).
- `drwcsd reconfigure` — reread and reboot the configuration file (it is performed quicker and without starting a new process).
- `drwcsd rerepository` – reread the repository from the drive.

- `drwcsd retemplate` – reread notification templates from the drive.

H5.11. The Description of Switches

- `-home=`*<root>* — Server installation folder (root folder). The structure of this folder is described in p. Installing the Anti-Virus Server for Windows NT/2000/XP/2003/Vista. By default, it is the current folder at start.
- `-bin-root=`*<folder_for_executables>* — the path to executable files. By default, it is the `bin` subfolder of the root folder.
- `-var-root=`*<folder_for_modified>* — path to a folder 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` subfolder of the root folder.
- `-conf=`*<configuration_file>* — name and location of the Server configuration file. By default, it is the `drwcsd.conf` file in the `etc` subfolder of the root folder.
- `-activation-key=`*<license_key>* — Server license key. By default, it is the `enterprise.key` file located in the etc subfolder of the root folder.
- `-id=`*<number>* — if enterprise.key allows to use more than one Server, it 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. By default, it is `drwcsd.pri` in the etc subfolder of the root folder.
- `-log=`*<log>* — Server log filename. A minus can be used instead of the filename (for Servers under UNIX OS only), which instructs standard output of the log. By default: for Windows platforms it is `drwcsd.log` in the folder specified by the `-var-root` switch, for UNIX platforms it is set by the `-syslog=user` switch (read below).

- -syslog=<*mode*> — possible for UNIX OS only. It instructs logging to the system log. Possible modes: auth, cron, daemon, kern, lpr, mail, news, syslog, user, uucp, local0 — local7 and for some platforms — ftp, authpriv and console.
- -rotate=Nf, Mu — rotation mode of the Agent log.

  Conventions: N - number of files; M - file size; u - unit of measurement,possible values: k, m, g; f specifies in which format to store the log files, possible values: z (zip) - compress rotated logs with a gzip-compatible packer, is used by default, or p (plain) - do not compress.

  The default is 10,10m, which means storing 10 files 10 megabites each, use compression. A special none format (-rotate=none) can also be used, it means "do not rotate, always write to the same file, which can reach any size".

  If the rotation mode is used, the names of log files are generated as follows. Assume the log file name (see the -log switch above) is file. log, then

  - file. log — current log file,
  - file. log-1 — previous log file,
  - file. log-2 and so on — the greater the number, the older the version.
- -pid=<*file*> —for UNIX OS only, a file to which the Server writes the identifier of its process.
- -user=<*user*>, -group=<*group*> — available for UNIX OS only, if run by the root user; it means to change the user or the group of process and to be executed with the permissions of the specified user (or group).
- -verbosity=<*details_level*> — log level of detail. By default, WARNING is specified; ALL, DEBUG3, DEBUG2, DEBUG1, DEBUG, TRACE3, TRACE2, TRACE1, TRACE, NOTICE, WARNING, ERROR are also possible. The ALL and DEBUG3 values are synonyms.
- -db-verify=on — check database integrity at Server start. This is the default value. It is not recommended to run with an explicit opposite value, except if run immediately after the database is checked by the drwcsd verifydb instruction, see above.

- `-help` — displays help. Similar to the programs described above.
- `-trace` — to log in detail the location of error origin.
- `-hooks` — to permit the Server to perform user extension scripts located in the `var\extensions` subcatalog of the Server's installation catalog. The scripts are meant for automation of the administrator work enabling quicker performance of certain tasks. All scripts are disabled by default.
- `-daemon` — for Windows platforms it means to launch as a service; for UNIX platforms - "daemonization of the process" (to go to the root folder, disconnect from the terminal and operate in the background).
- `-minimized` — (for Windows only, if run not as a service, but in the interactive mode) — minimize a window.
- `-screen-size=`<size> — (for Windows only, if run not as a service, but in the interactive mode) — log size in lines displayed in the Server screen, the default value is 1000.

H6. The Administrating Utility of the Internal Database

The start format:

`drwidbsh`

The program operates in the text dialog mode; it waits for instructions from a user (the instructions begin with a period). To receive help on other instructions, type `.help`.

For more information, use reference manuals on the SQL language.

H7. The Utility of Generation of Key Pairs and Digital Signatures

The names and location of encryption files in the Server installation directory:

- `\etc\drwcsd.pri` - private key,
- `\Installer\drwcsd.pub` - public key.

Variants of the instruction format:

- `\bin\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 private keys from copying.

- `\bin\drwsign sign [-private-key=<private>] <file>` — sign the *<file>* file using this private key.
- `\bin\drwsign check [-public-key=<public>] <file>` — check the file signature using *<public>* as a public key of a person who signed this file.
- `\bin\drwsign join432 [-public-key=<public>] [-private-key=<private>] <new_private>` — combines the public and private keys of the format for version **4.32** into a new format of the private key for version **4.33**.
- `\bin\drwsign extract [-private-key=<private>] <public>` — extracts the public key from the private key file of a complex format (version **4.33** and higher).
- `\bin\drwsign help [<instruction>]` — brief help on the program and on the command line format.

H8. Administration of the Server Version for UNIX® OS with the kill Instruction

The version of the Server for UNIX OS is administrated by the signals sent to the Server's processor by the `kill` utility.

Use the `man kill` instruction to receive help on the `kill` utility.

Below are listed the utility signals and the actions performed by them:

- `SIGWINCH` – log statistics to a file (CPU time, memory usage, etc.),
- `SIGUSR1` – reread the repository from the drive,
- `SIGUSR2` – reread templates from the drive,

- `SIGHUP` – restart the Server,
- `SIGTERM` – shut down the Server,
- `SIGQUIT` – shut down the Server,
- `SIGINT` – shut down the Server.

Similar actions are performed by the switches of the drwcsd instruction for the Windows version of the Server, read Appendix H5.4.

H9. Dr.Web Scanner for Windows® OS

This component of the workstation software has the command line parameters which are described in "**Dr.Web® Anti-Virus 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.

Also using the `-trace` switch is possible to log the location of error origin in detail, like in the applications above.

H10. ES Console

Start instruction format:
`drwconsole [parameters_switches]`

the following switches are allowed:

`-J-XmxXX` — at launch to allocate a certain RAM size to be used by the application, where `XX` is the size of RAM.

For example, `-J-Xmx1G or -J-Xmx512m`.

Unless the switch is specified, the Console determines the size of required RAM automatically:

32bit Console:

- for the computers with more than **512** MB RAM, the Console uses **512** MB RAM
- for the computers with less than **128** MB RAM, the Console uses **128** MB RAM (swapping)

- otherwise the Console uses all available RAM

64bit Console:

- for the computers with less than **128** MB RAM, The console uses **128** MB RAM (swapping)
- otherwise the console uses all available RAM

Appendix I. Environment Variables Exported by the Server

To simplify the setting of the processes run by the **ES** Server on schedule, the data on location of the Server's catalogs is required. To this effect, the Server exports the following variables of started processes into the environment:

- `DRWCSD_HOME` – path to the root folder (installation folder). The switch value is `-home`, if it was set at Server's launch; otherwise the current folder at launch.
- `DRWCSD_EXE` – path to the folder with executable files. The switch value is `-bin-root`, if it was set at Server's launch; otherwise it is the `bin` subfolder of the root folder.
- `DRWCSD_VAR` — path to the folder to which the Server has a write access and which is designed to store volatile files (for example, logs and repository files). The switchvalue is `-var-root`, if it was set at Server's launch; otherwise it is the var subfolder of the root folder.

