Dr.WEB®

Enterprise Security Suite

Defend what you create

Administrator Manual

Doctor Web

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

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

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

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

Table of Contents

Chapter 1: Welcome to Dr.Web® Enterprise Security 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 Security Suite** (hereinafter **Dr.Web ESS**).

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 **Dr.Web** components to assure the ultimate anti-virus protection.

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** at http://download.drweb.com/esuite/.

1.2. Conventions and Abbreviations

Conventions

The [following](#) conventions are used in the Manual.

Table 1-1. Conventions

Symbol	Comment
i Note, that	Marks important notes or instructions.
! Warning	Warns about possible errors.
Dr.Web ESS	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.

Abbreviations

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

- ◆ ACL – Access Control List,
- ◆ DB, DBMS — Database, Database Management System,
- ◆ DFS – Distributed File System,

◆ **Dr.Web GUS** — **Dr.Web Global Update System**,
◆ **Dr.Web ESS** — **Dr.Web Enterprise Security Suite**,
◆ EBNF — Extended Backus-Naur Form,
◆ GUI — Graphical User Interface, a GUI version of a program — a version using a GUI,
◆ LAN — Local Area Network,
◆ NAP — Network Access Protection,
◆ OS — operating system,
◆ PC — personal computer,
◆ UDS — UNIX domain socket.

1.3. About Dr.Web Enterprise Security Suite

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

Dr.Web Enterprise Security Suite 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 on all protected computers.

Dr.Web ESS 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 ESS has a *client-server* architecture. **Dr.Web ESS** components are installed on the computers of users and administrators and the computer(s) to function as the **Enterprise Server**(**s**), and

exchange information through network protocols TCP/IP, IPX/SPX, NetBIOS. An aggregate of computers on which **Dr.Web ESS** cooperating components are installed is called an *anti-virus network*.

An anti-virus network includes the following components:

Core components:

◆ *Dr.Web Enterprise Server (Enterprise Server)* stores distribution kits of anti-virus packages for different OS of protected computers, updates of virus databases, anti-virus packages and **Enterprise Agents**, user keys and package settings of protected computers. **Enterprise Server** sends necessary information to the correspondent computers on **Agents** requests and keeps a general log of events of the whole anti-virus network.

◆ *Dr.Web Control Center* is automatically installed with **Enterprise Server**. It is a certain extension of a web page and allows to administrate the anti-virus network by means of editing the settings of **Enterprise Server** and protected computers stored on **Enterprise Server** and protected computers.

◆ *Dr.Web Enterprise Agent (Enterprise Agent)* is installed on protected computers. It installs, updates and controls the anti-virus package as instructed by **Enterprise Server**. **Enterprise Agent** reports virus events and other necessary information about the protected computer to **Enterprise Server**.

Optional components:

◆ *Proxy server*. This component can optionally be included into the anti-virus network. The main function of the proxy server is to provide connection between **Enterprise Server** and **Enterprise Agents** in cases when direct connection is impossible. E.g. if the **Server** and **Agents** are located in different networks which do not have packet routing between them. At the expense of using caching function, reducing of network traffic and time of receiving **Agent** updates can be provided.

◆ *NAP Validator*. Allows to use *Microsoft Network Access Protection (NAP)* technology to check health of **Dr.Web** anti-virus software on protected workstations by enforcing compliance with system health requirements.

> **Enterprise 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 **Dr.Web Control Center** can be run on a different computer than the **Server**, there should be a network connection between them.
>
> The anti-virus network can incorporate several **Enterprise Servers**. The features of such configuration are described in the Manual in p. Peculiarities of a Network with Several Dr.Web Enterprise 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**. 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 **Enterprise Agent** functions. It is also an anti-virus scanner and uses the same virus databases and search engine. But this functionality is 'built in **Enterprise Agent**. **Dr.Web Enterprise Scanner** is meant to scan for viruses on demand: either according to the schedule, or a direct task from the **Dr.Web Control Center**. It has no special interface and no independent settings, it is configured only when run through the **Dr.Web Control Center** (when scanning is scheduled or initiated manually).

◆ *SelfPROtect System monitor* which protects files and directories used by **ESS** from unauthorized or accidental removal and modification by user or malicious software. With the system monitor running, access to these resources is granted to **Dr.Web** processes only.

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.

◆ *SpIDer Gate (an HTTP guard)* constantly resides in the computer memory and intercepts addresses to web sites. The guard neutralizes malicious software in http-traffic (for example, viruses in uploaded and downloaded files) and blocks access to suspicious or incorrect resources.

◆ *Dr.Web Office Control* resides in the computer memory and, with the respective settings, control access to network resources and specified local resources. In particular, allows you to limit access to specific web sites, which helps you control access to inappropriate web content. The component helps you ensure integrity of important files and protect them from threats, as well as limit access to inappropriate web sites for your employees.

◆ *Dr.Web FireWall* protects your computer from unauthorized access and prevents leak of vital data through networks. This component monitors connection attempts and data transfer and helps you block unwanted or suspicious connections both on network and application levels.

1.4. Benefits

Dr.Web ESS offers the following benefits:

◆ Cross-platform **Server** software enables using both Microsoft® Windows® and UNIX® system-based operated computers.

◆ Cross-platform **Agent** software enables anti-virus protection of computers operated under Microsoft Windows OS, Android OS, Microsoft® Windows® Mobile® OS, Novell® NetWare® OS, UNIX system-based OS and Mac OS X.

◆ Anti-virus protection of Microsoft® Outlook® mail system and mail system based on IBM® Lotus® Domino® server or Microsoft® Exchange Server.

◆ 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.

◆ Remote administration of the anti-virus protection (via the **Dr.Web Control Center**) almost from any computer under any OS.

◆ Centralized installation of **Enterprise 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 Server.**

◆ **Server** critical data (databases, configuration files, etc.) is backed up.

> In comparison to other anti-virus products, **Dr.Web ESS Anti-virus** can be installed on infected computers of users.

1.5. System Requirements

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

◆ **Enterprise 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**;

◆ for interaction between all anti-virus components, all following ports and sockets must be opened on computers with anti-virus components:

Number	Protocols	Purpose
2193, 2371 ports	TCP, UDP	For connection between the **Server** and anti-virus components.
2371 socket	IPX/SPX	For connection between the **Server** and anti-virus components.
2193, 2372 ports	UDP	For the Network Scanner.
139, 445 ports	TCP, UDP	For the **Network Installer**.
9080 port	http	For the Dr.Web Control Center.
9081 port	https	For the Dr.Web Control Center.

> The 2371 port is required for connection (via TCP and UDP protocols) between components of **4.XX** version. It is used for support of compatibility, particularly during upgrade of anti-virus network components.

The Dr.Web Enterprise Server requires:

◆ Intel® Pentium® III 667 MHz or faster;

◆ 512 MB RAM (1 GB 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);

> ⚠️ To install the **Server**, it is required at least 2,5 GB of free system disk space (it does not depend on **Server** installation disk) for the full distribution kit or 650 MB for the lite version of distribution kit to launch the installer and unpack temporary files.

◆ Microsoft Windows 2000 OS or later, Linux® OS, FreeBSD® OS or Solaris™ OS (see Appendix A. The Complete List of Supported OS Versions);

◆ For the installation of **Enterprise Server** for UNIX system-based OS: `libiconv` library v. `1.8.2` or later; `pcre`, `ncurses`, `openssl`, `libcrypto` and `libssl` (shared libraries, usually included into `openssl`), `libxml2`, `libpq` (only in case of using PostgreSQL database; in case of installation via the generic-packages, the library is already included in the package), `libcurl` v. `7.20.0` or later, `libldap`.

The Dr.Web Proxy Server requires:

◆ Intel Pentium III 667 MHz or faster;

◆ not less than 512 MB RAM;

◆ not less than 1 GB of free (available) disk space;

◆ Microsoft Windows 2000 OS or later, Linux OS, FreeBSD OS or Solaris OS (similarly to the **Dr.Web Enterprise Server**, see Appendix A. The Complete List of Supported OS Versions);

◆ For the installation of **Enterprise Server** for UNIX system-based OS: `libiconv` library v. `1.8.2` or later, `pcre`, `libxml2`.

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

The NAP requires:

For Server

◆ Microsoft® Windows Server® 2008 OS.

For the Agents

◆ Microsoft Windows XP SP3 OS, Windows Vista OS, Windows Server 2008 OS.

The Dr.Web Control Center requires:

◆ Windows® Internet Explorer® 7 and later or Mozilla® Firefox® 3.0 and later web browsers.

> ⚠️ Opera® 10 and later, Safari® 4 and later, Chrome® 7 and later web browsers also can be used. But operating under these web browsers is not guaranteed.
>
> If you install **Server** on a computer with a '_' (underline) character in the name, configuration of **Server** with **Dr.Web Control Center** by use of Windows Internet Explorer will not be available.
>
> In this case, use other web browser.
>
> For proper operation of **Control Center** in Microsoft Internet Explorer browser, IP address and/or DNS name of computer with installed **Enterprise Server** must be added to the trusted sites of browser, on which you open **Control Center**.
>
> For proper opening of **Control Center** via the **Start** menu in Microsoft Internet Explorer browser under Windows 8 and Windows Server 2012 OS with tiled interface, set the following parameters of a web browser: **Tools →** **Programs → Opening Internet Explorer** set the **Always in Internet Explorer** flag.

◆ **Dr. Web Browser-Plugin** to use **Dr.Web Control Center** in full. The plug-in is distributed with the **Server** installation package. It installs by browser request when you use elements

of **Dr.Web Control Center** which require the plug-in (for instance, for antivirus-components remote updater or **Network Scanner**).

⚠️ For operation of the **Dr.Web Browser-Plugin** at the **Network Scanner** page, under both Windows and GNU/Linux OS, you must have administrator (root) rights.

Under Safari web browser the **Dr.Web Browser-Plugin** is available under Windows OS only.

Under Mozilla Firefox, Opera and Chrome web browsers, the **Dr.Web Browser-Plugin** is available under Windows OS and Linux system-based OS only.

◆ Recommended screen resolution to use the **Dr.Web Control Center** is 1280x1024 pt.

The Dr.Web Enterprise Agent and the full anti-virus package require:

1. Minimal requirements:
   - ◆ Intel® Pentium® IV 1.6 GHz;
   - ◆ RAM 512 MB.

2. Recommended requirements:
   - ◆ Intel® Pentium® IV 2.4 GHz or faster;
   - ◆ RAM not less than 1 GB.

3. Not less than 250 MB of available disk space for executable files + extra disk space for logs and temporary files;

4. Operating systems (see <u>Appendix A. The Complete List of Supported OS Versions</u>):

   a) Microsoft Windows 98 OS, Windows Me OS, Windows NT4 OS (SP6) and later. Depending on OS, the following components can be installed:

Component	OS
SpIDer Gate, **SelfPROtect**, **Office Control**,	Windows 2000 with SP4 and later.

Component	OS
Dr.Web Browser-Plugin for Outlook	
SpIDer Guard NT4, **Dr.Web Scanner NT4**	• Windows 98, • Windows ME, • Windows NT4 (SP6a), • Windows 2000 with SP4 without Update Rollup1, • Windows XP without SP and with SP1, • Windows 2003 without SP.
FireWall, **SpIDer Guard G3**, **Dr.Web Scanner**	• Windows 2000 with SP4 and Update Rollup1, • Windows XP with SP2 and later, • Windows 2003 with SP1 and later, • Windows Vista and later.
SpIDer Mail NT4	• Windows 98, • Windows NT4 with SP6a.
SpIDer Mail	All supported OS later than systems for **SpIDer Mail NT4** version which are above-listed.

b) Microsoft® Windows Mobile® OS;

c) Novell NetWare OS;

d) UNIX system-based OS: Linux, FreeBSD and Solaris 10 (for Intel platform only);

e) Android OS;

f) Mac OS X.

5. For **Dr.Web for Outlook** plug-in the the Microsoft Outlook client from the Microsoft Office package is required:

   ◆ Outlook 2000 (Outlook 9),

   ◆ Outlook 2002 (Outlook 10 or Outlook XP),

   ◆ Office Outlook 2003 (Outlook 11),

   ◆ Office Outlook 2007,

◆ Office Outlook 2010.

6. The **Dr.Web Agent** context help requires Windows® Internet Explorer® 6.0 or later.

⚠️ 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 ESS**.

ℹ️ Functionality of **Agent** for Windows Mobile and Novell NetWare OS described in **Dr.Web Agent for Windows Mobile** and **Dr.Web Agent for Novell NetWare** user manuals.

1.6. Distribution Kit

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

1. For installation under UNIX system-base OSs, the following components are provided as `bzip2` archives or the respective OS installation packages:

   ◆ **Enterprise Server**,
   ◆ **Proxy Server**.

2. For installation under Microsoft Windows OS, the following components are provided as installation wizard executable files:

   ◆ **Enterprise Server**,
   ◆ **Proxy Server**,
   ◆ **Enterprise Agent** for Active Directory,
   ◆ **NAP Validator**.

The Enterprise Server is distributed in two variants:

1. *Full distribution kit* - includes distributions of all enterprise products, which are provided for installation at protected stations under all supported OS.

2. *Lite distribution kit* - distribution, whose composition is similar to composition of previous versions of **Dr.Web Enterprise Security Suite** distribution.

It is suitable for installing anti-virus protection, managed by **Dr.Web Enterprise Security Suite** on stations under Windows OS.

The Enterprise Server distribution kit contains the following components:

◆ **Enterprise Server** software for the respective OS,
◆ **Enterprise Agents** software and anti-virus packages software for supported OSs,
◆ **Dr.Web Control Center** 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

Rights to use the **Dr.Web ESS** are regulated by the following key files:

1. **Server** key file - `enterprise.key`.
2. Workstations key file - `agent.key`.

> ⚠️ 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 ESS** license parameters and price depend on the number of protected computers, which includes the servers protected by **Dr.Web ESS** network.

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

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

When purchasing a license for the **Dr.Web ESS** anti-virus, you receive registration keys or a registration card with a serial number.

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 key files for the **Server** and for workstations.

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 ESS** 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 Dr.Web Enterprise Server below.

The use of key files after the anti-virus network is established 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.

Chapter 2: Installation and Removal of Dr.Web Enterprise Security Suite Components

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 **Enterprise Server** software on the selected computer or computers.

3. Through the **Dr.Web Control Center**, update the product software in the **Server** repository.

4. Configure the **Server**(**s**) and workstations software.

5. Install and configure the **Proxy Server**, if necessary.

6. Install **Enterprise Agent** software on workstations and then register the anti-virus workstations at **Enterprise Server**.

> **i** **Agents** establish a connection with the **Server** immediately after the installation. Anti-virus workstations are authorized at the **Server** according to the set policy (see p. New Stations Approval Policy).

7. Through the **Dr.Web Control Center**, 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 **Enterprise Server**.

Enterprise Server can be installed on any computer of the local network, not only on that functioning as a local network server. General system requirements to this computer are described in p. System Requirements.

The **Dr.Web Control Center** can be run on a different computer than the **Server**, there should be a network connection between them.

The anti-virus network can incorporate several **Enterprise Servers**. The features of such configuration are described in p. Peculiarities of a Network with Several Dr.Web Enterprise Servers.

To install the **Server** and **Enterprise 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 **Enterprise Servers** and workstations.

2.2. Installing Dr.Web Enterprise Server

The installation of **Enterprise Server** is the first step in the installation of **Dr.Web ESS** anti-virus. Unless and until it is successfully installed, no other **ESS** components can be installed.

The installation procedure of **Enterprise Server** depends on **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.

If the **Server** software is already installed on your computer, see the Upgrading Dr.Web ESS for Windows® OS or Upgrading Dr.Web ESS for UNIX® System-Based Systems sections correspondingly.

If the previously installed **Server** was removed before installing the **Server** software, contents of the repository will be deleted during installation and the new version will be installed. If the repository of the previous version by some reason was not removed, it is necessary to manually delete the contents of the repository before installing the new version of the **Server** and then renew the repository after installation.

The language for the **Server** installation folder name must match to the language, specified in language settings of Windows OS for the non-Unicode programs. In opposite case, the **Server** will not be installed.

The english language is an exception for the installation folder name.

Together with **Enterprise Server**, the **Dr.Web Control Center** is installed, which serves to manage the anti-virus network and set up the **Server**.

By default, **Enterprise Server** will run automatically after the installation (for UNIX system-based OS you can change this option in installer settings).

2.2.1. Installing Dr.Web Enterprise Server for Windows® OS

Below is described the installation of **Enterprise 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 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.

Enterprise Server should be installed by a user with the administrator's rights to the computer.

After **Enterprise Server** is installed it is necessary to update all **Dr.Web ESS** components (see p. Manual Updating of the Dr.Web ESS 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).