Appendix J. Using the Script of ES Agent Initial Installation

The installation routine of the Agents onto workstations by using the network installer (`drwinst.exe`) is set by install.script. These files reside in the products root folder in the repository. In standard distributions they are located in the `10-drwupgrade` and `20-drwagntd` catalogs and describe the default installation.

If the .custom.install.script file is present in the folder, it is used instead of the standard installation routine.

Files with other names beginning with a period are not updated during the product update and do not influence the operation of the repository.

The sequence of operations during the installation:

1. The network installer requests the Server for the installation of the following platforms: `win-setup`, `common`, `win`, `win-nt` and `win-9x` – this is the list of standard platforms in the default order. The order of use of the platforms can be changed by the `-platforms=p1,p2,p3...` switch when calling drwinst. The `win-setup` platform is not included into a standard distribution and is designed for creation of its own installation routines, if necessary.
2. The Server forms a list of files according to the list of platforms, viewing all products step by step 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 created 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 executed by the network installer.

Now we consider `install.script` by example of the `20-drwagntd` folder.

```
; 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 folder where current file are
     ; located if `file.name' does not include
     ; folder 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 a file name only, it is searched for in the same folder as the current one. The use 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 transferred to the station and the construction of the formed script.

The order of the `platform{ }` constructions is also inessential.

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 are listed below.

Components to be installed:

- `spider.install = 'yes'`
- `spiderml.install = 'yes'`
- `scanner.install = 'yes'`
- `install.home – installation folder`
- `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'`
- `agent.discovery = 'udp/:2372'`
- `agent.startmsg = '2' (or agent.startmsg = 'NONE')`

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).

Now we create a nonstandard installation scenario in which SpIDer Guard is not installed and maximum detailed logging is set:

1. Create a .win-setup.inst.rexx file in the `20-drwagntd` folder and write to it

```
spider.install = 'no'
agent.loglevel = 'all'
```

2. Create the `.custom.install.script` file in the `20-drwagntd` folder and write to it

```
include install.script

platform{
      name: win-setup
      scripts{ .win-setup.inst.rexx }
}
```

3. Reboot the Server or instruct to reboot the repository:

   - for **UNIX** OS: `kill -USR1 cat `drwcsd.pid``
   - for **Windows**: `drwcsd.exe rerepository`

Appendix K. Regular Expressions Used in Dr.Web Enterprise Suite

K1. Options Used in Regular Expressions

Regular expressions are used in the configuration file and in the Console when objects to be excluded from scanning are specified. They are written as follows:

`qr{EXP}options`

where `EXP` is the expression itself; options stands for the sequence of options (a string of letters), and `qr{}` is literal metacharacters. The whole construction looks as follows:

`qr{pagefile\.sys}i` - Windows NT swap file

Below goes the description of options and regular expressions. For more details visit http://www.pcre.org/pcre.txt.

- Option `'a'` is equivalent to `PCRE_ANCHORED`

  If this option is set, the pattern is forced to be "anchored", that is, it is constrained to match only at the first matching point in the string that is being searched (the "subject string"). The same result can also be achieved by appropriate constructs in the pattern itself.

- Option `'i'` is equivalent to `PCRE_CASELESS`

  If this option is set, letters in the pattern match both upper and lower case letters. This option can be changed within a pattern by a (`?i`) option setting.

- Option `'x'` is equivalent to `PCRE_EXTENDED`

If this option is set, whitespace data characters in the pattern are totally ignored except when escaped or inside a character class. Whitespaces do not include the VT character (code 11). In addition, characters between an unescaped # outside a character class and a newline character inclusively are ignored. This option can be changed in the pattern by setting a (?x) option. This option enables including comments inside complicated patterns. Note, however, that this applies only to data characters. Whitespaces may not appear in special character sequences in a pattern, for example within the (?(sequence which introduces a conditional subpattern.

- Option 'm' is equivalent to PCRE_MULTILINE

  By default, PCRE treats the subject string as consisting of a single line of characters (even if it actually contains newlines). The "*start of line*" metacharacter "^" matches only in the beginning of a string, while the *"end of line"* metacharacter "$" matches only in the end of a string or before a terminating newline (unless PCRE_DOLLAR_ENDONLY is set).

  When PCRE_MULTILINE is set, the "*start of line*" and "*end of line* " metacharacters match any newline characters which immediately follow or precede them in the subject string as well as in the very beginning and end of a subject string. This option can be changed within a pattern by a (?m) option setting. If there are no "\n" characters in the subject string, or ^ or $ are not present in the pattern, the PCRE_MULTILINE option has no effect.

- Option 'u' is equivalent to PCRE_UNGREEDY

  This option inverts the "greediness" of the quantifiers so that they are not greedy by default, but become greedy if followed by "?". The same result can also be achieved by the (?U) option in the pattern.

- Option 'd' is equivalent to PCRE_DOTALL

  If this option is set, a dot metacharacter in the pattern matches all characters, including newlines. Without it, newlines are excluded. This option can be changed within a pattern by a (?s) option setting. A negative class such as [^a] always matches newline characters, regardless of the settings of this option.

- Option 'e' is equivalent to PCRE_DOLLAR_ENDONLY

If this option is set, a dollar metacharacter in the pattern matches only at the end of the subject string. Without this option, a dollar also matches immediately before a newline at the end of the string (but not before any other newline characters). The `PCRE_DOLLAR_ENDONLY` option is ignored if `PCRE_MULTILINE` is set.

K2. Peculiarities of PCRE Regular Expressions

A *regular expression* is a pattern that is matched against a subject string from left to right. Most characters stand for themselves in a pattern, and match the corresponding characters in the subject.

The power of regular expressions comes from the ability to include alternatives and repetitions in the pattern. These are encoded in the pattern by the use of metacharacters, which do not stand for themselves but instead are interpreted in a special way.

There are two different sets of metacharacters: those recognized anywhere in a pattern except within square brackets, and those recognized in square brackets. Outside square brackets, the metacharacters are as follows:

`\` general `escape` character with several uses,

`^` assert start of string (or line, in multiline mode),

`$` assert end of string (or line, in multiline mode),

`.` match any character except newline (by default),

`[` start character class definition,

`]` end character class definition,

`|` start alternative branch,

`(` start subpattern,

`)` end subpattern,

`?` extends the meaning of `(`,

also `0` or `1` quantifier,

also quantifier minimizer.

* 0 or more quantifier,

+ 1 or more quantifier,

also "possessive quantifier",

{ start min/max quantifier.

Part of a pattern that is in square brackets is called a "character class". In a character class the only metacharacters are:

\ general escape character,

^ negate the class, but only if the first character,

– indicates character range,

[POSIX character class (only if followed by POSIX syntax),

] terminates the character class.

K3. Use of Metacharacters

Backslash (\)

The backslash character has several uses. When it is followed by a non-alphanumeric character, it takes away any special meaning that character may have. This use of backslash as an escape character applies both inside and outside character classes.

For example, if you want to match a * character, you should write * in the pattern. This escaping action applies whether or not the following character would otherwise be interpreted as a metacharacter, so it is always safe to precede a non-alphanumeric with backslash to specify that it stands for itself. In particular, if you want to match a backslash, you write \\.

If a pattern includes the PCRE_EXTENDED option, whitespaces (other than in a character class) in the pattern, characters between # outside a character class and the next newline character will be ignored. An escaping backslash can be used to include a whitespace or # character as part of the pattern.

If you want to remove the special meaning from a sequence of characters, you can do so by putting them between \Q and \E. The \Q. . . \E sequence works both inside and outside character classes.

Non-printing characters

Backslash provides a way of encoding non-printing characters in patterns to make them visible. There is no restriction on the appearance of non-printing characters, apart from the binary zero at the end of a pattern. But when a pattern is being created in a text editor, it is usually easier to use one of the following escape sequences than the binary character it represents:

- \a alarm, i.e., the BEL character (hex 07)
- \cx "control-x", where x is any character
- \e escape (hex 1B)
- \f formfeed (hex 0C)
- \n newline (hex 0A)
- \r carriage return (hex 0D)
- \t tab (hex 09)
- \ddd character with octal code ddd, or back reference
- \xhh character with hex code hh

The precise effect of \cx is as follows: if x is a lower case letter, it is converted to upper case. Then bit 6 of the character (hex 40) is inverted. Thus \cz becomes hex 1A, but \c{ becomes hex 3B, while \c; becomes hex 7B.

After \x from zero to two hexadecimal digits are read (letters can be in upper or lower case).

After \0 up to two further octal digits are read. In both cases, if there are fewer than two digits, just those that are present are used. Thus the sequence \0\x\07 specifies two binary zeros followed by a BEL character (code value 7). Make sure you supply two digits after the initial zero if the pattern character that follows is itself an octal digit.

The handling of a backslash followed by a digit other than 0 is complicated. Outside a character class, PCRE reads it and any following digits as a decimal number. If the number is less than 10, or if there have been at least that many previous capturing left parentheses in the expression, the entire sequence is taken as a back reference.

Inside a character class, or if the decimal number is greater than 9 and there have not been that many capturing subpatterns, PCRE re-reads up to three octal digits following the backslash, and generates a single byte from the least significant 8 bits of the value. Any subsequent digits stand for themselves. For example:

- \040 is another way of writing a space
- \40 is the same, provided there are fewer than 40 previous capturing subpatterns
- \7 is always a back reference
- \11 might be a back reference, or another way of writing a tab
- \011 is always a tab
- \0113 is a tab followed by the character "3"
- \113 might be a back reference, otherwise the character with octal code 113
- \377 might be a back reference, otherwise the byte consisting entirely of 1 bits
- \81 is either a back reference, or a binary zero followed by the two characters "8" and "1"

Note that octal values of 100 or greater must not be introduced by a leading zero, because no more than three octal digits are ever read.

All the sequences that define a single character value can be used both inside and outside character classes. In addition, inside a character class, the sequence \b is interpreted as the backspace character (hex 08), and the sequence \X is interpreted as the character "X". Outside a character class, these sequences have different meanings.

Generic character types

The third use of backslash is for specifying generic character types. The following are always recognized:

- \d any decimal digit
- \D any character that is not a decimal digit
- \s any whitespace character
- \S any character that is not a whitespace character
- \w any "word" character
- \W any "non-word" character

Each pair of escape sequences partitions the complete set of characters into two disjoint sets. Any given character matches one, and only one, of each pair.

These character type sequences can appear both inside and outside character classes. They each match one character of the appropriate type. If the current matching point is at the end of the subject string, all of them fail, since there is no character to match.

\s does not match the VT character (code 11). This makes it different from the POSIX "space" class. The \s characters are HT (9), LF (10), FF (12), CR (13), and space (32).

Simple assertions

The fourth use of backslash is for certain simple assertions. An assertion specifies a condition that has to be met at a particular point in a match, without consuming any characters from the subject string. The use of subpatterns for more complicated assertions is described below. The backslashed assertions are:

- \b matches at a word boundary
- \B matches when not at a word boundary
- \A matches at start of subject
- \Z matches at end of subject or before newline at end
- \z matches at end of subject
- \G matches at first matching position in subject

These assertions may not appear in character classes (but note that \b has a different meaning, namely the backspace character, inside a character class).

Circumflex (^) and dollar ($)

Outside a character class, in the default matching mode, the circumflex character is an assertion that is true only if the current matching point is at the start of the subject string. Inside a character class, circumflex has an entirely different meaning (see below).

Circumflex need not be the first character of the pattern if a number of alternatives are involved, but it should be the first thing in each alternative in which it appears if the pattern is ever to match that branch. If all possible alternatives start with a circumflex, that is, if the pattern is constrained to match only at the start of the subject, it is said to be an "anchored" pattern. (There are also other constructs that can cause a pattern to be anchored.)

A dollar character is an assertion that is true only if the current matching point is at the end of the subject string, or immediately before a newline character that is the last character in the string (by default). Dollar need not be the last character of the pattern if a number of alternatives are involved, but it should be the last item in any branch in which it appears. Dollar has no special meaning in a character class.

The meanings of the circumflex and dollar characters are changed if the `PCRE_MULTILINE` option is set. When this is the case, they match immediately after and immediately before an internal newline character, respectively, in addition to matching at the start and end of the subject string. For example, the pattern `/^abc$/` matches the subject string "`def\nabc`" (where `\n` represents a newline character) in multiline mode, but not otherwise. Consequently, patterns that are anchored in single line mode because all branches start with `^` are not anchored in multiline mode, and a match for circumflex is possible when the startoffset argument of `pcre_exec()` is non-zero.

Full stop (period, dot)

Outside a character class, a period in the pattern matches any one character in the subject, including a non-printing character, but not (by default) newline. The handling of period is entirely independent of the handling of circumflex and dollar, the only relationship being that they both involve newline characters. Period has no special meaning in a character class.

Square brackets and character classes

An opening square bracket introduces a character class, terminated by a closing square bracket. A closing square bracket on its own is not special. If a closing square bracket is required as a member of the class, it should be the first data character in the class (after an initial circumflex, if present) or escaped with a backslash.

A character class matches a single character in the subject. A matched character must be in the set of characters defined by the class, unless the first character in the class definition is a circumflex, in which case the subject character must not be in the set defined by the class. If a circumflex is actually required as a member of the class, ensure it is not the first character, or escape it with a backslash.

For example, the character class `[aeiou]` matches any lower case vowel, while `[^aeiou]` matches any character that is not a lower case vowel. Note that a circumflex is just a convenient notation for specifying the characters that are in the class by enumerating those that are not. A class that starts with a circumflex is not an assertion: it still consumes a character from the subject string, and therefore it fails if the current pointer is at the end of the string.

When caseless matching is set, any letters in a class represent both their upper case and lower case versions.

The minus (hyphen) character can be used to specify a range of characters in a character class. For example, `[d-m]` matches any letter between d and m, inclusive. If a minus character is required in a class, it must be escaped with a backslash or appear in a position where it cannot be interpreted as indicating a range, typically as the first or last character in the class.

It is not possible to have the literal character "`]`" as the end character of a range. A pattern such as `[W-]46]` is interpreted as a class of two characters ("`W`" and "`-`") followed by a literal string "46]", so it would match "`W46]`" or "`-46]`". However, if the "`]`" is escaped with a backslash it is interpreted as the end of range, so [W-\]46] is interpreted as a class containing a range followed by two other characters. The octal or hexadecimal representation of "]" can also be used to end a range.

The character types `\d`, `\D`, `\p`, `\P`, `\s`, `\S`, `\w`, and `\W` may also appear in a character class, and add the characters that they match to the class.

The only metacharacters that are recognized in character classes are backslash, hyphen (only where it can be interpreted as specifying a range), circumflex (only at the start), opening square bracket (only when it can be interpreted as introducing a POSIX class name - see the next section), and the terminating closing square bracket. However, escaping other non-alphanumeric characters does no harm.

POSIX character classes

PCRE supports the POSIX notation for character classes. For example,