Figure 2-1 illustrates the flowchart of **Enterprise Server** installation procedure. Steps in the flowchart correspond with the detailed description of the installation procedure shown below.
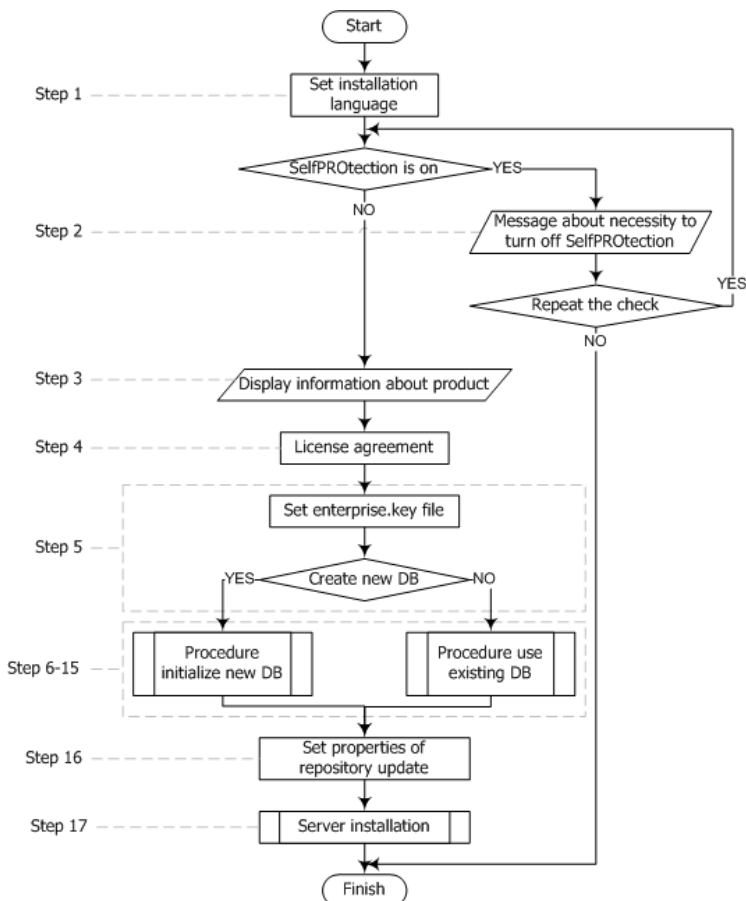
**Figure 2-1. The Dr.Web Enterprise Server installation procedure
flowchart (click any block in the flowchart to see its description)**

The flowchart contains three built-in procedures. The **Server
installation** procedure (step 17) does not require user intervention
(see description below) and is performed directly by the installer.

Figure 2-2. and Figure 2-3 illustrate installation procedure flowcharts
for cases **when a new DB is created** and **when an existing DB is
used**.
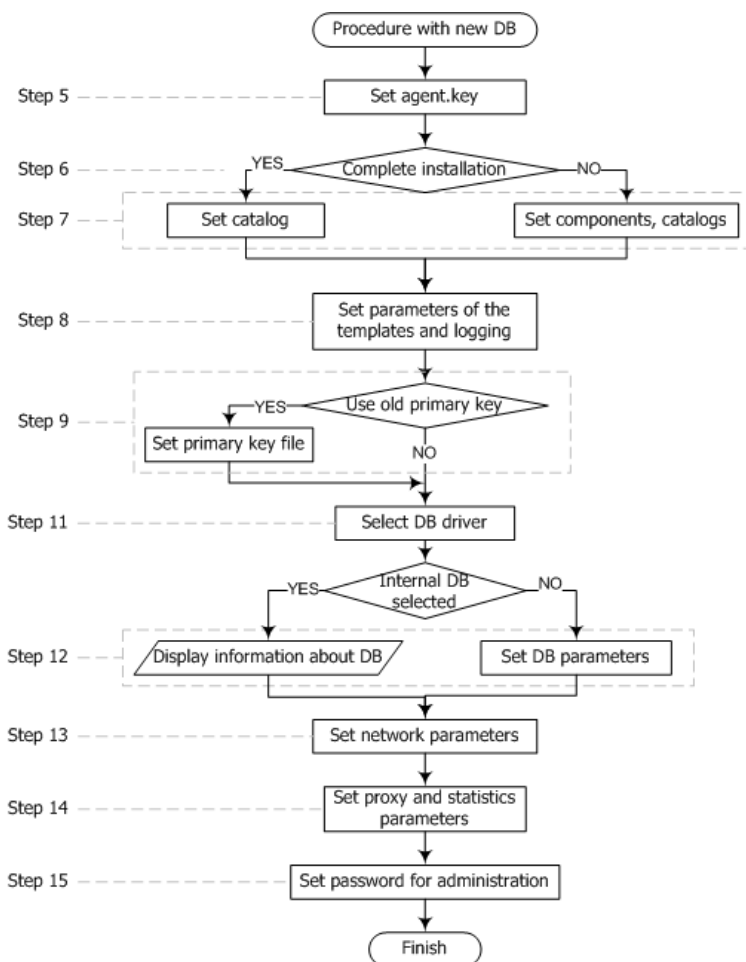
Figure 2-2. Flowchart of the installation procedure when a new DB is created (click any block in the flowchart to see its description)
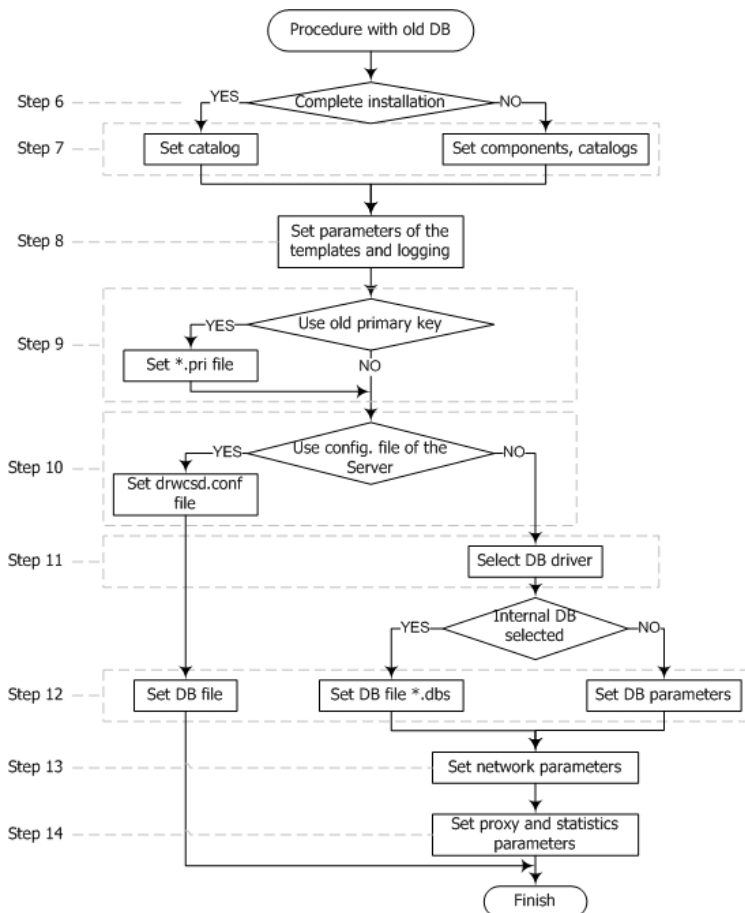
Figure 2-3. Flowchart of the installation procedure when an existing DB is used (click any block in the flowchart to see its description)

To install the Dr.Web Enterprise Server on a computer operated by Windows OS:

1. Run the distribution file. A window for choosing the language of the **Installation Wizard** will be opened. Select the necessary language and click **Next**.

2. If **Dr.Web Enterprise Security Suite** software is installed on

you computer and **Dr.Web SelfPROtect** is enabled, the wizard prompts you to disable it. Disable **SelfPROtect** and click **OK** to continue installation, or click **Cancel** to cancel **Server** installation.

3. A window with information about the program to be installed will be opened. Click **Next**.

4. A window with the text of the license agreement will be opened. 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**.

5. A window for selection of license key files will be opened.

   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**).

   For evaluation purposes a demo key file can be used. Click the **Demo keys** button to go to the official web site of **Doctor Web** company and receive the license key file (see Demo key files).

   Click **Next**.

6. A window for selecting the installation type will be opened. If you select **Complete**, all components of **Dr.Web Enterprise Security Suite** will be installed. If you select **Custom**, you will be able to specify the necessary components. After selecting the installation type click **Next**.

> ⚠️ If you are going to use the ODBC for Oracle as an external database, select the **Custom** option and disable the installation of Oracle client (in the **Database support** - **Oracle database driver** section) in the opened window.
>
> Otherwise, Oracle DB functioning will fail because of the libraries conflict.

7. If you selected **Complete** in the previous step, a window for changing the default installation folder (C:\Program Files\DrWeb Enterprise Server) will be opened. If necessary, click **Change** and specify the installation folder. Click **Next**.

   If you selected **Custom** in the previous step, a window for selecting the necessary components will be opened. You can change the installation parameters for each component in the context menu: install component locally, for network access or do not install component. If you wish to change the installation folder for a component, click **Change** and specify the installation folder. Click **Next**.

8. Next you can choose the language of the notification templates, set the **Agent** shared installation folder (hidden by default) and set up installation logging.

   If you want the **Server** to be started automatically after the installation, set the **Start service during setup** flag.

   If you want to add an exception for your operating system firewall (except the Windows 2000 OS) to allow **Server** operations, select **Add Server ports and interfaces to firewall exceptions**.

9. 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** flag and specify the file with the private key. A file with the public key will be created (contents of the public key will match the contents of the previous public key).

Otherwise after the installation it will be necessary to copy the new encryption key to all workstations, on which **Enterprise Agents** have been previously installed.

10. Next, if you have selected the existing database at step **5**, a window where you can specify a prearranged **Server** configuration file instead of that created by the installation program will appear.

    In the next series of windows the main settings stored in the **Server** configuration file should be specified (see Appendix G1. Dr.Web Enterprise Server Configuration File).

11. The database configuration dialog window allows you to adjust the parameters of the used database. These parameters depend on the database type specified in step **5** and the availability of the **Server** configuration file specified in step **10.**

    If you are creating a new DB or if the configuration file for an existing database was not specified, select the driver which should be used. The **IntDB database driver** option means that internal facilities of the **Enterprise Server** should be used. Other options imply usage of an external DB. Parameters of DBMS are described in the appendices (see Appendix B. The Description of the DBMS Settings. The Parameters of the DBMS Driver).

    Click **Next**.

12. If you selected **IntDB database driver** for creating a new DB in the previous step, the information for creating a new DB will be displayed.

    If you selected one of the options with an external DBMS, it will be necessary to specify access parameters for the DB.

    If you are using the **Server** DB from the previous installation and in the previous step you specify the **Server** configuration file or select **IntDB database driver**, it is necessary to specify the DB file. For this, click **Browse**. Set the **Verify database during setup** flag, to verify database integrity when installing the **Server**.

13. Next, if you selected creation of a new DB in step **5** or did not

specify the **Server** configuration file from previous installation in step **10** (for an existing DB), a window dedicated to network configuration will be opened. 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).

Specify appropriate **Server** access values in the **Interface** and **Port** fields. By default, interface is set to `0.0.0.0` which means that the **Server** can be accessed via any interface.

> By default port `2193` is using, but also port `2371` is supported for compatibility with anti-virus software older versions.

To limit the local access to the **Server**, set the **Restricted access to Dr.Web Enterprise server** flag. The Installer, **Agents** and other **Servers** (in case of an existing anti-virus network built with **Dr.Web Enterprise Security Suite**) will not be able to access the **Server**. You can change these settings later through **Dr.Web Control Center** menu **Administration → Dr.Web Enterprise Server → Modules**.

Set the **Server detection service** flag, 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** operation only to the internal network interface – `127.0.0.1,` click **Restricted**. With such settings the **Server** can be administrated only from the **Dr.Web Control Center** 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.

14. If you selected creation of a new DB in step **4** or did not specify the **Server** configuration file from previous installation in step **9** (for an existing DB), the next window will contain a request to send statistics on virus events to **Doctor Web** company. To do this, set the **Allow sending statistics** flag and edit corresponding fields. Default values for the **Server** is

stat.drweb.com, for **URL** – \update. You can also specify the **Username** and **Password** for identification of the sent statistics (contact the **Dr.Web Technical Support Service** for information about your user name and password). In the **Send every** <…> field specify an interval in minutes for sending the statistics. **Server** and **Send every** are the only obligatory fields.

If you are using a proxy server, you can also specify its parameters in this window. To do this, set the **Use proxy** flag and specify its address, user name and password.

The **Use proxy** flag will be available only if the **Server** installation folder does not contain configuration files from the previous installation.

15. If you selected creation of a new DB in step **4** in the next window specify an administrator password.

> ⚠ It is not allowed to use national characters in administrator password.

Click **Next**.

16. Next you are recommended to instruct updating of the repository during the installation. To do this, set the **Update repository** flag. Click **Next**.

17. Click **Install**. Further actions of the installation program do not require user intervention.

18. Once the installation is complete, click **Finish**.

> ⚠ Having installed the **Enterprise Server**, for correct forming of links during **Agent** installation packages creating, edit the value of the **ServerName** parameter in the webmin.conf configuration file located at the etc subfolder of the **Enterprise Server** installation folder. Uncomment this parameter and instead of www.example.com specify the IP address or DNS name of the computer on which **Enterprise Server** is installed and the port number in the following format:

> ServerName *<Server_Address>*:*<port_number>*
>
> Save the changes and restart the **Enterprise Server**.
>
> ---
>
> If you use a cluster system of **Enterprise Servers** and if you use custom port at the **Enterprise Server**, edit corresponding parameters in the download.conf configuration file, located in the etc subfolder of the **Enterprise Server** installation folder (see also Appendix G3. Download.conf Configuration File).

As a rule, **Enterprise Server** is administrated by means of the **Dr.Web Control Center**.

Elements to facilitate adjusting and managing the **Server** are placed in the main Windows OS menu by the installation wizard.

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

- ◆ 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** commands described in detail in Appendix H5. Dr.Web Enterprise Server.
- ◆ **Web interface** item opens the **Dr.Web Control Center** and connects to the **Server** installed at this computer (at the http:// localhost:9080).
- ◆ **Documentation** item opens administrator documentation in HTML format.

The installation folder of the Dr.Web Enterprise Server (for Windows OS) has the following structure:

- ◆ bin — here reside executable files of **Enterprise Server**;
- ◆ etc — contains the files where main program settings are stored, and licence keys of the **Server** (enterprise.key) and the **Agent** (agent.key);
- ◆ Installer — contains a program initializing the installation of **Enterprise Agent** on a computer and the public encryption

key file (`drwcsd.pub`);

◆ `update-db` — contains scripts necessary to update the structure of **Server** databases;

◆ `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 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.

◆ `webmin` — contains administrator's **Dr.Web Control Center**: documents, icons, modules.

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

2.2.2. Installing Dr.Web Enterprise Server for UNIX® System-Based OS

> Installation should be carried out in console under superuser account (**root**).

Package-based installation of the Dr.Web Enterprise Server on a UNIX system-based OS

1. To start installing the `drweb-esuite` package, use the following command:

For the Server under		Command
FreeBSD OS		`pkg_add` *<distribution_file_name>*`.tbz`
Solaris OS		1. `bzip2 -d` *<distribution_file_name>*`.bz2`
		2. `pkgadd -d` *<distribution_file_name>*
Linux OS	Debian® Ubuntu®	`dpkg -i` *<distribution_file_name>*`.deb`
	rpm-packages	`rpm -i` *<distribution_file_name>*`.rpm`

> **i** If **Enterprise 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` for **rpm distribution kits**;
> - `dpkg -i` *<distribution_file_name>*`.deb` for **deb distribution kits**.

Also, there are so-called `generic` packages, which can be installed on any Linux system-based OS including those which are not on the list of supported systems.

> ⚠ To install `generic` package under Linux system-based OS, it is required `glibc` library of same version as `generic` package is.

Installation is provided 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.

> Press ESC to return to the previous step of **Server** installation. Note, that in the step 2 in licence agreement window the ESC will exit installation.

> Administrator name is **admin** by default.

2. The following windows (the number and sequence of which can be different subject to the OS) contains information on the copyright and the text of the license agreement. To proceed the installation, you must accept the license agreement.

3. Next, you will be prompt to set the group and the user under name of which the **Server** will operate. The same user is the owner of the files of the **Enterprise Server**.

   For request on user creation, select **new**, to create a new user under name of which the **Dr.Web ESS** will be run. In the next menu, it is recommended to leave the default value and click **OK**. In the group selection menu, create a new group. In the next prompt, leave the default value.

4. In the next windows select the key file for the **Server** (enterprise.key) and for **Enterprise Agent** (agent.key), which are supplied with the distribution kit or for upgrade from the previous version, are stored in the /root/esuite_backup folder by default or in the folder, specified by you.

> ⚠️ During the installation in console mode quantity of wrong attempts of key input are restricted:
>
> ◆ for FreeBSD: 3 attempts;
>
> ◆ for Solaris: 2 attempts;
>
> On the expiry of all given attempts the installation will be terminated.

5. Next:

   ◆ In case you are installing a **Solaris** system-compatible version: you will be asked to create a new database for the **Enterprise 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 DB.

   If you are installing the **Enterprise Server** on your computer for the first time, press ENTER and specify the administrative password (login **admin**) password to access the **Server**. You can leave the default password - **root**. If you set you own password, for safety reasons, the typed password is not displayed on the screen. You must type the password twice (if specified passwords are differ, you will have to repeat the procedure - follow the instructions in appearing messages). The password should not be less than 4 characters.

   Next, you will be asked to create new encryption keys. If you have saved drwcsd.pri and drwcsd.pub keys, refuse to create a new DB (type **no**, press ENTER) and specify the full path to the existing keys. If you do not have saved keys, press ENTER to create new encryption keys.

   ◆ In case you are installing via the **deb** packages: you will be asked to specify the administrative password (login **admin**). You can leave the default password - **root**. If you set you own password, for safety reasons, the typed password is not displayed on the screen. You must type the password twice (if specified passwords are differ, you will have to repeat the procedure - follow the instructions in appearing messages). The password should not be less than 4 characters.

◆ For other cases: you will be asked to specify the administrative password (login **admin**). During password setting, for safety reasons, the typed password is not displayed on the screen. You must type the password twice (if specified passwords are differ, you will have to repeat the procedure - follow the instructions in appearing messages). The password should not be less than 8 characters.

⚠ It is not allowed to use national characters in administrator password.

After upgrade and manual initialization of DB, administration password is reset to default value.