```
[01[:alpha:]%]
```

matches "0", "1", any alphabetic character, or "%". The supported class names are

- alnum letters and digits
- alpha letters
- ascii character codes 0 - 127
- blank space or tab only
- cntrl control characters
- digit decimal digits (same as \d)
- graph printing characters, excluding space
- lower lower case letters
- print printing characters, including space
- punct printing characters, excluding letters and digits
- space white space (not quite the same as \s)
- upper upper case letters
- word "word" characters (same as \w)
- xdigit hexadecimal digits

Vertical bar (|)

Vertical bar characters are used to separate alternative patterns. For example, the pattern

```
gilbert|sullivan
```

matches either "gilbert" or "sullivan". Any number of alternatives may appear, and an empty alternative is permitted (matching the empty string). The matching process tries each alternative in turn, from left to right, and the first one that succeeds is used. If the alternatives are within a subpattern (defined below), "succeeds" means matching the rest of the main pattern as well as the alternative in the subpattern.

Internal option setting

The settings of the PCRE_CASELESS, PCRE_MULTILINE, and PCRE_EXTENDED options can be changed from within the pattern by a sequence of Perl option letters enclosed between "(?" and ")". The option letters are

- i for PCRE_CASELESS
- m for PCRE_MULTILINE
- x for PCRE_EXTENDED

For example, (?im) sets caseless multiline matching. It is also possible to unset these options by preceding the letter with a hyphen, and a combined setting and unsetting such as (?im-x), which sets PCRE_CASELESS and PCRE_MULTILINE while unsetting PCRE_EXTENDED, is also permitted. If a letter appears both before and after the hyphen, the option is unset.

Subpatterns

Subpatterns are delimited by parentheses (round brackets) which can be nested. Turning part of a pattern into a subpattern does two things:

1. It localizes a set of alternatives. For example, the pattern
   cat(aract|erpillar|)
   matches one of the words "cat", "cataract", or "caterpillar". Without the parentheses, it would match "cataract", "erpillar" or the empty string.
2. It sets up the subpattern as a capturing subpattern. Opening parentheses are counted from left to right (starting from 1) to obtain numbers for the capturing subpatterns.

For example, if the string "the red king" is matched against the pattern

```
the (( red| white) ( king| queen))
```

the captured substrings are "red king", "red", and "king", and are numbered 1, 2, and 3, respectively.

The fact that plain parentheses fulfil two functions is not always helpful. There are often times when a grouping subpattern is required without a capturing requirement. If an opening parenthesis is followed by "?: ", the subpattern does not do any capturing, and is not counted when computing the number of any subsequent capturing subpatterns. For example, if the string "the white queen" is matched against the pattern

```
the (( ?: red| white) ( king| queen))
```

the captured substrings are "white queen" and "queen", and are numbered 1 and 2. The maximum number of capturing subpatterns is 65535, and the maximum depth of nesting of all subpatterns, both capturing and non-capturing, is 200.

As a convenient shorthand, if any option settings are required at the start of a non-capturing subpattern, the option letters may appear between the "?" and the ": ". Thus the two patterns

```
( ?i: saturday| sunday)
( ?:( ?i) saturday| sunday)
```

match exactly the same set of strings. Because alternative branches are tried from left to right, and options are not reset until the end of the subpattern is reached, an option setting in one branch does affect subsequent branches, so the above patterns match "SUNDAY" as well as "Saturday".

Repetition

Repetition is specified by quantifiers, which can follow any of the following items:

- a literal data character
- the . metacharacter
- the \C escape sequence
- an escape such as \d that matches a single character
- a character class

- a back reference (see the next section)
- a parenthesized subpattern (unless it is an assertion)

The general repetition quantifier specifies a minimum and maximum number of permitted matches, by giving the two numbers in curly brackets (braces), separated by a comma. The numbers must be less than `65536`, and the first must be less than or equal to the second.

For example:

```
z{2,4}
```

matches "`zz`", "`zzz`", or "`zzzz`". A closing brace on its own is not a special character. If the second number is omitted, but the comma is present, there is no upper limit; if the second number and the comma are both omitted, the quantifier specifies an exact number of required matches.

Thus

```
[aeiou]{3,}
```

matches at least 3 successive vowels, but may match many more, while

```
\d{8}
```

matches exactly 8 digits. An opening curly bracket that appears in a position where a quantifier is not allowed, or one that does not match the syntax of a quantifier, is taken as a literal character. For example, `{,6}` is not a quantifier, but a literal string of four characters.

The quantifier `{0}` is permitted, causing the expression to behave as if the previous item and the quantifier were not present.

For convenience (and historical compatibility) the three most common quantifiers have single-character abbreviations:

- `*` is equivalent to `{0,}`
- `+` is equivalent to `{1,}`
- `?` is equivalent to `{0,1}`

It is possible to construct infinite loops by following a subpattern that can match no characters with a quantifier that has no upper limit, for example:

```
(a?)*
```

By default, the quantifiers are "greedy", that is, they match as much as possible (up to the maximum number of permitted times), without causing the rest of the pattern to fail. The classic example of where this gives problems is in trying to match comments in C programs. These appear between /* and */ and within the comment, individual * and / characters may appear. An attempt to match C comments by applying the pattern

```
/\*.*\*/
```

to the string

```
/* first comment */ not comment /* second comment */
```

fails, because it matches the entire string owing to the greediness of the * item.

However, if a quantifier is followed by a question mark, it ceases to be greedy, and instead matches the minimum number of times possible, so the pattern

```
/\*.*?\*/
```

does the right thing with the C comments. The meaning of the various quantifiers is not otherwise changed, just the preferred number of matches. Do not confuse this use of question mark with its use as a quantifier in its own right. Because it has two uses, it can sometimes appear doubled, as in

```
\d??\d
```

which matches one digit by preference, but can match two if that is the only way the rest of the pattern matches.

If the PCRE_UNGREEDY option is set, the quantifiers are not greedy by default, but individual ones can be made greedy by following them with a question mark. In other words, it inverts the default behaviour.

When a parenthesized subpattern is quantified with a minimum repeat count that is greater than 1 or with a limited maximum, more memory is required for the compiled pattern, in proportion to the size of the minimum or maximum.

Atomic grouping and possessive quantifiers

With both maximizing and minimizing repetition, failure of what follows normally causes the repeated item to be re-evaluated to see if a different number of repeats allows the rest of the pattern to match. Sometimes it is useful to prevent this, either to change the nature of the match, or to cause it fail earlier than it otherwise might, when the author of the pattern knows there is no point in carrying on.

Consider, for example, the pattern `\d+foo` when applied to the subject line

```
123456bar
```

After matching all 6 digits and then failing to match "`foo`", the normal action of the matcher is to try again with only 5 digits matching the `\d+` item, and then with 4, and so on, before ultimately failing. "Atomic grouping" (a term taken from Jeffrey Friedl's book) provides the means for specifying that once a subpattern has matched, it is not to be re-evaluated in this way.

If we use atomic grouping for the previous example, the matcher would give up immediately on failing to match "foo" the first time. The notation is a kind of special parenthesis, starting with `(?>` as in this example:

```
(?>\d+)foo
```

This kind of parenthesis "locks up" the part of the pattern it contains once it has matched, and a failure further into the pattern is prevented from backtracking into it. Backtracking past it to previous items, however, works as normal.

An alternative description is that a subpattern of this type matches the string of characters that an identical standalone pattern would match, if anchored at the current point in the subject string.

Atomic grouping subpatterns are not capturing subpatterns. Simple cases such as the above example can be thought of as a maximizing repeat that must swallow everything it can. So, while both `\d+` and `\d+?` are prepared to adjust the number of digits they match in order to make the rest of the pattern match, `(?>\d+)` can only match an entire sequence of digits.

Atomic groups in general can of course contain arbitrarily complicated subpatterns, and can be nested. However, when the subpattern for an atomic group is just a single repeated item, as in the example above, a simpler notation, called a "possessive quantifier" can be used. This consists of an additional + character following a quantifier. Using this notation, the previous example can be rewritten as

```
\d++foo
```

Possessive quantifiers are always greedy; the setting of the PCRE_UNGREEDY option is ignored. They are a convenient notation for the simpler forms of atomic group. However, there is no difference in the meaning or processing of a possessive quantifier and the equivalent atomic group.

When a pattern contains an unlimited repeat inside a subpattern that can itself be repeated an unlimited number of times, the use of an atomic group is the only way to avoid some failing matches taking a very long time indeed. The pattern

```
(\D+|<\d+>)*[!?]
```

matches an unlimited number of substrings that either consist of non-digits, or digits enclosed in <>, followed by either ! or ?. When it matches, it runs quickly. However, if it is applied to

```
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

it takes a long time before reporting failure. This is because the string can be divided between the internal \D+ repeat and the external * repeat in a large number of ways, and all have to be tried. (The example uses [!?] rather than a single character at the end, because PCRE has an optimization that allows for fast failure when a single character is set. They remember the last single character that is required for a match, and fail early if it is not present in the string.) If the pattern is changed so that it uses an atomic group, like this:

```
((?>\D+)|<\d+>)*[!?]
```

sequences of non-digits cannot be broken, and failure happens quickly.

Back references

Outside a character class, a backslash followed by a digit greater than 0 (and possibly further digits) is a back reference to a capturing subpattern earlier (that is, to its left) in the pattern, provided there have been that many previous capturing left parentheses.

However, if the decimal number following the backslash is less than 10, it is always taken as a back reference, and causes an error only if there are not that many capturing left parentheses in the entire pat- tern. In other words, the parentheses that are referenced need not be to the left of the reference for numbers less than 10. See the subsection entitled "Non-printing characters" above for further details of the handling of digits following a backslash.

A back reference matches whatever actually matched the capturing subpattern in the current subject string, rather than anything matching the subpattern itself. So the pattern

```
(sens|respons)e and \1ibility
```

matches "sense and sensibility" and "response and responsibility", but not "sense and responsibility". If caseful matching is in force at the time of the back reference, the case of letters is relevant. For example,

```
((?i)rah)\s+\1
```

matches "`rah rah`" and "`RAH RAH`", but not "`RAH rah`", even though the original capturing subpattern is matched caselessly.

Back references to named subpatterns use the Python syntax `(?P=name)`. We could rewrite the above example as follows:

```
(?(?i)rah)\s+(?P=p1)
```

There may be more than one back reference to the same subpattern. If a subpattern has not actually been used in a particular match, any back references to it always fail. For example, the pattern

```
(a|(bc))\2
```

always fails if it starts to match "`a`" rather than "`bc`". Because there may be many capturing parentheses in a pattern, all digits following the backslash are taken as part of a potential back reference number. If the pattern continues with a digit character, some delimiter must be used to terminate the back reference. If the `PCRE_EXTENDED` option is set, this can be whitespace. Otherwise an empty comment can be used.

A back reference that occurs inside the parentheses to which it refers fails when the subpattern is first used, so, for example, `(a\1)` never matches. However, such references can be useful inside repeated sub- patterns. For example, the pattern

```
(a|b\1)+
```

matches any number of "a"s and also "aba", "ababbaa", etc. At each iteration of the subpattern, the back reference matches the character string corresponding to the previous iteration. In order for this to work, the pattern must be such that the first iteration does not need to match the back reference. This can be done using alternation, as in the example above, or by a quantifier with a minimum of zero.

Assertions

An assertion is a test on the characters following or preceding the current matching point that does not actually consume any characters. The simple assertions coded as \b, \B, \A, \G, \Z, \z, ^ and $ are described above.

More complicated assertions are coded as subpatterns. There are two kinds: those that look ahead of the current position in the subject string, and those that look behind it. An assertion subpattern is matched in the normal way, except that it does not cause the current matching position to be changed.

Assertion subpatterns are not capturing subpatterns, and may not be repeated, because it makes no sense to assert the same thing several times. If any kind of assertion contains capturing subpatterns within it, these are counted for the purposes of numbering the capturing subpatterns in the whole pattern. However, substring capturing is carried out only for positive assertions, because it does not make sense for negative assertions.

Lookahead assertions

Lookahead assertions start with (?= for positive assertions and (?! for negative assertions. For example,

```
\w+(?=;)
```

matches a word followed by a semicolon, but does not include the semicolon in the match, and

```
foo(?!bar)
```

matches any occurrence of "foo" that is not followed by "bar". Note that the apparently similar pattern

```
(?!foo)bar
```

does not find an occurrence of "bar" that is preceded by something other than "foo"; it finds any occurrence of "bar" whatsoever, because the assertion (?!foo) is always true when the next three characters are "bar". A lookbehind assertion is needed to achieve the other effect.