For reasons of security policy, it is strongly recommended do not leave default registration data. Registration data (login and password) are needed for connecting to the **Server** via the **Control Center**.

6. If perl interpreter is installed, you will be prompt to configure some **Server** settings. In request for setup a certain type of parameters the default value is **no** (press ENTER), which means that parameters of this type will have default values. If you specify **yes** value, you will be able to set the values of proposed parameters (the default values of the parameters declared in the square brackets; to set them, press ENTER).

You can initiate the configuration of **Server** settings manualy (the perl environment must be installed as well). To do this, run the `configure.pl` script, that can be found in following directories:

◆ `/usr/local/drwcs/bin/` for FreeBSD OS;

◆ `/opt/drwcs/bin/` for Linux and Solaris OS.

`Configure.pl` script parameters described in the Application H5.9. Configuring the Dr.Web Enterprise Server Under UNIX System-Based OS.

7. 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.

Having installed the **Enterprise Server**, for correct forming of links during **Agent** installation packages creating, edit the value of the **ServerName** parameter in the `webmin.conf` configuration file located at:

- ◆ `/var/drwcs/etc` for **FreeBSD** OS and **Solaris** OS
- ◆ `/var/opt/drwcs/etc` for **Linux** OS

Uncomment this parameter and instead of www.example.com specify the IP address or DNS name of the computer on which **Enterprise Server** is installed and the port number in the following format:

ServerName <*Server_Address*>:<*port_number*>

Save the changes and restart the **Enterprise Server**.

If you use a cluster system of **Enterprise Servers** and if you use custom port at the **Enterprise Server**, edit corresponding parameters in the `download.conf` configuration file, located in the `etc` subfolder of the **Enterprise Server** installation folder (see also Appendix G3. Download.conf Configuration File).

In the course of the installation of the **Enterprise 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 **Enterprise 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.

2.2.3. Installing Dr.Web Browser-Plugin

Under Mozilla Firefox, Opera ans Chrome web browsers,
the **Dr.Web Browser-Plugin** installation is available under
Windows OS and Linux system-based OS only.

Dr.Web Browser-Plugin is used to operate the **Dr.Web Control
Center** in full (see also the System Requirements section).

The plug-in is distributed with the **Server** installation package and can
be installed:

1. Automatically, by browser request when you use **Dr.Web
   Control Center**, particularly, elements which require the plug-
   in (antivirus-components remote updater or **Network
   Scanner**).
2. Manually, via the **Dr.Web Browser-Plugin** installer.

Manually Installation of Dr.Web Browser-Plugin

***To download Dr.Web Browser-Plugin for manually
installation:***

1. Open the **Dr.Web Control Center**. If **Dr.Web Browser-
   Plugin** for using browser is not installed yet, under the main
   menu, recommendation on plug-in installation will be
   presented.
2. Follow the **Install Dr.Web Browser-Plugin** link.

Figure 2-4. Section for downloading Dr.Web Browser-Plugin

3. In the plug-in download section, version of current browser and offered plug-in bit rate (x86 or x64) are represented.

   For UNIX system-based systems you can select distribution kit for corresponding OS from the drop-down list.

4. To download and save the plug-in, click **Download**. After this, you can install the plug-in manually.

5. To change the bit rate of the plug-in, click the link under download button, after this you can download installer as described at step **4**.

To install the Dr.Web Browser-Plugin under Windows OS:

1. Run the installation file. On the Welcome page of the **InstallShield Wizard**, click **Next**.

2. On the **License Agreement** page, read the agreement. To accept the agreement and proceed with the installation, select **I accept the terms of the license agreement** and click **Next**. To exit the wizard, click **Cancel**.

3. A window for changing the default installation folder will be opened. If necessary, click **Change** and specify the installation folder. Click **Next**.

4. Click **Install**. The installation begins. Further actions of the installation program do not require user intervention.

5. When installation completes, click **Finish**.

To install the Dr.Web Browser-Plugin under UNIX system-based OS:

Execute the following command:

- for **deb** packages:

  ```
  dpkg   -i   drweb-esuite-plugins-linux-
  <distribution_version>.deb
  ```

- for **rpm** packages:

  ```
  rpm    -i    drweb-esuite-plugins-linux-
  <distribution_version>.rpm
  ```

- for other systems (**tar.bz2** and **tar.gz** packages):

  1. Unpack the archive with browser plug-in.

  2. Create a directory for browser plug-ins, if it is not exist.

  For example, for Mozilla Firefox browser: `mkdir /usr/ lib/mozilla/plugins`

  3. Copy unpacked at step 1 library to the plug-ins directory.

  For example, for Mozilla Firefox browser: `cp libnp*.so /usr/lib/mozilla/plugins`

> After installation of the **Dr.Web Browser-Plugin** under UNIX system-based OS, restart web browser, if it was started.

2.3. Installing Dr.Web Enterprise Agent under Windows® OS

> **Enterprise Agent** should be installed under Administrator account of the respective computer.
>
> If **Enterprise Agent** is installed on the computer, you must uninstall the **Agent** before the installation.

Enterprise Agent and the anti-virus package can be installed in two ways:

1. Remotely – on the **Server** through the network. Performed by the anti-virus network administrator. No user interference required. You can find detailed description in the Remote Installation of the Dr.Web Enterprise Agent (for Windows® OS) section.

2. Locally – directly on the user's machine. May be performed both by the administrator or the user. For installation, you can use the following files (see Installation Files for details):

    ◆ `esinst.exe` Installation Package.
    ◆ `drwinst` **Agent** Network Installer.

For installation of Enterprise Agent on LAN servers and cluster computers, consider the following:

◆ For installation on computers which implement terminal servers functions (the **Terminal Services** are installed on Windows OS), to provide **Agents** operation in user's terminal sessions, **Agents** software must be installed locally, via the Add or Remove Programs Wizard on **Control Panel** of Windows OS.

◆ It is not recommended to install **SpIDer Gate**, **SpIDer Mail** and **Dr.Web Firewall** components on servers which implement significant network functions (domain controllers, licence distribution servers and etc.) to avoid probable conflicts between network services and internal components of **Dr.Web** antivirus.

◆ Installation of the **Agent** on a cluster must be performed separately on each cluster node.

◆ The operation principles for **Agents** and anti-virus package on the cluster node are similar to those on a standard LAN server, thus, it is not recommended to install **SpIDer Gate**, **SpIDer Mail** and **Dr.Web Firewall** components on cluster nodes.

◆ If access to quorum resource of a cluster is severely restricted, it is recommended to exclude it from the scan by the **SpIDer Guard** and confine by regular checks of the resource via **Scanner** launched by scheduler or manually.

2.3.1. Installation Files

Installation Package (esinst)

After a new user account is created, `esinst` **Agent** installation package is generated.

Link for the **Agent** installation package for the concrete station downloading is available:

1. After adding a new station (see the **11** step in the Creation of a New User Account section).
2. In any time after station adding:
    ◆ in station properties after its creation,
    ◆ in the **Selected objects** section for the station selected in hierarchical list.

Network Installer (drwinst)

The `drwinst` **Agent** network installer and the `drwcsd.pub` public encryption key reside in the `Installer` folder (the shared hidden resource) of the **Enterprise Server** installation folder. Network sharing at the 8 step during **Enterprise Server** installation is set. You can change this resource further.

The **Agent** installer and the public key are also available at the installation page of the **Dr.Web Control Center**.

Installation Page

At the installation page of the **Dr.Web Control Center** you can download:

1. The `drwinst` **Agent** network installer.

    Installers for different OS in corresponding named folders are

located.

2. The `drwcsd.pub` public encryption key.

From any computer with network access to the **Server**, installation page is available at the following address:

`http://`*<Server_address>*`:`*<port_number>*`/install/`

where *<Server_address>* is the IP address or DNS name of the computer on which **Enterprise Server** is installed. And the *<port_number>* should be `9080` (or `9081` for https).

2.3.2. Installing Dr.Web Enterprise Agent via the Installation Package

To install the Agent and anti-virus package, do the following:

1. Via the **Control Center**:
   ◆ Create an account for a new user at the **Server**.
   ◆ Get a link to download the **Agent** installation file.
2. Send the **Agent** installer link to the customer.
3. Install the Agent on a workstation. As a rule, users install **Enterprise Agent** software on their computers independently.
4. The new anti-virus workstation will be automatically authorized at the **Server** by default (see also p. New Stations Approval Policy).

2.3.2.1. Creation of a New User Account

To create a user account or several user accounts, use the **Dr.Web Control Center**.

> ⚠️ Make sure that the **ServerName** parameter in the configuration file `webmin.conf` has the value of the following format:

<Server_address>:9080,

where *<Server_address>* is IP address or DNS name of the computer with the **Enterprise Server** installed.

> ⚠️ The name of the **Server** to which the **Control Center** connects is specified in **Enterprise Agent** installation packages. Therefore, when you create a new account via the **Control Center**, make sure that the **Control Center** connects to the **Server** using the IP-address of the domain for which you create an account. Otherwise you will not be able to connect to the **Server** when installing the **Agent**.
>
> When you setting a connection between the **Control Center** and the **Server**, make sure that the **Server** address is not a loopback (127.0.0.1).

To create a new user via the Dr.Web Control Center, do the following:

1. Select the **Network** item in the main menu of the **Control Center**.

2. In the toolbar, click ➕ **Add a station or a group**. In the opened submenu, select the 📥 **Add a station** option. A pane for the new user account creation will be opened in the right pane of the **Dr.Web Control Center**.

3. In the **Count** entry field, specify the number of accounts to be created.

4. In the **ID** field, unique identifier of created station will be generated automatically. You can edit it, if necessary.

5. In the **Name** field, specify the station name, that will be displayed in the anti-virus network hierarchical list. Further, after the station is connected with the **Server**, this name can be automatically changed to the station name, which is specified locally.

6. In the **Password** and **Retype password** fields, specify a password for accessing the **Server**.

> When creating more than one account, **ID**, **Name** and **Password** (**Retype password**) fields are set automatically and can not be changed at the station creation stage.

7. In the **Description** field, specify additional information about the customer. This parameter is optional.

8. In the **Groups** section, specify groups in which the created station will be included. By default, station is included in the **Everyone** group. If custom groups are available, you can include the station in those groups. To do this, click the group name in the **Known groups** list. To exclude a station from customer groups, click the group name in the **Member of** list.

   To set a primary group for the creating station, click the icon of the corresponding group from the **Member of** list. The **1** will appear on the group icon.

   You cannot exclude stations from the **Everyone** and a primary groups.

9. Specify parameters of the **Security** section, if necessary. Parameters of this section are described in the p. Management of Stations Configuration.

10. Specify parameters of the **Location** section, if necessary.

11. Click **Save** in the upper right corner. The opened pane contains information about successful creation of a station, its ID and the link to download the **Agent** distribution kit.

> Link for the **Agent** installation package downloading is also available:
> ◆ in station properties after its creation,
> ◆ in the **Selected objects** section for the station selected in hierarchical list.
>
> See also the Installation Files section.

12. Further actions to install the **Agent** described below.

> ⚠️ **Enterprise Agent** should be installed by a user with the administrator rights to the computer.
>
> If anti-virus software has already been installed on a workstation, then before starting installation the installer will attempt to remove it. If the attempt fails, the user will have to uninstall the anti-virus software from his computer by himself.

2.3.2.2. Installing Dr.Web Enterprise Agent and Anti-Virus Package

To install the anti-virus software (Dr.Web Enterprise Agent and anti-virus package):

1. Download **Agent** installation file. To do this, follow the link generated in the **Control Center**.
2. Run the downloaded `esinst.exe` file at the station. A window of the **Installation Wizard** of the **Dr.Web** anti-virus will be opened.
3. Before installation, Wizard asks you to confirm that there is no anti-virus programs on you computer. Make sure, that there is no anti-virus software (including other versions of **Dr.Web** programs) installed on your computer and set the **I do not have other anti-viruses installed on my computer** flag. Click **Next**.
4. In the next window, choose the type of installation:
   - ◆ **Quick (Recommended)** - the most simple type of installation. All parameters are set automatically. Next, go to step **8**.
   - ◆ **Custom** - the type of installation that allows you to choose anti-virus components to install on your computer.
   - ◆ **Administrative** - the most detailed type of installation. Allows you to set/change all parameters of installation and anti-virus software.
5. If you choose **Custom** or **Administrative** types of installation, in the next window you will be offered to overview the components of **Dr.Web** anti-virus package. Set the flags

for components you want to install on your computer.

In the **Installation folder** field specify the path to install the anti-virus software. To set/change the default path, click the **Browse** and specify the necessary path.

Click **Next**.

For the **Custom** type of the installation, go to the step **8**.

6. If you choose **Administrative** type of installation, in the next window specify the settings of **Network installer**:

   ◆ In the **Dr.Web Enterprise Server** field, set the network address of the **Server** from which the **Agent** and the anti-virus package will be installed. If you specified **Server** address while launching the installer, it will be automatically set in this field.

   i   If you use the installer, created in the **Control Center**, the **Dr.Web Enterprise Server** field will be set automatically.

   If you do not know the **Server** address, click the **Find** button. The window for network searching of active **Servers** will be opened. Specify the necessary fields (in format: *<Server_name>*@*<IP-address>*/*<network_prefix>*:*<port>*) and click **Find**. In the list of founded **Servers** choose one for installation of the anti-virus software and click **OK**.

   ◆ In the **Dr.Web Enterprise Server public key** field, specify the path to the public key (drwcsd.pub) on your computer (if launching the installer from the Server via network, the key will be copied to the temporary files and after the installation it will be moved to the installation folder).

   ◆ In the **Installation directory** field, specify the path to your computer for the anti-virus software installation. By default, it is the Dr.Web Enterprise Suite folder located at the Program files at the system disk.

- ◆ In the **Use compression during download** section, select the traffic compression option: **Yes** - use compression, **No** - do not use compression, **Maybe** - **Server** choice.

- ◆ The **Add Dr.Web Agent to windows firewall exclusion list** flag prescribes to add ports and interfaces of **Agent** for an exception for your operating system firewall (except Windows 2000 OS). It is recommended to set the flag. It will help to avoid errors, e.g. during the automatic updates of the anti-virus software and virus bases.

- ◆ Set the **Register Agent in system list of installed software** flag, if necessary.

  This option also allows to delete the **Agent** and antivirus package by means of standard Windows OS services (see Uninstalling the ESS Software for Windows® OS).

7. For the **Administrative** type of the installation: in the next window specify the settings of **Agent**:

- ◆ In the **Authorization** section the parameters for **Agent** authorization at **Server** are set. For the **Automatic (Default)** option, the mode of the station access defines at **Server**. For the **Manual** option, you must specify the authorization parameters: the station **Identifier** and its **Password** for the access to **Server**. The station will have access permission without manually confirmation by the administrator at **Server**.

> If you use the installer, created in the **Control Center**, **Identifier** and **Password** fields will be set automatically.

- ◆ In **Compression** and **Encryption** sections set modes of traffic between **Agent** and **Server** (for more details, see p. Traffic Encryption and Compression).

  Click **Next**.

8. The installation of **Agent** and anti-virus components will start (does not require user intervention).

9. After the installation is complete, the Installation Wizard will request to restart you computer. Click **Finish** for the

Installation Wizard closedown.

10. Restart the computer.

> ℹ️ Immediately after installation **Agents** automatically establish a connection with the **Server**. Once an **Agent** has connected to the **Server** the name of the respective workstation appears in the anti-virus network catalog of the **Dr.Web Control Center**.

Enterprise Agents can be installed on workstations remotely through the **Dr.Web Control Center**.

2.3.3. Installing Dr.Web Enterprise Agent via the Network Installer

> ⚠️ You must update the **Server** repository before the first installation of the **Agent** (see p. Manual Updating of the Dr.Web ESS Components, p. **Checking for Updates**).

If the network installer is run in the normal installation mode (i.e. without –uninstall switch) on stations where the installation has already been performed, this will not incur any actions. The installer program terminates with a help window, contains available switches.

There are two modes of installation via the Network installer:

1. Background mode.
2. Graphical mode.

You can also install **Enterprise Agent** remotely with the help of the **Dr.Web Control Center**, or the facilities of **Active Directory** (see p. Remote Installation of the Dr.Web Enterprise Agent).

2.3.3.1. Installing Dr.Web Enterprise Agent in the Background Mode of the Installer

To install Dr.Web Enterprise Agent in the background mode of the installer:

1. From the workstation, on which you want to install the anti-virus software, enter the network catalog of **Agent** installation located at the **Server** (by default, it is `Installer` folder) and run the `drwinst` programm.

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

   > When you use the **Multicast** mode to find active **Servers**, the **Agent** installation is performed from the first founded **Server**. If the `pub`-key is not fitted to the **Server** key, installation will be failed. In this case, expressly specify the **Server** address (as described below).

   The `drwinst` command may be used with switches:

   - ◆ If the **Multicast** mode is not used to detect the **Server**, it is recommended to specify a domain name for the **Enterprise Server** in the DNS service and use this name when installing the **Agent**:

     `drwinst` *<Server_DNS_name>*

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

   - ◆ You can expressly specify the **Server** address as follows:

     `drwinst 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.

◆ To launch the installation in the graphical mode, use the –`interactive` parameter.

> ⓘ The complete list of **Network Installer** parameters is describe in the Appendix H4. Network Installer.

2. After the installation, the software of **Enterprise Agent** is installed on your computer (anti-virus package is not installed yet).

3. After the station has been approved at the **Server** (if it is required by **Enterprise Server** settings), the anti-virus package will be automatically installed.

4. Restart the computer on **Agent** request.

2.3.3.2. Installing Dr.Web Enterprise Agent in the Graphical Mode of the Installer

To install Dr.Web Enterprise Agent in the graphical mode of the installer:

1. From the workstation, on which you want to install the anti-virus software, enter the network catalog of **Agent** installation located at the **Server** (by default, it is `Installer` folder) and run the `drwinst.exe` with the `–interactive` parameter.