If you want to force a matching failure at some point in a pattern, the most convenient way to do it is with (?!) because an empty string always matches, so an assertion that requires there not to be an empty string must always fail.

Lookbehind assertions

Lookbehind assertions start with (?<= for positive assertions and (?<! for negative assertions. For example,

(?<!foo)bar

does find an occurrence of "bar" that is not preceded by "foo". The contents of a lookbehind assertion are restricted such that all the strings it matches must have a fixed length. However, if there are several alternatives, they do not all have to have the same fixed length. Thus

(?<=bullock|donkey)

is permitted, but

(?<!dogs?|cats?)

causes an error. Branches that match different length strings are permitted only at the top level of a lookbehind assertion. An assertion such as

(?<=ab(c|de))

is not permitted, because its single top-level branch can match two different lengths, but it is acceptable if rewritten to use two top-level branches:

(?<=abc|abde)

The implementation of lookbehind assertions is, for each alternative, to temporarily move the current position back by the fixed width and then try to match. If there are insufficient characters before the current position, the match is deemed to fail.

PCRE does not allow the \C escape to appear in lookbehind assertions, because it makes it impossible to calculate the length of the lookbehind. The \X escape, which can match different numbers of bytes, is also not permitted.

Atomic groups can be used in conjunction with lookbehind assertions to specify efficient matching at the end of the subject string. Consider a simple pattern such as

```
abcd$
```

when applied to a long string that does not match. Because matching proceeds from left to right, PCRE will look for each "a" in the subject and then see if what follows matches the rest of the pattern. If the pattern is specified as

```
^.*abcd$
```

the initial .* matches the entire string at first, but when this fails (because there is no following "a"), it backtracks to match all but the last character, then all but the last two characters, and so on. Once again the search for "a" covers the entire string, from right to left, so we are no better off. However, if the pattern is written as

```
^(?>.*)(?<=abcd)
```

or, equivalently, using the possessive quantifier syntax,

```
^.*+(?<=abcd)
```

there can be no backtracking for the .* item; it can match only the entire string. The subsequent lookbehind assertion does a single test on the last four characters. If it fails, the match fails immediately. For long strings, this approach makes a significant difference to the processing time.

Using multiple assertions

Several assertions (of any sort) may occur in succession. For example,

```
(?<=\d{3})(?<!999)foo
```

matches "foo" preceded by three digits that are not "999". Notice that each of the assertions is applied independently at the same point in the subject string. First there is a check that the previous three characters are all digits, and then there is a check that the same three characters are not "999". This pattern does not match "foo" preceded by six characters, the first of which are digits and the last three of which are not "999". For example, it doesn't match "123abc-foo". A pattern to do that is

```
(?<=\d{3}...)(?<!999)foo
```

This time the first assertion looks at the preceding six characters, checking that the first three are digits, and then the second assertion checks that the preceding three characters are not "999".

Assertions can be nested in any combination. For example,

```
(?<=(?<!foo)bar)baz
```

matches an occurrence of "baz" that is preceded by "bar" which in turn is not preceded by "foo", while

```
(?<=\d{3}(?!999)...)foo
```

is another pattern that matches "foo" preceded by three digits and any three characters that are not "999".

Conditional subpatterns

It is possible to cause the matching process to obey a subpattern conditionally or to choose between two alternative subpatterns, depending on the result of an assertion, or whether a previous capturing subpattern matched or not. The two possible forms of conditional subpattern are

```
(?(condition)yes-pattern)
(?(condition)yes-pattern|no-pattern)
```

If the condition is satisfied, the yes-pattern is set; otherwise the no-pattern (if present) is set. If there are more than two alternatives in the subpattern, a compile-time error occurs.

There are three kinds of condition. If the text between the parentheses consists of a sequence of digits, the condition is satisfied if the capturing subpattern of that number has previously matched. The number must be greater than zero. Consider the following pattern, which contains non-significant white space to make it more readable (assume the PCRE_EXTENDED option) and to divide it into three parts for ease of discussion:

```
( \( )?    [^()]+    (?(1) \) )
```

The first part matches an optional opening parenthesis, and if that character is present, sets it as the first captured substring. The second part matches one or more characters that are not parentheses. The third part is a conditional subpattern that tests whether the first set of parentheses matched or not. If they did, that is, if subject started with an opening parenthesis, the condition is true, and so the yes-pattern is executed and a closing parenthesis is required. Otherwise, since

no-pattern is not present, the subpattern matches nothing. In other words, this pattern matches a sequence of non-parentheses, optionally enclosed in parentheses.

If the condition is the string `(R)`, it is satisfied if a recursive call to the pattern or subpattern has been made. At "top level", the condition is false.

If the condition is not a sequence of digits or (R), it must be an assertion. This may be a positive or negative lookahead or lookbehind assertion. Consider this pattern, again containing non-significant white space, and with the two alternatives on the second line:

```
(?(?=[^a-z]*[a-z])
\d{2}-[a-z]{3}-\d{2}  |  \d{2}-\d{2}-\d{2} )
```

The condition is a positive lookahead assertion that matches an optional sequence of non-letters followed by a letter. In other words, it tests for the presence of at least one letter in the subject. If a letter is found, the subject is matched against the first alternative; otherwise it is matched against the second. This pattern matches strings in one of the two forms `dd-aaa-dd` or `dd-dd-dd`, where aaa are letters and `dd` are digits.

Frequently Asked Questions

Changing the Type of the DBMS for Dr.Web Enterprise Suite

For Windows OS

1. Stop **Dr.Web® Enterprise Server** through Windows services or **Dr.Web® Enterprise Console**.
2. Run `drwcsd.exe` using the `exportdb` switch to export the content of the database to a file. The full command line (for Windows) looks as follows:

   ```
   "C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Enterprise Server" -var-root="C:\Program Files\DrWeb Enterprise Server\var" -verbosity=all exportdb D:\esbase.es
   ```

   It is presumed that **Dr.Web® Enterprise Server** is installed to the `C:\Program Files\DrWeb Enterprise Server` folder and the database is exported to a file `esbase.es`, which is in the root of disc `D`. Copy the line above to the clipbоard and paste to the cmd file and run the file.

   If the path to a file (or a file name) contains spaces or national characters, the path should be put in quotation marks:

   ```
   "D:\long name\esbase.es"
   ```

3. Start the **ES Server**, connect the Console to the Server and configure the Server to use a different DBMS. Cancel restarting the Server.
4. Stop the **ES** Server through Windows services or **Dr.Web® Enterprise Console**.
5. Run `drwcsd.exe` using the `initdb` switch to initialize a new database. The command line will look as follows:

```
"C:\Program Files\DrWeb Enterprise
Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Enterprise Server"
-var-root="C:\Program Files\DrWeb
Enterprise Server\var" -verbosity=all
initdb D:\Keys\agent.key - - root
```

It is presumed that the Server is installed to the `C:\Program Files\DrWeb Enterprise Server` folder and `agent.key` resides in `D:\Keys`. Copy this line to the clipboard and paste to the cmd file. Run the file then.