   A window of the **Installation Wizard** of the **Dr.Web** anti-virus will be opened.

2. Before the installation, the Wizard asks you to confirm that there is no anti-virus plug-ins on you computer. Make sure, that there is no anti-virus software (including other versions of **Dr.Web** programs) installed on your computer and set the **I do not have other anti-viruses installed on my computer** flag. Click **Next**.

3. In the next window choose type of installation:

   ◆ **Quick (Recommended)** - the most simple type of installation. All parameters are set automatically. Next, go to step **7**.

◆ **Custom** - the type of the installation that allows you to choose the anti-virus components to install on your computer.

◆ **Administrative** - the most detailed type of installation. Allows you to set/change all parameters of the installation and the anti-virus software.

4. If you choose **Custom** or **Administrative** types of installation, in the next window you will be offered to overview the components of **Dr.Web** anti-virus package. Set flags for the components you want to install on your computer.

In the **Installation path** field specify the path to install the anti-virus software. To set/change the default path, click the **Browse** and specify the necessary path.

Click **Next**.

If you chose **Custom** type of installation, go to the step **7**.

5. For the **Administrative** type of the installation: in the next window specify the settings of the **Network installer**:

◆ In the **Dr.Web Enterprise Server** field, set the network address of the **Server** from which the **Agent** and the anti-virus package will be installed. If you specified the **Server** address while launching the installer, it will be automatically set in this field. If you do not know the **Server** address, click the **Find** button. The window for network searching of active **Servers** will be opened. Specify the necessary fields in format: *<Server_name>*@*<IP-address>*/
<network_prefix>:*<port>* and click **Find**. In the list of founded **Servers** choose the one for the installation of the anti-virus software and click **OK**.

◆ In the **Dr.Web Enterprise Server public key** field, specify the path to the public key (drwcsd.pub) on your computer (if launching the installer from the **Server** via network, the key will be copied to the temporary files and after the installation it will be moved to the installation folder).

◆ In the **Installation directory** field, specify the path to the anti-virus software installation. By default, it is the `Dr.Web Enterprise Suite` folder located at the `Program files` at the system disk.

◆ At the **Use compression during download** section, select the traffic compression option: **Yes** - use compression, **No (Default)** - do not use compression, **Possible** - **Server** choice.

◆ The **Add Dr.Web Agent to windows firewall exclusion list** flag prescribes to add the ports and interfaces of the **Agent** for an exception for your operating system firewall (except the Windows 2000 OS). It is recommended to set the flag. It will help to avoid errors, e.g. during the automatic updates of the anti-virus software and virus bases.

◆ Set the **Register Agent in system list of installed software** flag, if necessary.

This option also allows to delete the **Agent** and antivirus package by means of standard Windows OS services (see Uninstalling the ESS Software for Windows® OS).

6. For the **Administrative** type of the installation: in the next window specify the settings of the **Agent**:

◆ In the **Authorization** section set parameters for **Agent** authorization at **Server.** For the **Automatic (Default)** option, authorization parameters (ID and password) are generated at the **Server** automatically, and the mode of the station access is defined at **Server**. For the **Manual** option, you must specify following authorization parameters: the station **Identifier** and its **Password** for access to the **Server**. The station will have access permission without manually confirmation by administrator at **Server**.

◆ In **Compression** and **Encryption** sections set modes of traffic between **Agent** and **Server** (for more details, see p. Traffic Encryption and Compression).

Click **Next**.

7. Installation of **Agent** will start. When installation is complete, click **Finish** for Installation Wizard closedown.

8. After the station has been approved at the **Server** (if it is required by **Enterprise Server** settings or if the **Manual** option has not been set at step 6 during **Administrative** installation), the anti-virus package will be automatically installed.

9. Restart the computer on **Agent** request.

2.4. Remote Installation of the Dr.Web Enterprise Agent under Windows® OS

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

> ⚠ Remote installation of **Enterprise Agents** is possible only on workstations operated by Windows 2000 and later OS (see Appendix A. The Complete List of Supported OS Versions), except Starter and Home editions.
>
> Remote installation of **Enterprise Agents** is possible only from the **Control Center** opened under Windows XP and later OS (see Appendix A. The Complete List of Supported OS Versions), except Starter and Home editions.
>
> To install the anti-virus software on workstations, you must have administrator rights on the correspondent computers.

Remote installation does not require extra configuration of the remote station, if it is inside a domain and the domain account is used. If the remote station is outside a domain, or if the local account has been used during installation, for some of Windows OS, the extra configuration of the remote station is required.

Extra Configuration for Remote Installation to a Station outside a Domain or Using the Local Account

> ⚠️ Specified options can reduce remote station security. It is strongly recommended to examine functions of these options before editing the system settings or do not use remote installation and install the Agent manually.

To install the **Agent** to a remote workstation outside a domain, or/and using the local account, do the following on the computer where you want to install the **Agent**:

Operating System	Configuring
◆ Windows 2000 ◆ Windows Server 2000	Extra configuration is not required.
◆ Windows XP	1. Setup the mode of access to shared files: **Control Panel** → **Folder Properties** → the **View** tab → clear the **Use Simple Sharing (recommended)** flag. 2. Set the following mode of network authentication model in the local policies: **Control Panel** → **Administrative Tools** → **Local Security Policy** → **Security Settings** → **Local Policies** → **Security Options** → **Network Access: Sharing and security model** → **Classic - local users authenticate as themselves**.
◆ Windows Server 2003	Extra configuration is not required.

Operating System	Configuring
◆ Windows Vista ◆ Windows 7 ◆ Windows Server 2008	1. Enable the **File sharing** option: **Control Panel → Network and Internet → Network and Sharing Center → Sharing and discovery → File Sharing → Enable**. 2. Enable the local administrator account and set a password for it. Use this account during installation: **Control Panel → System and Maintenance → Administrative Tools → Computer management → Local Users and Groups → Users**. Click the **Administrator** item → clear the **Account is disabled** flag → **OK**. Right-click the item → **Change password** → set the password.

If user account at the remote computer has the empty password, set the access policy with empty password in local policies: **Control Panel → Administrative Tools → Local Security Policy → Security Settings → Local Policies → Security Options → Accounts: Limit local account use of blank passwords to console logon only → Disabled**.

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

2.4.1. Installing Dr.Web Enterprise Agent Software via the Dr.Web Control Center

The following means of remote Agent installation on network workstations are available:

1. Installation via the Network Scanner.

   Allows to perform preliminary search of unprotected computers in the network and installation the **Enterprise Agents** on them.

2. Installation using the Network Installation tool.

   Fits for cases, when address of station or groups of stations on which the **Agent** will be installed, is previously known.

3. Installation on stations with specified ID.

   Allows to install **Agents** for selected accounts (including all new accounts) with specified ID and password for **Server** access on stations and groups of stations.

> For proper operation of **Network Scanner** and the **Network Installation** tool under Microsoft Internet Explorer browser, IP address and/or DNS name of computer with installed **Enterprise Server** must be added to the trusted sites of browser, on which you open **Control Center** for remote installation.

Using the Network Scanner

In the **Dr.Web Control Center**, the anti-virus network hierarchical list 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 Security Suite** and to install anti-virus components remotely.

To quickly install the **Agent** software on workstations, it is recommended to use **Network Scanner** which searches for

computers by IP addresses.

To install the Dr.Web Enterprise Agent via the Network Scanner:

1. Open the Network Scanner. On the **Administration** menu of the **Dr.Web Control Center**, select **Network scanner**. A **Network scanner** window with no data loaded will be opened.

2. In the **Networks** field specify networks in the following format:

    ◆ with a hyphen (for example, `10.4.0.1–10.4.0.10`)

    ◆ separated by a comma with a whitespace (for example, `10.4.0.1–10.4.0.10,` `10.4.0.35–10.4.0.90`)

    ◆ with a network prefix (for example, `10.4.0.0/24`).

    Detailed description of additional parameters is given in p. Network Scanner.

3. Click **Start Scanner**. The catalog (hierarchical list) of computers demonstrating where the **Dr.Web ESS** anti-virus software is installed will be loaded into this window.

4. Unfold the catalog elements corresponding to workgroups (domains). All elements of the catalog corresponding to workgroups and individual stations are marked with different icons the meaning of which is given below.

Table 2-1. Icons of the Network scanner

Icon	Meaning
Workgroups	
⚠	The work groups containing inter alia computers on which the **Dr.Web ESS** anti-virus software can be installed.
🔘	Other groups containing protected or unavailable by network computers.
Workstations	
🖥	The detected station is registered in the DB and active (i.e. the workstation with installed anti-virus software).
🖥	The detected station is registered in the DB as deleted (i.e. the workstation is listed in the table of deleted stations).
🖥	The detected station is not registered in the DB (i.e. there is no anti-virus software on the station).
🖥	The detected station is not registered in the DB (the station is connected to another **Server**).
🖥	The detected station is registered in the DB, bus it is not active and the port is closed.

You can also unfold catalog items corresponding to computers with the 🖥 or 🖥 icon, and check which program components are installed there.

To open the component settings window, click the 🔷 station component icon.

5. Select an unprotected computer (or several unprotected computers by pressing CTRL or SHIFT buttons) in the **Network scanner** window.

6. Select **Install Dr.Web Enterprise Agent** in the toolbar.

7. A window for a remote installation task will be opened.

8. In the **Dr.Web Network Installer** section you can set up the installation parameters of the **Agent** software.

9. In the **Computer names** field, the target computer IP addresses are specified.

◆ For installation on stations, found via the **Network Scanner**, the address of station or several stations, on which installation will be performed, already specified in the **Computer names** field.

◆ Otherwise, specify address of a station or several stations. When the **Agent** software is installed on several computers at the same time, you can specify several IP addresses or computer names:

• with a hyphen (for example, `10.4.0.1–10.4.0.10`)

• separated by a comma with a whitespace (for example, `10.4.0.1–10.4.0.10,10.4.0.35–10.4.0.90`)

• with a network prefix (for example, `10.4.0.0/24).`

> Besides, you can enter computer domain names instead of the IP addresses.
>
> If installation is implemented by computer name, which contains hyphen '-', such name must be included into quotes, e.g., "123-456".

10. By default the **Agent** software is installed to `C:\Program Files\DrWeb Enterprise Suite`. If necessary, specify another location in the **Install path** field.

11. By default in the **Server** field the IP address or the DNS name of **Enterprise Server** to which the **Dr.Web Control Center** is connected are given. If necessary, specify the **Server** address, from which the anti-virus software will be installed.

12. 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.

> The paths to the public key and the executable file must be specified in the network address format.

13. If necessary, type the network installer command line parameters in the **Additional parameters** field (read more in Appendix H4. Network Installer). In the **Log level** field specify

the level of detail.

14. In the **Log level** drop-down list, select the level of details for the installation log.

15. In the **Installation timeout (sec.)** field, specify maximum time to wait for the **Agent** installation to complete in seconds. Valid values: 1-600. 180 seconds is set by default. If network channel capacity between the **Server** and the **Agent** is low, it is recommended to enlarge the value of this option.

16. If necessary, set the **Register installation in Add/Remove Program database** flag.

17. In the **Install** section, select the anti-virus components to install on the station. Also specify the parameters of traffic compression during installation.

18. In the **Authorization** section, specify the parameters of authorization for access to the remote computer.

    You can set several administrator accounts. To do this:

    a) Click   **+**   to add specified account from the **Authorization** section to the list of accounts, which are used during installation.

    b) To add one more account, specify authorization parameters repeatedly and click **+**. Similarly, for each new record.

    c) In the list of used accounts, you can disable of enable accounts disabled earlier. To do this, clear or set flags for corresponding accounts.

    During **Agent** installation, the first account in the list is used at first. If installation under this account failed, the next account in the list is used, and etc.

19. Having set up all the necessary parameters of the **Dr.Web Network Installer** section, click **Next**.

20. On the **Dr.Web Enterprise Agent settings** tab, you can specify the following parameters:

◆ In the **Authorization** section, you can specify the parameters of authorization of the **Agent** at the **Server**. If the **Set authorization** flag is cleared and the corresponding fields are not set, the authorization parameters will be set automatically.

◆ In the **Encryption** and **Compression** sections, you can enable using encryption and compression of traffic between the **Agent** and the **Server**.

In the sequel, you can change this options in the settings of the Enterprise Agent and in the station settings.

21. After all necessary parameters have been specified, click **Install**.

---

i   For launching the installation of the anti-virus software, the build-in service is used.

---

22. **Enterprise Agent** will be installed on the selected workstations. After the workstation has been approved at the **Server** (if it is required by **Enterprise Server** settings, see also Establishing a Simple Anti-Virus Network), the anti-virus components will be automatically installed.

23. Restart the computer on **Agent** request.

Using the Network Installation Tool

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

1. Select the **Administration** item in the main menu. Then, in the opened window select the **Network installation** item in the control menu.

2. Further steps are similar to **8-23** above.

Installation for Accounts with Specified ID

To perform remote Agent installation for accounts with selected ID:

   a) When creating a new station account:

   1. Add a new station account or several station accounts (see Creation of a New User Account).

   2. Right after adding account, in the right part of a main window, the **Install Dr.Web Enterprise Agent** pain opens. Click **OK**.

   3. The **Network Scanner** window opens.

   4. Further steps are similar to **2-23** above.

   5. After installation is complete, check if icons of corresponding stations are changed in the hierarchical list.

   b) When using existing station account:

   1. In the hierarchical list of antivirus network, select a new station or group of stations, for which **Agents** are not installed, or the **New** group (for installation on all new accounts).

   2. Click 🟢 **Install Dr.Web Enterprise Agent** on the toolbar.

   3. The **Network Scanner** window opens.

   4. Further steps are similar to **2-23** above.

   5. After installation is complete, check if icons of corresponding stations are changed in the hierarchical list.

ℹ️ **Agent** installation on stations with selected ID is also available of group administrators.

⚠️ See the Remote Installation Trouble Shooting section, if an error has occurred.

2.4.2. Installing Dr.Web Enterprise Agent Software via 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.

> The **Agent** installation via Active Directory service is also available when using Distributed File System (see the Using DFS During Installation the Agent via the Active Directory section).

Dr.Web Enterprise Agent Installation

To install the Agent using the Active Directory:

1. Download a copy of **Enterprise Agent** installer for networks with **Active Directory** at http://download.drweb.com/esuite/.
2. Install **Enterprise 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)**.

> If you upgrade the **Server**, you do not have to upgrade **Enterprise Agent** installer for networks with Active Directory. After upgrading the **Server** software, the **Agents** and the anti-virus software will be upgraded at the stations automatically.

(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 <package_name>.msi /qn [<parameters>]
```

The `/a` parameter launches installation of the administrative package.

Package name

The name of the installation package for the **Agent** through Active Directory usually has the following format:

```
drweb-es-agent-<version>-<release_date>-windows-nt-
<capacity>.msi.
```

Parameters:

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

- ◆ `ESSERVERADDRESS=<DNS_name>` - set the address of **Enterprise Server** to which the **Agent** is to be connected. For the possible formats see Appendix E3.
- ◆ `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` – the network folder for the **Agent** image (modified installation package), which will be select via the Group Policy Object Editor for the selected installation. This folder must have read and write access. The path should be given in the network addresses format even if the folder is a locally accessible resource; the folder should be accessible from the target stations.

> ⚠️ Before administrative installation the destination directory for the **Agent** image (see the `TARGETDIR` parameter) should not contain the **Enterprise Agent** Installer for networks with **Active Directory** (`<package_name>.msi`).

> After deployment the administrative package, in the
> *<destination_dir>*\Program Files\DrWeb
> Enterprise Suite directory only the README.txt
> file must resides.

Examples:

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

```
msiexec /a ESS_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.

Next on a local network server, where Active Directory administrative
tools are installed, appoint installation of the package (see procedure
below).

(B) To Set All Necessary Installation Parameters in the Graphic Mode

> ⚠ Before administrative installation, make sure that the
> destination directory for the **Agent** image does not contain
> the **Enterprise Agent** Installer for networks with **Active
> Directory** *(<package_name>*.msi).

> **i**   After deployment the administrative package, in the
> *<destination_dir>*\Program Files\DrWeb
> Enterprise Suite directory only the README.txt
> file must resides.

1. Issue the command

   msiexec /a *<path>**<package_name>*.msi

2. An **InstallShield Wizard** window with information on the program selected for installation will be opened. Click **Next**.

> **i**   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 **Enterprise Server** (see Appendix E3). Specify the location of the public key file of the **Server** (drwcsd.pub). Click **Next**.

4. 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**.

5. After installation is finished, the settings window displays which helps you configure installation of the package on network workstations.

Installation of the Package on Selected Workstations

1. In **Control Panel** (or in the **Start** menu for Windows 2003/2008 Server OS, in the **Start** → **Programs** menu for the Windows 2000 Server OS), select **Administrative Tools** → **Active Directory Users and Computers** (when you install **Agent** in the graphic mode, this window displays automatically).

2. In the domain containing the computers on which **Enterprise Agents** are to be installed, create an organizational unit (hereinafter OU), name it, for example, **ESS**. To do this, in the domain context menu, select **New → Organizational unit**.

   In the opened window, type the new unit name and click **OK**. Include the computers, on which the **Agent** is to be installed, into this unit.

3. Open the group policy editor. To do this:

   a) for Windows 2000/2003 Server OS: on the OU context menu, select **Properties**. In the opened window go to the **Group Policy** tab.

   b) for Windows 2008 Server OS: select **Start → Administrative tools → Group Policy management.**

4. For the created OU, set the group policy. To do this:

   a) for Windows 2000/2003 Server OS: click **Add** and create an element named **ESS** policy. Double-click it.

   b) for Windows 2008 Server OS: on the OU context menu, select **Create a GPO in this domain, and Link it here**. In the opened window, specify the name of the new group policy object and click **OK**. In the new group policy context menu, select **Edit**.

5. In the **Group Policy Object Editor** window, specify the settings for the group policy created on step 4. To do this:

   a) for Windows 2000/2003 Server OS: in the hierarchical tree, select **Computer Configuration → Software Settings → Software Installations**.

   b) for Windows 2008 Server OS: in the hierarchical tree, select **Computer Configuration → Policies → Software Settings → Software Installations**.

6. On the context menu of **Software Installations**, select **New → Package**.

7. Specify the **Agent** installation package. To do this, specify the address of the network shared resource which contains the **Agent** image you created during the administrative installation. 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 be opened. 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 be opened.

   ◆ Set the **Ignore language when deploying this package** flag.

   ◆ If you plan to install **Enterprise Agent** via the customize msi package on 64-bit OS, set the **Make this 32-bit x86 application available to Win64 machines** flag.

12. Click **OK** twice.

13. **Enterprise Agent** will be installed on selected computers at their next registration in the domain.

Policies Assignment in Consideration of Previous Agent Installations

When you assign an Active Directory policy to install the **Agent**, you should consider a possibility, that the **Agent** is already installed at the station. There are three possible options:

1. **The Enterprise Agent is not installed at the station**.

   After policies assignment, the **Agent** will be installed by general rules.

2. **The Enterprise Agent is already installed at the station without using the Active Directory service**.

   After Active Directory policy assignment, installed **Agent** will remain at the station.

In this case, the **Agent** is installed at the station, but for the Active Directory service **Agent** is not installed. So, after every station startup, attempt of unsuccessful **Agent** installation will be repeated.

To install the **Agent** via the Active Directory, you must uninstall the **Agent** manually (or via the **Control Center**) and assign the Active Directory policy for this station repeatedly.

3. **The Enterprise Agent is already installed at the station via the Active Directory**.

   After assignment the policy:

   a) If the rights for deleting the **Agent** are permitted for this station, the **Agent** will be deleted. To install the Agent via the Active Directory, you must assign the Active Directory policies for this station repeatedly.

   In this case, you must assign policies for the **Agent** installation repeatedly, because after the first policies assignment, the **Agent** has been deleted from the station, but for the Active directory service the **Agent** is still installed.

   b) If the rights for deleting the **Agent** are prohibited for this station, assignment policies will not take any affect to the anti-virus software state at the station. For further actions, permit the rights for the Agent deletion (see the Setting Users Permissions section) and assign the Active Directory policies for this station repeatedly. Further actions are similar to the **a)** step.

   To assign the Active Directory policies repeatedly, you can use any convenient way.

2.5. Installing NAP Validator

Dr.Web NAP Validator checks health of anti-virus software on protected workstations. It is installed on the computer where a configured NAP server resides.

To install NAP Validator

1. Run the installation file. In the dialog window, select the language to use during install. Select **English** and click **Next**.
2. On the Welcome page of the **InstallShield Wizard**, click **Next**.
3. On the **License Agreement** page, read the agreement. To accept the agreement and proceed with the installation, select **I accept the terms of the license agreement** and click **Next**. To exit the wizard, click **Cancel**.
4. On the next page, specify **Enterprise Server** IP **Address** and **Port** and click **Next**.
5. Click **Install**. The installation begins.
6. When installation completes, click **Finish**.

After you install **Dr.Web NAP Validator**, add **Enterprise Server** to the trusted NAP servers group.

To add Dr.Web Enterprise Server to the trusted NAP servers group

1. To open NAP server configuration component, run the `nps.msc` command.
2. In the **Remediation Servers Group** section, click **Add**.
3. In the dialog window, enter the name for the new remedial server and the **Enterprise Server** IP address.
4. Click **OK** to save changes.

2.6. Installing Proxy Server

One or several **Proxy servers** can be included into the anti-virus network.

When choosing a computer where the **Proxy server** should be installed, consider that it should be accessible from all networks and segments which require data redirection between them.

> **i** To install the **Proxy server**, you must have administrator rights on this computer.

Below is described the installation of the **Proxy server** for Windows OS. The set and the order of steps may somewhat differ depending on the distribution file version.

To install the Proxy Server on a computer operated by Windows OS

1. Run the distribution file. A window of **Installation Wizard** with information about the program to be installed will be opened. Click **Next**.

2. A window with the text of the license agreement will be opened. 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**.

3. A window for changing the default installation folder (`C:\Program Files\DrWeb Enterprise Proxy`) will be opened. If necessary, click **Change** and specify the installation folder. Click **Next**.

4. A window for setting **Proxy server** parameters will be opened:

    ◆ In the **Listen to** field, specify an IP address, which will be "listened" by the **Proxy server**. By default, it is `any` (`0.0.0.0`) value, which means "listen" to all interfaces.

◆ In the **Port** field, specify a port, which the **Proxy server** listens. By default, it is **2193** port or **23** port for NetBIOS protocol.

◆ In the **Protocol** drop-down list, select a type of the protocol for accepting incoming connections by the **Proxy server**.

◆ Set the **Enable discovery** flag to enable the **Server** imitation mode. This mode allows **Network scanner** to detect the **Proxy server** as an **Enterprise Server**.

◆ In the **Multicast group**, specify an IP address of a multicast group, in which the **Proxy server** is included. Specified interface will be listened by the **Proxy server** for interaction with **Network installers** during active **Enterprise Servers** searching.

◆ In the **Redirect to** section, specify an address or the list of addresses of **Enterprise Servers**, where the connection established by the **Proxy server** should be redirected to.

After you specify **Proxy server** settings, click **Next**.

5. A window with information, that the **Proxy server** is ready to install, will be opened. Click **Install**.

6. Once the installation is complete, click **Finish**.

After installation you can change operation parameters of the **Proxy server**. For this you can use the drwcsd-proxy.xml configuration file which is located in the **Proxy server** installation folder. Parameters of the configuration file are given in <u>Appendix G4</u>.

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

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 Linux-based 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>*

After that you need to move all unpacked folders into the root directory.

In the course of the installation for **FreeBSD** OS an `rc` script `/usr/local/etc/rc.d/0.dwcp-proxy.sh` will be created.

◆ To manually stop the **Proxy server**, use the command:

`/usr/local/etc/rc.d/0.dwcp-proxy.sh`
`stop`

◆ To manually start the **Proxy server**, use the command:

`/usr/local/etc/rc.d/0.dwcp-proxy.sh`
`start`

During the installation for **Linux** OS and **Solaris** OS, an `init` script (`/etc/init.d/dwcp-proxy`) for the launching and termination of the **Server** will be created.

2.7. Removing Dr.Web Enterprise Security Suite Components

2.7.1. Removing Dr.Web ESS Software for Windows® OS

Uninstalling Dr.Web Enterprise Server

To remove the **Server** or the **Dr.Web Browser-Plugin** software, run the installation file of the corresponding product of currently installed version. The installation program will automatically detect the software product and offer to remove it. To remove software, click **Remove**.

The **Server** and **Dr.Web Browser-Plugin** software can also be removed using standard Windows OS tools via the **Add or Remove Programs** element in **Control Panel**.

Uninstalling Dr.Web Enterprise Agent and Anti-Virus Package Remotely

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

If you uninstall the **Agent** and anti-virus package via the **Control Center**, the **Quarantine** will not be deleted from the station.

To uninstall the anti-virus software from a workstation (for Windows OS only):

1. Select the **Network** item in the main menu of the **Dr.Web Control Center**.

2. In the opened window select the necessary group or certain anti-virus stations.

3. Click ⭐ **General** → 🗙 **Uninstall Dr.Web Agent** in the toolbar of the anti-virus network catalog.

4. The **Agent** software and the anti-virus package will be removed from the workstations selected.

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

Uninstalling Dr.Web Enterprise Agent and Anti-Virus Package Locally

> ⚠️ To remove the **Agent** and the anti-virus package locally, this option must be allowed at the **Server** in the **Rights** section.

You can remove the station anti-virus software (**Agent** and anti-virus package):

1. By means of standard Windows OS services.
2. By using the **Agent** installer.

> ℹ️ If the **Agent** and anti-virus package are uninstalled via the standard Windows OS services or via the **Agent** installer, user will be prompt for **Quarantine** deleting.

Removing by Means of Standard Windows OS Services

> This removing method will be available only if you installed the **Agent** by using the graphical installer and set the **Register Agent in system list of installed software** flag.
>
> If the **Agent** installed in the background mode of the installer, the removing of the anti-virus software with the standard Windows OS services will be available only if the –regagent switch was used for installation.

To remove the **Agent** and the anti-virus package, use standard Windows OS tools: the **Add or Remove Programs** element in **Control Panel** (see the **Agent** **User Manual** for details).

Removing by Using the Agent Installer

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

Example:
```
drwinst –uninstall –interactive
```

2.7.2. Removing Dr.Web Enterprise Agent Software through Active Directory

1. In **Control Panel**, select **Administrative Tools → Active Directory users and computers**.
2. Right-click your **ESS** organizational unit in the domain. On the

context menu, select **Properties**. An **ESS Properties** window will be opened.

3. Go to the **Group Policy** tab. Select **ESS policies**. Double-click the item. A **Group Policy Object Editor** window will be opened.

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. **Enterprise Agent** will be removed from the stations at the next registration in the domain.

2.7.3. Removing Dr.Web Enterprise Server Software for UNIX® System-Based OS

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

To remove Dr.Web Enterprise Server:

1. Execute the following command:

For the Server under		Command
FreeBSD OS		`pkg_delete drweb-esuite`
Solaris OS		1. Stop the **Server**: `/etc/init.d/drwcsd stop` 2. Run the command: `pkgrm DWEBesuit`
Linux OS	Debian Ubuntu	`dpkg –r drweb-esuite`
	rpm package	`rpm –e drweb-esuite`
	generic package	`/opt/drwcs/bin/drweb-esuite-`

For the Server under			Command
			`uninstall.sh`

> ⓘ 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**).

Enterprise Server software will be removed.

> ⓘ On **FreeBSD** OS and **Linux** 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 **Linux** 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.

To remove Dr.Web Browser-Plugin:

Execute the following command:

- ◆ for **deb** packages:
    ```
    dpkg -P drweb-esuite-plugins
    ```
- ◆ for **rpm** packages:
    ```
    rpm -e drweb-esuite-plugins
    ```
- ◆ for other systems (**tar.bz2** and **tar.gz** packages):
    ```
    rm -f <plugins_directory>/libnp*.so
    ```

For exmaple, for Mozilla Firefox browser:
```
rm -f /usr/lib/mozilla/plugins/libnp*.so
```

2.7.4. Removing Proxy Server

Uninstalling Proxy Server for Windows OS

During **Proxy server** uninstallation, the `drwcsd-proxy.xml` configuration file is deleted. If necessary, save configuration file manually before **Proxy server** uninstallation.

The **Proxy server** software uninstallation is performed via the standard Windows OS tools at **Control Panel → Add or Remove Programs** (**Programs and components** for Windows 2008 OS).

Uninstalling Proxy Server for UNIX System-Based OS

To uninstall the Proxy server, perform the following:

For Proxy server under		Command
FreeBSD OS		`pkg_delete drweb-esuite-proxy`
Solaris OS		`pkgrm DWEBespxy`
Linux OS	deb package	`dpkg -P drweb-esuite-proxy`
	rpm package	`rpm -e drweb-esuite-proxy`
	generic package	Delete files from the **Proxy server** installation folder manually.

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

3.1. Dr.Web Enterprise Server

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

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

Enterprise Server is a memory-resident component. **Enterprise Server** software is developed for various OS (see Appendix A. The Complete List of Supported OS Versions).

Basic Functions

The Dr.Web Enterprise Server performs the following tasks:

◆ initializes of installation of 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.

Collecting Information on Anti-Virus Network

Communicating with **Enterprise Agents**, **Enterprise 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 200-300 computers) an internal database can be used. In larger networks it is recommended to use an external database.

> ⚠️ An internal DB can be used, if at most 200-300 stations are connected to the **Server**. If the hardware configuration of the computer with **Enterprise Server** and the load level of other executing tasks are permissible, up to 1000 stations can be connected.
>
> Otherwise, you must use an external DB.
>
> If you use an external DB and more than 10 000 stations are connected to the **Server**, it is recommended to perform the following minimal requirements:
>
> ◆ 3 GHz processor CPU,
>
> ◆ RAM at least 4 Gb for **Enterprise Server** and at least 8 Gb for the DB server,
>
> ◆ UNIX system-based OS.

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.

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

Interface

Enterprise Server as it is has no interface. Basic instructions necessary to manage the **Server** are listed in the Server control directory.

As a rule, **Enterprise Server** can be managed through the **Dr.Web Control Center** which acts as an interface for the **Server**.

Start and Stop the Dr.Web Enterprise Server

By default, the **Enterprise Server** automatically starts after installation and every time after restarting the operating system.

Also you can start or start, restart or stop the **Enterprise Server** by one of the following ways:

For UNIX system-based OS

- ◆ Using the corresponding console command (see also Appendix H5. Dr.Web Enterprise Server):
  - ○ Start:
    - for FreeBSD OS:
      ```
      # /usr/local/etc/rc.d/drwcsd.sh start
      ```
    - for Linux OS and Solaris OS:
      ```
      # /etc/init.d/drwcsd start
      ```
  - ○ Restart:
    - for FreeBSD OS:
      ```
      # /usr/local/etc/rc.d/drwcsd.sh restart
      ```
    - for Linux OS and Solaris OS:
      ```
      # /etc/init.d/drwcsd restart
      ```

 ○ Stop:

   • for FreeBSD OS:
    `# /usr/local/etc/rc.d/drwcsd.sh stop`

   • For Linux OS and Solaris OS:
    `# /etc/init.d/drwcsd stop`

 ◆ Stop and restart via the **Control Center**:

   • In the **Administration** section, use buttons: to restart, to stop (is absent under Solaris OS).

For Windows OS

 ◆ General case:

   • Using the corresponding command, located in the **Start → Programs → Dr.Web Enterprise Server** menu.

   • Via the services management tools in the **Administrative Tools** section at the **Control Panel** of Windows OS.

 ◆ Stop and restart via the **Control Center**:

   • In the **Administration** section, use buttons: to restart, to stop.

 ◆ Using the console commands run from the `bin` subfolder of the **Server** installation folder (see also Appendix H5. Dr.Web Enterprise Server):

   • `drwcsd start` — start the **Server**.

   • `drwcsd restart` — total restart of the **Server** service.

   • `drwcsd stop` — normal shutdown of the **Server**.

3.2. Dr.Web Enterprise Agent

Principle of Operation

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

The packages operate by **Enterprise Agents**, which is installed and constantly resided in the memory of protected workstations. They maintain connection to **Enterprise Server**, thus enabling administrators to centralized configure anti-virus packages on workstations from the **Dr.Web Control Center**, schedule anti-virus checks, see the statistics of anti-virus components operation and other information, start and stop remotely anti-virus scanning, etc.

Enterprise Servers opportunely download updates and distribute them to the **Agents** connected to them. Thus due to **Enterprise 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, **Enterprise 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.

Basic Functions

The Dr.Web Enterprise Agent is designed to perform the following:

- ◆ installs, updates and sets up the anti-virus package, starts scannings, and performs other tasks given by the **Enterprise Server**;
- ◆ allows to call for execution the **Dr.Web** anti-virus package files through a special interface;
- ◆ sends the results of tasks execution to the **Enterprise Server**;
- ◆ sends notifications of predefined events in the operation of the anti-virus package to the **Enterprise Server**.

Every **Enterprise Agent** is connected to **Enterprise Server** and is included in one or several groups registered on this **Server** (for more, see p. System and User Groups). The **Agent** and **Enterprise Server**

communicate through the protocol used in the local network (TCP/IP, IPX or NetBIOS).

> Hereinafter a computer on which **Enterprise 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.

Management Interface under Windows OS

When run in the Windows OS environment, **Enterprise Agent** displays an icon in the Taskbar.

The icon visual representation depending on components state, is listed in the .

Table 3-1. The icon visual representation

Icon	Description	State
	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, or components **SelfPROtect** or **Spider Guard** are disabled.
→	The background of the icon changes color from green to red.	An error occurred during updating of the package components.
	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).

Some administrative functions over the anti-virus workstation are accessible through the context menu of this icon, which is shown in Figure 3-1.

Language ▶
Resync now ▶
Settings ▶
Run mode ▶
Schedule ▶
Mobile mode ▶
Statistics
Status
Scanner
Quarantine
Firewall log
Firewall settings …
Office Control settings…
SpIDer Gate settings…
SpIDer Guard Settings …
SpIDer Mail settings…
✔ Firewall
✔ Network access
✔ Outlook plug-in
Prevent suspicious actions ▶
✔ Self-protection
✔ SpIDer Gate
✔ SpIDer Guard
✔ SpIDer Mail
About
Help
Doctor Web, Ltd.
Prepare logs
Support
Exit

Figure 3-1. The context menu of Enterprise 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 **Enterprise Agent** help.
>
> About the settings of **Enterprise Agent** read p. Editing the Parameters of the Dr.Web Enterprise Agent.

Start and Stop the Dr.Web Enterprise Agent under Windows OS

> The **Exit** command in the **Agent** context menu only stops the Agent GUI (see the Management Interface under Windows OS section) and removes the icon from the notification area of the Taskbar. The **Agent** will remain running.

To terminate the program itself, execute the following command:

```
net stop drwagntd
```

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, execute the following command:

```
net start drwagntd
```

3.3. Dr.Web Control Center

To manage the anti-virus network and set up the **Server**, the in-built **Dr.Web Control Center** serves.