If the path to a file (or a file name) contains spaces or national characters, the path to the key should be put in quotation marks:

```
"D:\long name\agent.key"
```

6. Run drwcsd.exe using the `importdb` switch to import the database from the file. The command line will look as follows:

```
"C:\Program Files\DrWeb Enterprise
Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Enterprise Server"
-var-root="C:\Program Files\DrWeb
Enterprise Server\var" -verbosity=all
importdb D:\esbase.es
```

Copy this line to the clipboard and paste to the cmd file. Run the file.

7. Start **Dr.Web® Enterprise Server** through Windows services or **Dr.Web® Enterprise Console** and make sure everything works normally.

For UNIX OS

1. Stop **Dr.Web® Enterprise** Server using the script
   - for **Linux** OS: `/etc/init.d/drwcsd stop`
   - for **FreeBSD** OS: `/usr/local/etc/rc.d/drwcsd.sh stop`

   or via **Dr.Web® Enterprise** Console.

2. Start the Server with the `exportdb` switch to export the database to a file. The command line from the Server installation folder will look as follows:
   - for **Linux** OS: `"/etc/init.d/drwcsd exportdb /var/esbase.es"`

- for **FreeBSD** OS:
  `"/usr/local/etc/rc.d/drwcsd.sh exportdb /var/drwcs/esbase.es"`

It is presumed that the database is exported to `esbase.es`, which resides in the specified folder.

3. Start **Dr.Web® Enterprise** Server using the script

   - for **Linux** OS: `/etc/init.d/drwcsd start`
   - for **FreeBSD** OS:
     `/usr/local/etc/rc.d/drwcsd.sh start`

   connect **Dr.Web Enterprise Console** to the Server and configure the Server to use another database through the **ES Console** menu: **Administration** -> **Configure Dr.Web® Enterprise Server** -> **Database** tab.

You can also reconfigure the Server to use another database/DBMS by editing the Server configuration file `drwcsd.conf` directly. To do this, you should comment/delete the entry about the current database and enter the new database (for more details see Appendix G. Server Configuration File).

You will be prompted to restart the Server. Reject restarting.

4. Stop **Dr.Web® Enterprise Server** (see step **1**).

5. Run `drwcsd` using the `initdb` switch to initialize a new database. The command line will look as follows:

   - for **Linux** OS: `"/etc/init.d/drwcsd initdb /root/keys/agent.key -- root"`
   - for **FreeBSD** OS:
     `"/usr/local/etc/rc.d/drwcsd.sh initdb /root/keys/agent.key -- root"`

   It is presumed that the `agent.key` resides in the `/root/keys` folder.

6. Run `drwcsd` using the `importdb` switch to import the database from a file. The command line will look as follows:
   - for **Linux** OS: `"/etc/init.d/drwcsd importdb /var/esbase.es"`
   - for **FreeBSD** OS: `"/usr/local/etc/rc.d/drwcsd.sh importdb /var/esbase.es"`
7. Start **Dr.Web® Enterprise Server** (see step **3**).

If you want to change the parameters at Server start (for example, specify the Server installation folder, change the log level, etc.), you will have to edit the start script:
- for **FreeBSD** OS: `/usr/local/etc/rc.d/drwcsd.sh`
- for **Linux** OS and **Solaris** OS: `/etc/init.d/drwcsd`

Restoring the Database of Dr.Web Enterprise Suite

Dr.Web® ES regularly backs up important data (database contents, Server license key, private encryption key, Server configuration key, and Web Server configuration key). The backup files are stored in `\var\Backup`. For that purpose a daily task is included to the Server schedule. If such task is missing, it is strongly recommended to create it.

The copies are stored in the `.dz` format unpackable with `gzip` and other archivers. After unpacking all the files, except for the database contents, are ready to use. To restore the data, the database contents can be imported from the backup to another database of the Server by means of the `importdb` switch.

For Windows OS

1. Stop the **ES** Server.
2. Remove `dbinternal.dbs`.
3. Initialize a new database. In Windows the command line will look as follows:
   ```
   "C:\Program Files\DrWeb Enterprise Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Enterprise Server" -var-root="C:\Program Files\DrWeb Enterprise Server\var" -verbosity=all initdb D:\Keys\agent.key - - root
   ```
   The command must be entered in a single line. It is presumed that **Dr.Web® Enterprise Server** is installed to the `C:\Program Files\DrWeb Enterprise Server` folder and agent.key is located in `D:\Keys`.

   Once this command is executed, a new `dbinternal.dbs` of about 200 Kb will be generated in the var subfolder of the **ES** Server installation folder.
4. Import the content of the database from the correspondent backup file. The command line will look as follows:

```
"C:\Program Files\DrWeb Enterprise
Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Enterprise Server"
-var-root="C:\Program Files\DrWeb
Enterprise Server\var" -verbosity=all
importdb
"disc:\path_to_the_backup_file\database.dz"
```

The command must be entered in a single line. It is presumed that **Dr.Web® Enterprise Server** is installed to the `C:\Program Files\DrWeb Enterprise Server` folder.

5. Start the **ES** Server.

For UNIX OS

1. Stop the **ES** Server.
   - for **Debian** OS and **Solaris** OS:
     `/etc/init.d/drwcsd stop`
   - for **FreeBSD** OS:
     `/usr/local/etc/rc.d/drwcsd.sh stop`
   - for **other** supported versions:
     `/bin/drwcs.sh stop`
2. Remove `dbinternal.dbs` from the `var` subfolder of the Server installation folder.
3. Make sure that the `agent.key` file is in the `etc` subfolder of the Server installation folder. Then initialize the Server database. The command will look as follows:

   ```
   su drwcs -c "bin/drwcsd -var-root=./var
   -verbosity=all -log=./var/server.log initdb
   etc/agent.key - - password"
   ```

   It is presumed that **Dr.Web® Enterprise Server** is installed to the `C:\Program Files\DrWeb Enterprise Server` folder and `agent.key` resides in `D:\Keys`.

   Once this command is executed, a new dbinternal.dbs database of about 200 Kb will be generated in the var subfolder of the **ES** Server installation folder.
4. Import the content of the database from the correspondent backup. The command line will look as follows:

```
bin/drwcsd -var-root=./var -verbosity=all
-log=logfile.log importdb
/path_to_the_backup_file/database.dz
```

5. Start the **ES** Server.
   - for **Debian** OS and **Solaris** OS:
     `/etc/init.d/drwcsd start`
   - for **FreeBSD** OS:
     `/usr/local/etc/rc.d/drwcsd.sh start`
   - for **other** supported versions:
     `/bin/drwcs.sh start`

If some Agents were installed after the last backup had been made they will not be connected to the Server after the database has been restored from the backup. You should remotely reset them to the newbie mode. To do this, on Console's **Administration** menu, select **Configure Dr.Web® Enterprise Server**. A **Dr.Web® Enterprise Server configuration** window will open on the **General** tab. Select the **Reset unauthorized to newbie** checkbox.