Connecting to the Dr.Web Enterprise Server

> ⚠️ For correct functioning of the **Dr.Web Control Center** under Microsoft Internet Explorer browser, you should add the **Dr.Web Control Center** address to the list of trusted sites in the Web browser settings: **Tools → Internet Options → Security → Trusted Sites**.
>
> For correct functioning of the **Dr.Web Control Center** under Chrome browser, you should turn on cookies.

From any computer with network access to the **Server**, **Dr.Web Control Center** is available at the following address:

`http://<Server_Address>:9080`

or

`https://<Server_Address>:9081`

where *<Server_Address>* is the IP address or domain name for the computer on which **Enterprise Server** is installed.

> ℹ️ Ports numbers for http connection and for protected https connection are differ: `9080` and `9081` correspondingly.

In the authorization dialog window specify the user name and password of the administrator (by default, administrator name is **admin** and the password is the same, as was specified during **Server** installation).

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 **Dr.Web Control Center**.

> Some browsers, e.g. **FireFox 3** and later report errors
> when connecting through https and refuse connection to
> the **Dr.Web Control Center**. To solve this problem, add
> the **Dr.Web Control Center** to the list of exceptions by
> clicking **Add site** in the warning message. This allows
> connection to the **Dr.Web Control Center**.

Dr.Web Control Center Interface

The **Dr.Web Control Center** window (see figure 3-2) is divided in
header and *working area*.

The *header* contains:

- the **Dr.Web Enterprise Security Suite** logo, which opens the
  main window of the **Dr.Web Control Center**, if you click it
  (the same as when you select the **Network** item in the main
  menu),
- main menu,
- the name of the current administrator logged into the **Dr.Web
  Control Center**,
- **Logout** - close the current **Dr.Web Control Center** session.

> If automatic authorization in **Control Center** is enabled,
> after clicking **Logout**, information about administrator's
> login and password is deleted.
>
> At next logon in the **Control Center**, it is necessary to
> repeat standard authorization procedure with specifying
> login and password. If automatic authorization is enabled,
> specified login and password are saved for the current web
> browser and authorization in **Control Center** become
> automatic (without login and password confirmation) till
> next **Logout** clicking.

The working area is used to perform all the main functions of the **Dr.Web Control Center**. It consists of two or three panels depending on the actions which are being performed. Items in the panels are nested from left to right:

◆ the *control menu* is always located in the left part of the working area,

◆ depending on the selected item, one or two additional panels are displayed. In the latter case, the rightmost panel contains the settings of elements from the central panel.

The interface language must be set individually for each administrator account (see p.).

Main menu

The main menu consists of the following items:

◆ Administration,
◆ Network,
◆ Preferences,
◆ Neighborhood,
◆ Help,
◆ Search panel.

Figure 3-2. The Dr.Web Control Center window.
Click the main menu option to see the description

Search Panel

The search panel located in the top right part of the **Dr.Web Control Center** and used to simplify searching for elements. It can find both groups and separate workstations according to specified parameters.

To find a workstation or group of workstations:

1. Select the search criterion in the drop-down list of the search panel:

   ◆ **Station -** to search stations by name,

   ◆ **Group -** to search groups by name,

   ◆ **ID -** to search stations and groups by identifier,

   ◆ **Description -** to search stations and groups by their description,

   ◆ **IP address -** to search stations by their IP address.

2. Enter a parameter value to search. You can search values by specifying:

◆ specific string for full match with search value,

◆ a mask for search string: the * and ? symbols are allowed.

3. Press ENTER to start the search.

4. The search results contain a hierarchical list of elements according the search parameters.

   ◆ If you searched for a workstation, occurrence of the workstation in groups will be displayed.

   ◆ If no elements are found, the message **Nothing found** will be displayed in the empty hierarchical list.

You can also use the **Advanced search** option.

To perform an advanced search:

1. Click the 🔍 button in the search panel.

2. Specify the following parameters on the **Search for Groups and Stations** panel:

   ◆ **Station name** - specify keyword(s) which will be searched for in the names of workstations.

   ◆ **Group name** - specify keyword(s) which will be searched for in the names of groups.

   ◆ **ID -** specify keyword(s) which will be searched in the identifiers,

   ◆ **IP address** - specify keyword(s) which will be searched for in the IP addresses of workstations,

   ◆ **Description** - specify the description in compliance to which the element will be searched for.

   You can specify parameters for one, several or all advanced search fields.

   If you specify parameters in several fields, the program searches for elements, which comply with any of them (integration of search values according to the *OR* principle).

3. After you specify all the necessary parameters, click **Search**.

4. All the found elements or the message "**Nothing found**" will be displayed in the hierarchical list.

3.3.1. Administration

Select the **Administration** item in the main menu of the **Dr.Web Control Center**. The control menu in the left part of the window is used to view and edit information in the opened window.

The control menu consists of the following items:

1. **Administration**
   - ◆ **Dr.Web Enterprise Server** — opens the panel which shows basic information about the **Server** and lets you restart or shutdown it via the 🔄 and ⏻ (is absent under Solaris OS) buttons in the top right part of the panel.
   - ◆ **Unapproved stations** — opens the panel with the list of unapproved workstations (see New Stations Approval Policy).
   - ◆ **License Manager** — helps you to manage the license key files of **Server** and **Agent** (see License Manager).
   - ◆ **Encryption keys** — allows to export (save locally) public and primary encryption keys.

2. **Tables**
   - ◆ **Audit log** — lets you view the log of events and changes carried out by the **Dr.Web Control Center**.
   - ◆ **Jobs execution log** — contains a list of **Server** tasks with completion marks and comments.
   - ◆ **Server statistics** — contains statistics of this **Server** operating.

3. **Configuration**
   - ◆ **Administrator accounts** — opens the panel for managing anti-virus network administrator accounts (see Management of Administrative Accounts).
   - ◆ **Repository state** — lets you check status of the repository: the date when repository components were last updates and their current status (see Checking the Repository State).

◆ **Authorization** — opens the panel to manage authentication methods of **Dr.Web Control Center** administrators (see Authentication of Administrators);

◆ **Configure repository** — opens the repository editor window (see Editing the Configuration of the Repository).

◆ **Configure Dr.Web Enterprise Server** — opens the panel with main settings of the **Server** (see Setting the Dr.Web Enterprise Server Configuration).

◆ **Dr.Web Enterprise Server schedule** — opens the panel with **Server** task schedule settings (see Setting the Dr.Web Enterprise Server Schedule).

◆ **Edit templates** — opens the alert template editor window (see Setting Alerts).

4. **Installations**

◆ **Network Scanner** — lets you specify a list of networks, search for installed anti-virus software in networks to determine protection status of computers, and install anti-virus software (see Network Scanner).

◆ **Network installation** — lets you simplify installation of the **Agent** software on certain workstations (see Installing the Dr.Web Enterprise Agent Software through the Dr.Web Control Center).

3.3.2. Anti-Virus Network

Select the **Network** item in the main menu of the **Dr.Web Control Center**. The control menu in the left part of the window is used to view and edit information in the opened window.

Hierarchical list

In the middle part of the window there is a hierarchical list of the anti-virus network. The list (catalog) represents the tree structure of the anti-virus network elements. The nodes in this structure are groups and workstations within these groups.

You can perform the following through the hierarchical list elements:

◆ Left-click the the name of the corresponding element to open the control menu (left part of the window) of a group or workstation.

◆ Left-click the icon of the group to see the contents of a group.

> **i** To select several elements of the hierarchical list, press and hold CTRL or SHIFT during selection.

The appearance of the icon depends on the type and status of this element (see table 3-2).

Table 3-2. Icons of elements in the hierarchical list

Icon	Description	Meaning
	Groups	
	yellow folder	Groups always shown on the hierarchical list.
	white folder	If groups marked with this icon are empty, their showing on the hierarchical list may be disabled.
	Workstations	
	green icon	Available workstations with installed anti-virus software.
	gray icon	The station is unavailable.
	crossed computer icon	Anti-virus software on the station is uninstalled.

> **i** If station or group has a personal settings (or group includes stations with personal settings), this group or station has a ● sign over its icon in the hierarchical list. E.g., if an available workstation with installed anti-virus software has a personal settings, its icon looks as follows: ⬚.

To display icons with personal settings, select the ▦ **Tree settings** item on the toolbar and set the **Display personal settings** flag.

Management of the anti-virus network catalog elements is carried out via the toolbar of the hierarchical list.

Toolbar

The toolbar of the hierarchical list contains the following elements:

⭐ **General**. Manage the general parameters of the hierarchical list. Select the corresponding item in the drop-down list:

❌ **Remove selected objects**. Remove an item(s) from the hierarchical list. Select the item(s) in the list and click **Remove selected objects**.

✏️ **Edit**. Opens settings of the station or group in the right pane of the **Dr.Web Control Center**.

▣ **Become primary**. Determine the selected group as primary for all workstations in it.

▣ Set **a primary group for the stations**. Assign a primary group for selected workstations. If a group is selected in the hierarchical list instead of workstations, the specified primary group will be assigned to all workstations from this group.

🌱 **Merge stations**. Join workstations under a single account in the hierarchical list. It can be used if a workstation had been registered under several accounts (see p. Merging Stations).

🗑️ **Remove personal settings**. Remove individual settings of selected objects. Settings of the parent group will be used. All workstations inside a group will also have their settings removed.

🔑 **Import key**. Set a key for workstation or group.

📧 **Send message**. Send notifications to users of workstations (see Sending Notifications to the Users).

Uninstall Dr.Web Agent. Remove the **Agents** and anti-virus software from the selected workstation(s) or group(s).

Install Dr.Web Enterprise Agent. Open the <u>Network scanner</u> for **Agent** installation to the selected stations. This option is enabled only if new approved stations or stations with deinstalled **Agent** are selected.

Restore deleted stations. Allows to restore stations deleted earlier (see also p. <u>Removing and Restoring Stations</u>). This option is active only if stations from the **Deleted** subgroup of the **Status** group are selected.

Add a station or a group. Add a new element of anti-virus network. Click the corresponding item in the drop-down menu:

Add station. Add a new station (see <u>Creation of a New User Account</u>).

Add group. Add a new group (see <u>Creating and Deleting Groups</u>).

Data Export. Save common data about workstations in the anti-virus network to a CSV, HTML or XML file. Select the file format in the drop-down menu.

Change group visibility settings. Change the appearance of groups in the list. Select one of the following in the drop-down list (the icon of the group will change, see <u>table 3-2</u>):

Hide group - means that the group will not be displayed in the hierarchical list.

Hide if empty - means that the group will not be displayed if the group is empty (does not contain any workstations).

Show - means that the group will always be displayed in the hierarchical list.

Managing components. Manage the components on the workstation. Select the necessary action in the drop-down menu:

Update all components. Update all installed components of the anti-virus, e.g., when the **Agent** has not been connected to

the **Server** for a long time, etc. (see also p. Manual Updating of the Dr.Web ESS Components).

Update failed components. Force synchronization of the components that failed to update.

Interrupt running components. Stop all active scans at the station. For more details about termination of scanning processes of a certain type, see Terminating Running Components by Type.

Scan. Scan stations in one of the modes, selected in the drop-down menu (see also Launching Scan on Station):

Dr.Web Scanner for Windows. Express scan. In this mode the following objects are scanned:

- main memory (RAM),
- boot sectors of all disks,
- autorun objects,
- root directory of the boot sector,
- root directory of the Windows OS installation disk,
- system directory of the Windows OS,
- `My documents` folder,
- temporary directory of the system,
- temporary directory of the user.

Dr.Web Scanner for Windows. Complete scan. In this mode all hard disks and removable disks (including the boot sectors) will be fully scanned.

Dr.Web Scanner for Windows. Custom scan. In this mode you will be able to choose files and folders to scan.

Dr.Web Enterprise Scanner for Windows. In this mode the scan will be done via the **Dr.Web Enterprise Scanner**.

Dr.Web Enterprise Scanner for Mac OS X. To scan stations, operate under Mac OS X family, with specified parameters.

Dr.Web Enterprise Scanner for Unix. To scan stations, operate under UNIX system-based OS, with specified parameters.

Tree settings. Adjust the appearance of the list:

◆ for groups:

- **All groups membership** – show a station in all groups it is a member of (only for groups under the white folder icon, see Table 3-2). If the flag is set, the station will be shown in all member groups. If the flag is cleared, the station will be shown only in the top white folder.

- **Show hidden groups** – show all groups included in the anti-virus network. If you clear the flag, all empty groups (not containing stations) will be hidden. It may be convenient to remove extra data, for example, when there are many empty groups.

◆ for stations:

- **Show station ID** – show unique identifiers of stations in the hierarchical list.

- **Show station name** – show names of stations in the hierarchical list, if such are given.

- **Show station address** – show IP-addresses of stations in the hierarchical list.

- **Show station server** – show names or addresses of **Enterprise Servers** to which stations are connected.

◆ for all elements:

- **Display personal settings** – enables/disables marker on icon of workstations and groups which shows whether individual settings are present.

- **Show descriptions** – enables/disables showing of groups and stations descriptions (the descriptions are set in the properties of an element).

Property Pane

The property pane shows the properties and settings of workstations.

To display the property pane

1. To display the attributes, click the ⭐ **General** → ✏ **Edit**
   element of the Toolbar.
2. A pane with properties of the station will be opened in the right
   pane of the **Dr.Web Control Center**. This panel contains the
   following settings: **General**, **Configuration**, **Groups**,
   Location. For more details about this settings see p.
   Management of Stations Configuration.

3.3.3. Preferences

Select the **Preferences** item in the main menu of **Dr.Web Control
Center**.

> ℹ All settings of this section are valid only for the current
> administrator account.

The control menu consists of the following items:

◆ **My account**.
◆ **Interface**.

My Account

Using this section, you can manage the current account of the
administrator of the anti-virus network (see also p. Management of
Administrative Accounts).

> ℹ Values of fields, marked by the * sign, must be obligatory
> specified.

You can edit the following settings, if necessary:

- ◆ Administrator account **Login** for **Dr.Web Control Center** access.
- ◆ Set the **ReadOnly** flag for administrator's rights limitation.
- ◆ **First name**, **Middle name** and **Last name** of the administrator.
- ◆ **Language** of the interface used by the administrator.
- ◆ **Date format**, which is used by this administrator during editing settings that contain dates. The following formats are available:
  - European: `DD-MM-YYYY HH:MM:SS`
  - American: `MM/DD/YYYY HH:MM:SS`
- ◆ Account **Description**.
- ◆ Set the **Can manage a limited number of groups** flag to set groups access for the groups administrator.
- ◆ To change the password, click 🔑 **New password** at the toolbar.

The following parameters are read only:

- ◆ Dates of creation and last modification of the account.
- ◆ **Status**. Displays the network address of the last connection under this account.

Click **Save** after you have changed all necessary parameters.

For read only accounts only the following fields can be edited:

- ◆ **Interface language**.
- ◆ **Description**.

Interface

Tree settings

Parameters of this section let you adjust the appearance of the list and they are similar to the settings, located in the ⬚ option of the toolbar of the **Network** item of the main menu.

- ◆ for groups:

  - **All groups membership** – show a station in all groups it is a member of (only for groups under the white folder icon, see <u>Table 3-2</u>). If the flag is set, the station will be shown in all member groups. If the flag is cleared, the station will be shown only in the top white folder.

  - **Show hidden groups** – show all groups included in the anti-virus network. If you clear the flag, all empty groups (not containing stations) will be hidden. It may be convenient to remove extra data, for example, when there are many empty groups.

- ◆ for stations:

  - **Show station ID** – show unique identifiers of stations in the hierarchical list.

  - **Show station name** – show names of stations in the hierarchical list, if such are given.

  - **Show station address** – show IP-addresses of stations in the hierarchical list.

  - **Show station server** – show names or addresses of **Enterprise Servers** to which stations are connected.

- ◆ for all elements:

  - **Display personal settings** – enables/disables marker on icon of workstations and groups which shows whether individual settings are present.

  - **Show descriptions** – enables/disables showing of groups and stations descriptions (the descriptions are set in the properties of an element).

Network scanner

> ⚠️ The **Network scanner** requires Dr.Web Browser-Plugin.

The settings of this section let you configure the default parameters of Network Scanner.

To launch the **Network scanner**, select **Administration** item in the main menu. In control menu (pane on the left), select **Network scanner**.

Specify the following parameters of **Network scanner**:

1. In the **Networks** field specify networks in the following format:
   - with a hyphen (for example, `10.4.0.1-10.4.0.10`)
   - separated by a comma with a whitespace

     (for example, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`)
   - with a network prefix (for example, `10.4.0.0/24`).
2. Change **Port** and **Timeout** parameters, if necessary.
3. Click **Save** to save these parameters as default. After that, when you use the Network scanner, this parameters will be set automatically.

Time Interval

In this section, you can specify settings of time interval to display statistics data (see Viewing the Statistics section):

- In the **Default interval for statistics data** drop-down list, specify the time interval, which is set as default for all sections of statistics data.

  When you open the page for the first time, statistics will be displayed for this time interval. You can change the time interval at statistics pages directly, if necessary.

◆ Set the **Save last interval for statistics data** flag, to save the interval, specified last time at statistics sections.

If the flag is set, when you open the page for the first time, statistics will be displayed for the last period, specified at the Web browser.

If the flag is cleared, when you open the page for the first time, statistics will be displayed for the period, specified in the **Default interval for statistics data** drop-down list.

Authorization

Set the **Automatic authorization** flag to allow automatic authorization for all **Control Centers** with the same administrator's login and password in the current browser.

After setting this flag, login and password specified by administrator at next logon in the **Control Center**, will be saved via the **Dr.Web Browser-Plugin**.

> ⚠ **Automatic authorization** option requires Dr.Web Browser-Plugin.

Further, for any **Control Center** in this web browser, authorization will be proceeded automatically, if the user with these login and password is registered at the **Server**. If the login and password do not much (e.g., such user is not registered or the user with this name has the different password), the standard **Dr.Web Control Center** authorization window will be given.

> ⓘ After clicking **Logout** in the header of the **Control Center**, information about administrator's login and password is deleted.

At next logon in the **Control Center**, it is necessary to repeat standard authorization procedure with specifying login and password. If automatic authorization is enabled, specified login and password are saved for the current web browser and authorization in **Control Center** become automatic (without login and password confirmation) till next **Logout** clicking.

3.3.4. Neighborhood

Select the **Neighborhood** item in the main menu of **Dr.Web Control Center**. The control menu in the left part of the window is used to select viewing information.

Administration

Administration section of the control menu contains the **Neighborhood** item, that serves to manage connections between **Servers** in a multi-server anti-virus network (for more details, see Peculiarities of a Network with Several Dr.Web Enterprise Servers).

The hierarchical list represents all of the **Enterprise Server**, connected to this **Server**.

Setting of new interserver connections is described in Setting Connections between Several Dr.Web Enterprise Servers.

Tables

The **Tables** section of the control menu contains information about the operation of the anti-virus network received from other **Servers** (see also Peculiarities of a Network with Several Dr.Web Enterprise Servers).

To view the summary tables with data from other **Servers**, select the corresponding item in the **Tables** section.

3.3.5. Help

Select the **Help** item in the main menu of the **Dr.Web Control Center**.

The control menu in the left part of the window contains the following elements:

1. **General**

   ◆ **Forum** - opens official forums of **Doctor Web** company.

   ◆ **Ask for support** - opens the web page of the **Doctor Web** technical support.

   ◆ **Send a virus** - opens a web form for sending a virus to the **Dr.Web Virus Laboratory**.

   ◆ **Report a Parental Control error** - opens a web form for sending a message about false alarm or detection failure in **Parental control** module.

2. **Documentation**

   ◆ **Administrator manual** - opens administrator documentation in HTML format.

   ◆ **User manual** - opens user documentation in HTML format.

   ◆ **XML Web API** - opens administrator documentation on XML Web API (see also Appendix N. Integration of XML Web API and Dr.Web Enterprise Security Suite) in HTML format.

   ◆ **Release notes** - opens release notes for **Dr.Web Enterprise Security Suite** of installed version.

3.4. Dr.Web Control Center Components

3.4.1. Network Scanner

Enterprise Server contains the **Network Scanner** component.

> ⚠️ It is not recommended to launch the **Network Scanner** under Windows 2000 and earlier operating systems due to possible insufficiencies of network review.
>
> The functioning of the **Network Scanner** is guarantied under UNIX system-based operating systems and Windows XP or later Microsoft Windows operating systems.
>
> The **Network scanner** requires Dr.Web Browser-Plugin.

Network Scanner provides the following functions:

- ◆ Scan (browse) the network for workstations.
- ◆ Detect **Enterprise Agents** on stations.
- ◆ Install **Enterprise Agent** on the detected stations as instructed by the administrator. **Enterprise Agent** installation is described in detail in p. Installing the Dr.Web Enterprise Agent Software through the Dr.Web Control Center.

To scan (browse) the network

1. Open the **Network Scanner** window: select the **Administration** item in the main menu of the **Dr.Web Control Center** and select **Network Scanner** item in the control menu.
2. If necessary, set the **Quick scan** flag for express scanning.
3. In the **Networks** field specify networks in the following format:
   - ◆ with a hyphen (for example, `10.4.0.1–10.4.0.10`)
   - ◆ separated by a comma with a whitespace (for example, `10.4.0.1–10.4.0.10,` `10.4.0.35–10.4.0.90`)

◆ with a network prefix (for example, `10.4.0.0/24`).

4. Specify the port to connect with the **Agent**.

5. If necessary, change the value of timeout in seconds, which defines time limit for receiving an answer from inquired stations.

6. Set the **Show the station name** flag to display either IP address and DNS name of found network stations.

   If a station is not registered at DNS server, only its IP address displays.

7. Set the **Correlate with stations list from database** flag to enable synchronization of **Network Scanner** search results with the stations list stored at the **Server** DB. If the flag is set, the list of found network stations contains stations from the **Server** DB list that are not found by the **Network Scanner** during current search, e.g. if a firewall installed at stations blocks the transfer of packets needed to establish a TCP connection.

   During synchronization of **Network Scanner** search results with **Server** DB data, the **Server** DB data has priority, i.e. if station statuses from search results and from DB are differ, the status from DB is set.

8. Click the **Scan** button to launch network scanning.

9. The catalog (hierarchical list) of computers demonstrating where the **Dr.Web ESS** anti-virus software is installed will be loaded into this window.

   Unfold the catalog elements corresponding to workgroups (domains). All elements of the catalog corresponding to workgroups and individual stations are marked with different icons the meaning of which is given below.

Table 3-3. Icons of the Network scanner

Icon	Meaning
	Workgroups
⚠	The work groups containing inter alia computers on which the **Dr.Web ESS** anti-virus software can be installed.

Icon	Meaning
	Other groups containing protected or unavailable by network computers.
Workstations	
	The detected station is registered in the DB and active (i.e. the workstation with installed anti-virus software).
	The detected station is registered in the DB as deleted (i.e. the workstation is listed in the table of deleted stations).
	The detected station is not registered in the DB (i.e. there is no anti-virus software on the station).
	The detected station is not registered in the DB (the station is connected to another **Server**).
	The detected station is registered in the DB, bus it is not active and the port is closed.

You can also unfold catalog items corresponding to computers with the or icon, and check which program components are installed there.

Click the icon of component at the station, connected to this **Server**, to open component settings window.

Interaction with Dr.Web Enterprise Agents

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

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

Enterprise Agents 4.44 and older installed on protected stations process respective calls of **Network Scanner** received at a certain port. By default port udp/2193 is using, but also port udp/2372 is supported for compatibility with older versions. 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/2193`, the **Agent** will not be
> detected and consequently **Network Scanner** considers
> that there is no **Agent** installed on the station.

Quick Scan

If the **Quick scan** option is enabled, the following actions will be
performed:

1. Ping requests are sent to network computers.
2. The parallel poll for **Agents** detection is performed only for
   computers which has answered to ping requests.
3. **Agents** detection procedure is implemented according to
   general rules.

> ℹ️ Ping requests can be blocked because of network policies
> (e.g. by firewall settings).
>
> **For example:**
>
> If in Windows Vista and later OS network settings the
> **Public location** options is set, OS will block all ping
> requests.

During regular scanning, ping requests are not sent and all stations in
the network are sequentially scanned to detect **Agents**. This method
can be used as an addition to quick scan, if there are stations in the
network, whereon ping requests are blocked.

Quick scan is parallel, regular scan is sequential.

The **Network scanner** operating speed is different for these cases.
Maximal scanning time is calculated in the following way:

◆ for regular scan: *<N>* * *<timeout>*,

◆ for quick scan: *<N>*/40 + 2**<timeout>*,

where: *<N>* - stations quantity, *<timeout>* - value, specified in the **Timeout** field.

3.4.2. License Manager

Enterprise Server contains the **License Manager** component. This component helps you to manage the license key files of **Server** and **Agent**.

To open the **License manager** select **Administration** item in the main menu of **Dr.Web Control Center**. In the opened window select the License manager item in the control menu (pane on the left).

The main pane of the **License manager** consist of hierarchical list that contains:

◆ Server keys. This section contains records with license keys of **Server**. Note that only one record is active (using by **Server** at the moment).

◆ Agent keys. This section contains records with license keys of **Agent**. Each license key can be assign for several stations or groups, displayed as nested items of the key record.

To manage license keys use the items of the toolbar:

➕**Add key** - lets you to add a new record with the key file. To do this, select the option in the drop-down menu:

🔲 **Add server key** - add a new key file for **Server**.

🔲 **Add agent key** - add a new key file for **Agent**.

🔑 **Remove key** - delete a records for a key files.

> ℹ️ You can not delete a record for an **Agent** key file, assigned for the **Everyone** group, and the current active record of a **Server** key file.

Edit - view the information about the license, its activation (only for **Server**) and replace the key file (only for an **Agent**), if necessary. This option is active only if the record for **Server** or **Agent** key is selected in the main pane.

Propagate these settings to another object - allows to assign selected key tor the group or the station, specified in the opened window. This option is active only if the record for an **Agent** key is selected in the main pane.

Export key - allows to save local copy of file for the key selected in the list.

Replacing Keys Example

If you want to change all licence keys (for example, to renew the expired licence) of anti-virus network components (either the **Server** and the **Agent**), perform the following actions in the **Licence Manager**:

1. Add the new Server key.
2. Activate the new Server key.
3. Delete the old Server key.
4. Replace the Agent licence key for the **Everyone** group and, if necessary, for all other stations and groups with the personal licence keys.

3.4.2.1. Dr.Web Enterprise Server Keys

Via the License Manager, you can implement the following actions for the Dr.Web Enterprise Server license keys:

1. View the summaries about license.
2. Add new license keys for the Server.
3. Change the license activity.
4. Remove the licence keys for the Server.

View the Summaries about License

To view the summaries about the **Server** licence, in the main pane of the **License manager**, select the record to view the detail information and click the ✎ **Edit** at the toolbar. In the opened pane you can view the following information:

   ◆ the owner of the license,
   ◆ the dealer, who sold the license,
   ◆ identification number of the license,
   ◆ license expiration date,
   ◆ Inclusion of the **Anti-spam** component.

Add New License Keys for the Server

To add new license keys for the Server:

1. Click the ➕ at the toolbar and select the ➕ **Add server key** in the drop-down menu.
2. At the opened pane, click **Browse** and select **Server** license key file.
3. Click **Save**.

> ⓘ   Several license keys records can be specified. But only one record is active.

> ⚠   If during change procedure (activating a new key file), the ID1 parameters of the **Server** in old and new key files are differ, then the **Server** schedule, connections between **Servers** and statistics of **Server** tasks will be lost.
>
> To remain the **Server** schedule, export it before changing the licence key file and import - after the changing.

Change the Server License Activity

In case of several license keys records only one record is active (using by a **Server** at the moment).

To change the Server license activity:

1. Select the record of a licence you want to set for a **Server** and click ✏ **Edit** at the toolbar.
2. At the opened pane, click **Activate**.
3. After the new key activation, reload the **Server** to continue.

Removing the License Keys for the Server

> ℹ️ You can not delete the current active record of a **Server** key file.

To remove the Server licence key:

1. In the main pane of the **License manager**, select the key you want to delete and click the 🔑❌ **Remove key** at the toolbar.
2. In the dialog box, confirm the key deletion.

3.4.2.2. Dr.Web Enterprise Agent Keys

Via the License Manager, you can implement the following actions for the Dr.Web Enterprise Agent license keys:

1. View the summaries about the license.
2. Add new license keys of the Agent.
3. Change the current Agent license key on the new one.
4. Change current Agent license keys on keys already included in the anti-virus network.
5. Remove the licence keys of the Agent.

View the Summaries about the License

To view the summaries about the license, in the main pane of the **License manager**, select the record to view the detail information and click the ✎ **Edit** at the toolbar. In the opened pane you can view the following information:

- ◆ owner of the license,
- ◆ the dealer, who sold the license,
- ◆ identification number of the license,
- ◆ license expiration date,
- ◆ Inclusion of the **Anti-spam** component,
- ◆ Anti-virus components, permissible to support by this license.

Add New License Keys of the Agent

> ⓘ Several **Agent** license keys records can be specified.

To add the new license keys for the Agent:

1. Click the ➕ at the toolbar and select the 🗂️ **Add agent key** in the drop-down menu.
2. At the opened pane, click **Browse** and select **Agent** license key file.
3. Click **Save**.

Change the Current Agent License Key on the New One

Change the current Agent license key for the new one:

1. In the main pane of the **License manager**, select the object (station or group), for which the key is specified and you want to change and click the ✏ **Edit** at the toolbar.

2. In the opened pane, click **Browse** and select the **Agent** license key file.

3. Click **Save**.

4. If the list of components, licensed for installation at the station, in the new key differs from the list in the old key, request for specifying settings according to the components list from the new key will be prompt.

   In the offered objects list, stations and groups, for which lists in the old key and in the imported key are differ, and the differences list (which components are absented and added in the new key) are presented. Set flags for objects, for those you want to set new settings for installing components list. For other objects (with cleared flags), settings specified before key changing, will remain the same.

Change the Current Agent License Key on the Already Included

To change current Agent license key for key already included in the anti-virus network:

1. In the main pane of the **License manager**, select the **Agent** key record you want to assign for the object (station or group) and click the 🔑 **Propagate these settings to another object** at the toolbar.

2. In the opened pane, select the necessary station or group (must not be empty). To select several objects, left-click them, similarly to clear selection.

3. Click **Save**.

> If the license key is already assigned to the station or group in their personal settings, to assign a new key from the list of the **License manager** main pane, drag and drop this station or group on the key record (small delay can occur during update of the main pane list).

4. If the list of components, licensed for installation at the station, in the new key differs from the list in the old key, request for specifying settings according to the components list from the new key will be prompt.

   In the offered objects list, stations and groups, for which lists in the old key and in the imported key are differ, and the differences list (which components are absented and added in the new key) are presented. Set flags for objects, for those you want to set new settings for installing components list. For other objects (with cleared flags), settings specified before key changing, will remain the same.

Removing the License Keys of the Agent

> You can not delete a record for an **Agent** key file, assigned for the **Everyone** group.

To remove the Agent licence key:

1. In the main pane of the **License manager**, select the key you want to delete or the object (station or group) for which this key is specified and click the **Remove key** at the toolbar.

2. In the dialog box, confirm the key deletion.

3. If for the object with deleted key, personal settings for installed components list are set, request for deleting personal settings will be prompt.

   In the offered objects list, stations and groups with personal settings are presented. Set flags for objects, for those you want

to set the inheritance of parental group settings. For other objects (with cleared flags), personal settings for installed components lists specified before key changing, will remain the same.

Changing of Installed Components List

Replacing or Adding the New Licence Key

If installed components lists in the new key and in the old key are differ, settings for installed components lists of the object can be changed or remain the same (see Change the Agent License Key).
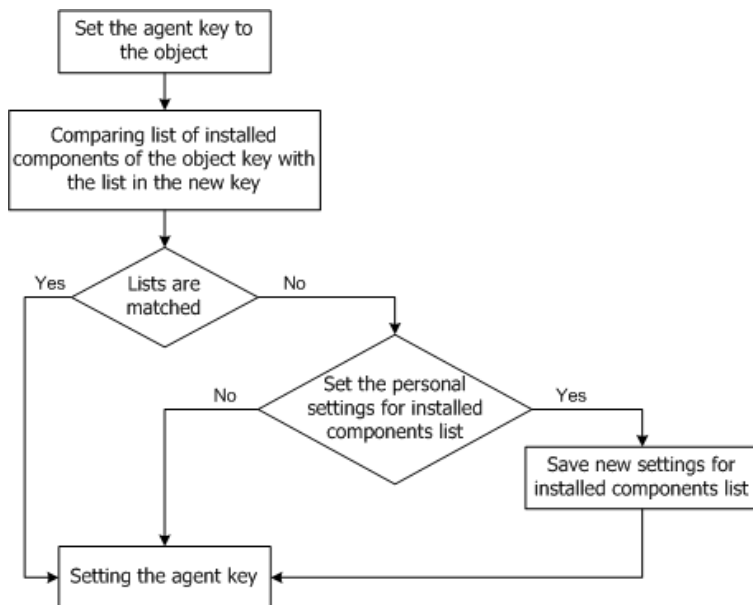
Procedure for replacing or adding the new Agent licence key

When specifying new settings:

1. If the new key contains components which are not presented in the old key, for those components the **may** value will be set in the **Installed components** list (see Management of Stations Configuration). In the sequel, user will be able to install those components to stations which are licensed with the new key.

2. If the new key does not contain components, which had been included into the old key, for those components the **cannot** value will be set in the **Installed components** list and they will be uninstalled from stations which are licensed with the new key.

3. For all other components, which were included into both old and new keys, settings, specified before key changing at the **Installed components** page, will remain the same.

When remaining settings:

Settings, specified before key changing at the **Installed components** page, will be remained.

Removing the Licence Key

Settings for installed components lists can be inherited from the parental group or remain the same (see Removing the License Keys for the Agent).
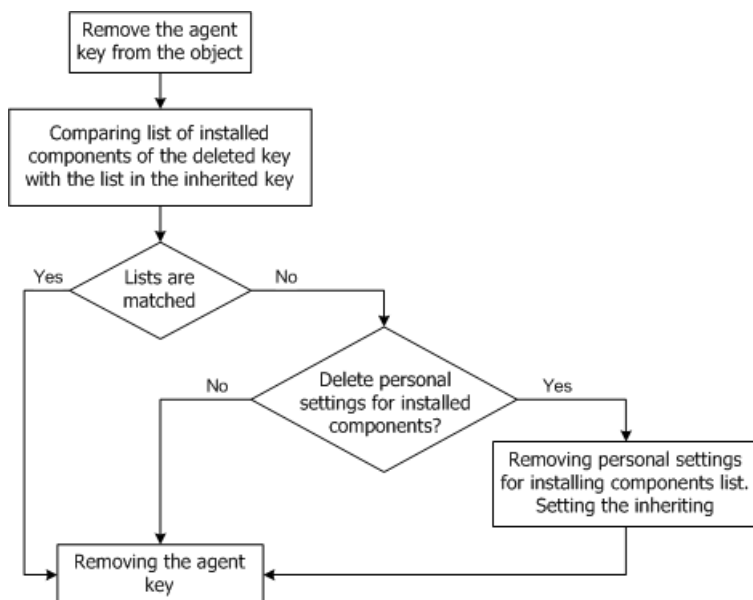
Procedure for removing Agent licence key

When inheriting settings:

Personal settings, specified before key changing at the **Installed components** page, will be deleted and inheritance of settings from the parental group will be set.