As soon as the database is restored from the backup it is recommended to connect the Console to the Server. On the **Administration** menu, select **Dr.Web® Enterprise Server schedule** and check that the **Back up critical server data** task is on the list. If this task is absent, add it to the list.

Restoring the Server from Data Backup

Dr.Web® Enterprise Suite regularly backs up important data (database contents, Server license key, private encryption key, Server configuration key, and Web Server configuration key). The backup files are stored in `\var\Backup`. For that purpose a daily task is included to the Server schedule. If such task is missing, it is strongly recommended to create it.

The copies are stored in the `.dz` format unpackable with `gzip` and other archivers. After unpacking all the files, except for the database contents, are ready to use. To restore the data, the database contents can be imported from the backup to another database of the Server by means of the importdb switch (see p. Restoring the Database of Dr.Web Enterprise Suite).

It is also recommended to store copies of the following files on another PC: encryption keys `drwcsd.pri` and `drwcsd.pub`, license keys `enterprise.key` and `agent.key`, SSL certiifcate `certificate.pem`, and regularly copy Server database contents backup `database.dz`, Server and Web Server configuration files `drwcsd.conf` and `webmin.conf` to another PC. Thus you will be able to avoid data loss should the PC, on which the **ES** Server is installed, be damaged, and to fully restore the data and the functionality of the Server. If license keys are lost they may be requested once again, as specified in p. Key Files.

To restore a Server for Windows OS

Install **ES** Server software of the same version as the lost one on a working PC (see p. Installing the Anti-Virus Server for Windows). During the installation:

- If there is a copy of the DB (internal or external) on another PC and it is not damaged, in the respective dialog boxes of the installer specify it along with the saved files of the Server license key, private encryption key and Server configuration.

- If the Server DB (internal or external) was lost, but a backup of its contents database.dz is saved, then in the respective dialog boxes of the installer select creating a new database, specify the saved files of the Server and Agent license keys, private encryption key and Server configuration. After the installation import the DB contents from the backup (see p. Restoring the Database of Dr.Web Enterprise Suite).

Install the Console of the same version as the Server's (see p. Installing the Anti-Virus Server for Windows).

To restore a Server for Solaris OS

Install **ES** Server software of the same version as the lost one on a working PC (see p. Installing the Anti-Virus Server for UNIX system-based Operating Systems). During the installation:

- If there is a copy of the DB (internal or external) on another PC and it is not damaged, in the respective dialog boxes of the installer specify it along with the saved files of the Server license key, private encryption key and Server configuration.
- If the Server DB (internal or external) was lost, but a backup of its contents database.dz is saved, then in the respective dialog boxes of the installer select creating a new database, specify the saved files of the Server and Agent license keys, private encryption key and Server configuration. After the installation import the DB contents from the backup (see p. Restoring the Database of Dr.Web Enterprise Suite).

Install the Console of the same version as the Server's (see p. Installing the Anti-Virus Server for UNIX system-based Operating Systems).

To restore a Server for other UNIX system-based OS's

1. Install **ES** Server software of the same version as the lost one on a working PC (see p. Installing the Anti-Virus Server for UNIX system-based Operating Systems).
2. Put the saved files to:
   - for **Debian** OS: `/var/opt/drwcs/etc`, except for the public key. Put the latter to `/opt/drwcs/Installer/`

- for **FreeBSD** OS: `/var/drwcs/etc`, except for the public key. Put the latter to `/usr/local/drwcs/Installer/`
- for **Solaris** OS: `/var/drwcs/etc`, except for the public key. Put the latter to `/opt/drwcs/Installer/`

For all replaced files assign the same permissions as those set at the previous (lost) installation of the Server.

3. Generate a new SSL certificate:
   - for **Debian** OS and **Solaris** OS:
     `/etc/init.d/drwcsd selfcert`
   - for **FreeBSD** OS:
     `/usr/local/etc/rc.d/drwcsd.sh selfcert`
   - for **other** supported versions:
     `/opt/drwcs/bin/drwcsd -var-root=/var/drwcs -log=/var/drwcs/log/drwcsd.log selfcert`
4. The next steps depend on the availability of the Server database:
   a) If you have a working external DB, no further restoring procedures are needed, provided that you have the configuration file and the Server build is the same as the old one. Otherwise you will have to register the database in the configuration file and/or update the structure of the database with the upgradedb switch (see variant **c** below).
   b) If you have a backup of internal or external DB contents (`database.dz`), start the Server, remove the internal DB created at the installation, initiate creating a new one and import the contents of the old DB from the backup copy (see p. Restoring the Database of Dr.Web Enterprise Suite).
   c) If you have a saved copy of the internal DB, replace the new file with it:

   for **Debian** OS: `/var/opt/drwcs/dbinternal.dbs`

   for **FreeBSD** OS and **Solaris** OS: `/var/drwcs/dbinternal.dbs`

For all replaced files assign the same permissions as those set at the previous (lost) installation of the Server.

To upgrade the databases, execute the following commands:

for **Debian** OS and **Solaris** OS:

```
/etc/init.d/drwcsd upgradedb
```

for **FreeBSD** OS:

```
/usr/local/etc/rc.d/drwcsd.sh upgradedb
```

for **other** supported versions:

```
/opt/drwcs/bin/drwcsd -var-root=/var/
drwcs -log=/var/drwcs/log/drwcsd.log
upgradedb update-db
```

Launch the **ES** Server.

5. Install the Console of the same version as the Server's (see p. Installing the Anti-Virus Server for UNIX system-based Operating Systems).

If some Agents were installed after the last backup had been made they will not be connected to the Server after the database has been restored from the backup. You should remotely reset them to the newbie mode. For that purpose, on Console's **Administration** menu, select **Configure Dr.Web® Enterprise Server**. A **Dr.Web®** Enterprise Server configuration window will open on the **General** tab. Select the **Reset unauthorized to newbie** checkbox.

Converting the Private Encryption Key drwcsd.pri of Version 4.32 to the New Format

If you initially installed the Server version **4.32**, then after subsequent upgrading from **4.33** to **4.44** the private encryption key drwcsd.pri remains in the old format **4.32**. This key format is incompatible with the Server version **4.44** and higher, therefore having upgraded the Server from 4.33 to **4.44**, you have to convert the private encryption key to the new format. To do this

1. After you have installed Server version **4.44**, issue the following instruction:
   `\bin\drwsign join432 [-public-key=`*<path_name>*`] [-private-key=`*<path_name>*`]` *<new_private>*
2. Start the Server.
   - for **Windows** OS:
     `\bin\drwcsd start` or through the **Start menu** -> **Programs** -> **Dr. Web (R) Enterprise Server** -> **Server Control** -> **Start**.
   - for **UNIX** OS:
     `/usr/local/etc/init.d/drwcsd start`
   - for **FreeBSD** OS:
     `/usr/local/etc/rc.d/drwcsd start`.

Index

Index

Index

Index

Index