When remaining settings:

On the **Installed components** page, settings will remain as they were before key removal.

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

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

The scheme illustrates an anti-virus network built with only one

Server. In large companies it is worthwhile installing several **Enterprise Servers** to distribute the load between them.

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

When a Dr.Web Enterprise Server is launched, the following sequence of commands is performed:

1. **Enterprise Server** files are loaded from the `bin` catalog,
2. the **Server Scheduler** is loaded,
3. the content of the centralized installation catalog and update catalog is loaded, notification system is initialized,
4. **Server** database integrity is checked,
5. **Server Scheduler** tasks are performed,
6. the **Server** is waiting for information from **Enterprise Agents** and commands from **Dr.Web Control Center**.

	Dr.Web Enterprise Server	----	HTTP/HTTPS
	Dr.Web Control Center	——	TCP, IPX, NetBIOS network
	Protected local computer		
	Unprotected local computer		
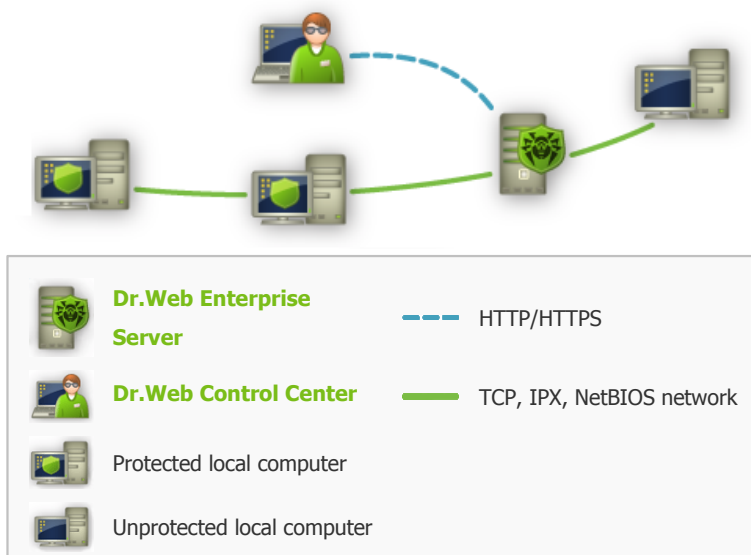
Figure 3-3. The physical structure of the anti-virus network

The whole stream of instructions, data and statistics in the anti-virus network always goes through the **Enterprise Server**. **Dr.Web Control Center** exchange information only with **Servers**. Based on **Dr.Web Control Center** commands, **Servers** transfer instructions to **Enterprise Agents** and change the configuration of workstations.

Thus, the logical structure of the fragment of the anti-virus network looks as in the Figure 3-4.

	Dr.Web Enterprise Server	` - - - `	HTTP/HTTPS
	Dr.Web Control Center	―――	TCP, IPX, NetBIOS network
	Protected computer	―――	Transfer of updates via HTTP
	Dr.Web GUS		
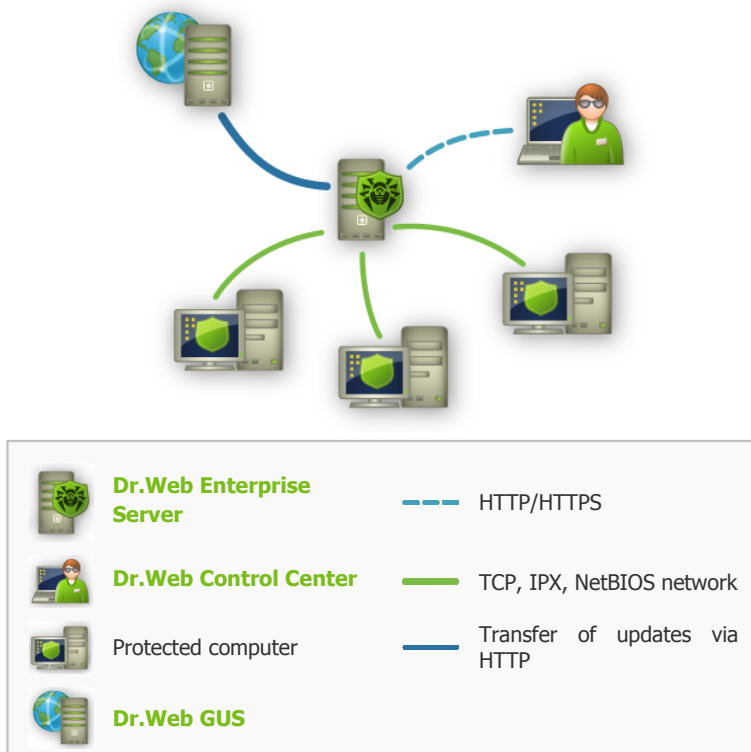
Figure 3-4. The logical structure of the anti-virus network

Between the **Server** and workstations (a thin continuous line in the Figure 3-4) transferring 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** 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 **Dr.Web ESS** provides for the possibility to compress traffic. See the description of this optional mode in p. Traffic Encryption and Compression below.

Traffic between the **Enterprise Server** and **Enterprise 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 **Enterprise Server** (a thick continuous line in the Figure 3-4) 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 ESS** 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 **Dr.Web Control Center** (a dashed line in Figure 3-4) data about the configuration of the **Server** (including information about the network layout) and workstations settings are passed. This information is visualized on the **Dr.Web Control**

Center, 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 **Dr.Web Control Center** 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**.

Chapter 4: Getting Started. General Information

4.1. 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** critical data (see p. Setting the Dr.Web Enterprise Server Schedule). It is advisable to keep the backup folder on another local disk in order to reduce the risk of losing **Server** software files and backup copies at the same time.

Connecting via the Dr.Web Control Center

The **Server** is started automatically once the installation of the **Server** is complete (see also Dr.Web Enterprise Server).

To set up the **Server** and configure the anti-virus software, the **Dr.Web Control Center** should be run on the computer of the administrator and a connection to the **Server** should be established.

From any computer with network access to the **Server**, **Dr.Web Control Center** is available at the following address:
`http://<Server_Address>:9080`

or
`https://<Server_Address>:9081`

where <*Server_Address*> is the IP address or domain name for the computer on which **Enterprise Server** is installed.

In the authorization dialog window specify the user name and password of the administrator (by default, administrator name is

admin and the password is the same, as was specified during **Server** installation, see Installing the Dr.Web Enterprise Server).

If registration at the **Server** is successful, the main **Dr.Web Control Center** window will be opened. In this window information on the anti-virus network managed from this **Server** can be viewed (for details, see p. Dr.Web Control Center).

Anti-virus Network Managing

Now you can administer the **Server** and the anti-virus network:

- ◆ create anti-virus stations (see Installing the Dr.Web Enterprise Agent Software via the Dr.Web Control Center),
- ◆ approve stations,
- ◆ edit, configure and remove anti-virus stations (see Administration of Anti-Virus Stations),
- ◆ configure and edit connections with neighbour **Enterprise Servers** (see Peculiarities of a Network with Several Dr.Web Enterprise Servers),
- ◆ view logs of current and neighbour **Servers** and other data.

Main controls are placed on the main menu, the control menu and the toolbar (see Dr.Web Control Center).

Connecting of Dr.Web Enterprise Agent

After the **Agent** has been installed on a workstation via the installation package, 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 Approva 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 Dr.Web Enterprise Server:

1. Select the **Administration** menu of the **Dr.Web Control Center**.
2. At the opened window, select **Unapproved stations** in the control menu.
3. A list of detected but not approved workstations with installed **Agent** will be opened.
4. Select the station in the list (set a flag), and on the toolbar, select **Approve and set primary group** to approve the access for this workstation and specify the primary group for the station.

> Read more about primary groups in p. Inheriting Stations Configuration from Groups. Primary Groups.

5. 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.

Anti-Virus Software Installation

Installation of other software components (of **Agent** and anti-virus package) is proceeded without administrator intervention.

Anti-virus components, specified at the primary group settings, are installed on the station. Later, you can change the list of components at the station primary group settings or specify corresponding personal settings for a certain 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** icon in the **Taskbar** (see also Dr.Web Enterprise Agent).

4.2. Setting the Network Connections

General Information

The following clients are connected to **Enterprise Server**:

◆ **Enterprise Agents**,
◆ **Network Installers** of **Enterprise Agents**,
◆ other **Enterprise Servers**.

Connection is always initiated by a client.

The following schemas for connection to the **Server** are available:

1. Using Direct connections.

   This approach has a lot of advantages, but it is not preferable in some situations (also, there are some situations, that are not compatible with this approach).

2. Using Server Detection Service.

   Clients use this **Service** by default (if the other is not set obviously).

   You can use this approach, if the resetting of all system is needed, in particular, if you need to move the **Server** to

another computer or change the IP-address of a computer with the **Server**.

If you configure the anti-virus network for using the direct connections, the **Server Detection Service** can be disabled. To do this, at the transport settings (**Administration** → **Dr.Web Enterprise Server Configuration** → **Transport** tab) leave the **Cluster address** field empty.

Direct Connections

Dr.Web Enterprise Server Setup

In the **Server** settings the address must be set (see Appendix E. The Specification of Network Addresses) to listen for accepting incoming TCP-connections.

You can specify this parameter in the following **Servers** settings: **Administration** → **Dr.Web Enterprise Server Configuration** → **Transport** → **Address** field.

To be listened by the **Server** the following parameters are set by default:

- ◆ `tcp/0.0.0.0:2371` - supported for backward compatibility; in particular, to avoid some problems with upgrading to the **5.0** version from the **4.XX** version, which uses the `2371` port.
- ◆ `tcp/0.0.0.0:2193` - to use the `2193` port, registered for **Dr.Web** in IANA.

`0.0.0.0` designation means "all network interfaces" for this computer, on which the **Server** is installed.

For the proper functioning of all **Dr.Web Enterprise Security Suite** anti-virus network, it is enough for the **Server** to listen at least one TCP-port, which is known by all clients.

Dr.Web Enterprise Agents Setup

During the **Agent** installation, the **Server** address (IP-address or hostname of the computer, on which the **Server** is launched) can be directly set in installation parameters:

`drwinst` *<Server_Address>*

For the **Agent** installation it is recommended to use the **Server** name, registered in DNS service. This will simplify the setting of the anti-virus network in case of moving **Enterprise Server** to another computer.

By default the `drwinst` instruction launched without parameters will scan the network for **Enterprise Servers** and will try to install **Agent** from the first found **Server** (the **Multicast** mode with using Server Detection Service).

Thus, the **Server** address become known for the **Agent** during installation.

You can change the **Server** address in the **Agent** settings manually later. To view and edit the settings of connection to the **Server**, use the **Agent** context menu item **Settings → Connection**.

Dr.Web Enterprise Server Detection Service

In this connection scheme, client does not know the **Server** address preliminary. Before establishing each connection, the **Server** will be searched in the network. To do this, the client sends the broadcast query and waits for the respond, that includes **Server** address. After the client gets respond, it will establish a connection with the **Server**.

To realize this scheme, the **Server** must "listen" the network for such queries.

Several variants of realization of this scheme is available. Most important is that the **Server** search method at the clients side must be matched with the **Server** respond part.

The *Multicast over UDP* mode is used by default in the **Dr.Web Enterprise Security Suite**:

1. **Server** gets registered in the multicast group with `231.0.0.1` address.

2. **Agents** send multicast queries to the `231.0.0.1` group address during **Server** search.

Server listens by default (similarly to direct connections):

◆ `udp/231.0.0.1:2371`
◆ `udp/231.0.0.1:2193`

This parameter is set at the **Servers** settings: **Administration** →

Dr.Web Enterprise Server Configuration → **Transport** tab → **Cluster address** field.

Firewall Setup

For anti-virus network components communication, all ports and interfaces, which are used by this components, must be opened on all computers in the anti-virus network.

During **Server** installation, the installer allows to add an exceptions to OS firewall settings (except Windows 2000 OS). To do this, set the **Add Server ports and interfaces to firewall exceptions** flag.

If a non-built-in Windows firewall is in use, the network administrator should set it up manually.

Chapter 5: Anti-Virus Network Administrators

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 **Enterprise Server**. Such employer should either be a local network administrator or work closely with such person.

> To manage the **Dr.Web ESS 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 **Enterprise Server** requires full access to its installation catalog.

5.1. Authentication of Administrators

To connect to the Enterprise Server, administrator can authenticate by the following ways:

1. With storing administrative account information in the **Server** DB.
2. Via the Active Directory (for **Servers** under Windows OS).
3. Via the LDAP protocol.
4. Via the RADIUS protocol.

Authentication methods are used sequentially according to the following rules:

1. The order of authentication methods usage depends on the order of their following in the settings, specified in the **Control Center**.

2. Authentication of administrator from the **Server** DB is always tried first.

3. By default, LDAP authentication is used by the second, via the Active Directory - the third, via the RADIUS - the fourth.

4. Authentication methods via LDAP, Active Directory and RADIUS can be swapped in the **Server** settings, but authentication of administrator from the **Server** DB is always used first.

5. Authentication methods via LDAP, Active Directory and RADIUS are disabled by default.

To swap the usage of authentication methods:

1. Select **Administration** in the main menu of the **Control Center**.

2. Select **Authorization** in the control menu.

3. In the opened window, list of authentications types is represented in the order of use. To change this order, click the arrow on the left of authentication type name. Corresponding authentication methods will be switched.

Authentication of Administrators from the Server DB

Authentication method with storing administrative account information in the **Server** DB is used by default.

To manage administrators list:

1. Select **Administration** in the main menu of the **Control Center**.

2. Select **Administrative accounts** in the control menu. The list of all administrators registered in the DB will be opened.

   See the Management of Administrative Accounts section for details.

Active Directory Authentication

To enable Active Directory authentication:

1. Select **Administration** in the main menu of the **Control Center**.
2. Select **Authorization** in the control menu.
3. In the opened window, select **Microsoft Active Directory** section.
4. Set the **Use Microsoft Active Directory authorization** flag.
5. Click **Save**.

For Active Directory authentication, only enabling of using this authentication method is configured in **Control Center**.

You must edit Active Directory administrators' settings manually at the Active Directory server.

To edit Active Directory administrators:

> ⚠ The following operation must be carried out from a computer with Active Directory Service snap-in.

1. To enable editing of administrator parameters, do the following:
   a) Modify Active Directory scheme with the `drwschema-modify.exe` utility (is included in the **Enterprise Server** distribution kit). Modification may take some time. Note that depending on the domain configuration, it may take up to 5 minutes and more to synchronize and apply the modified scheme.
   b) Register Active Directory Schema snap-in, execute the `regsvr32 schmmgmt.dll` command with the administrative privileges, then run `mmc` and add the **Active Directory Schema** snap-in.

c) Using the Active Directory Schema snap-in, add the auxiliary **DrWebEnterpriseUser** class to the **User** and (if necessary) **Group** classes.

> If the scheme modification and application process has not finished, the **DrWebEnterpriseUser** class may be not found. In this case, wait for a few minutes and retry to add the class as described in **c)** step.

d) With the administrative privileges run the `drweb-esuite-aduac-600-xxxxxxxxx-windows-nt-xYY.msi` file (is included in the **Enterprise Security Suite 6.0.4** distribution kit) and wait until the installation finishes.

2. Visual editing of attributes is available from the **Active Directory Users and Computers** control panel → **Users** section → in the **Administrator Properties** window for editing settings of selected user → on the **Dr.Web Authentication** tab.

3. The following parameters are available for editing (**yes**, **no** or **not set** values can be set for each attribute):

◆ **User is administrator** indicates that the user is full-rights administrator.

◆ **User is read-only administrator** indicates that the user is administrator with read-only rights.

If the **yes** value is set for the **User is administrator** parameter only, the user is full-rights administrator.

If the **yes** value is set for both **User is administrator** and **User is read-only administrator** parameters, the user is administrator with read-only rights.

◆ **Inherit permissions from groups** parameter allows inheriting of the rest parameters values from the user groups. If any parameter (or several parameters) has **not set** value and the **Inherit permissions from groups** parameter is set to **yes**, values of not specified parameters are inherited

from the user groups.

> **i** Algorithms of operating principles and attributes handling during authorization are described in the Appendix O.

LDAP Authentication

To enable LDAP authentication:

1. Select **Administration** in the main menu of the **Control Center**.
2. Select **Authorization** in the control menu.
3. In the opened window, select **LDAP authorization** section.
4. Set the **Use LDAP authorization** flag.
5. Click **Save**.

You can configure authorization using LDAP protocol at any LDAP server. Also you can use this mechanizm to configure the **Server** under UNIX system-based OS for authorization in Active Directory on a domain controller.

> **i** Settings of LDAP authorization are stored in the `auth-ldap.xml` configuration file.
>
> General xml attributes are described in the Appendix O.

Unlike to Active Directory, this mechanizm can be configures to any LDAP scheme. By default **Server** attributes are used as they were defined for Active Directory.

LDAP authorization process can be presented as the following:

1. LDAP server address is specified via the **Control Center** or xml configuration file.
2. For the specified user name, the following actions are performed:

◆ Translation of name to the DN (Distinguished Name) using DOS-like masks (with * symbol), if rules are specified.

◆ Translation of name to the DN using regular expressions, if rules are specified.

◆ Custom script for translation of name to the DN is used, if it is specified in settings.

◆ If matches in translation rules are not found, specified name is used as it is.

> Format of user names specifying is not predefined and not fixed - it can be any as it is accepted in the company, i.e. forced modification of LDAP scheme is not demanded. Translation according given scheme is performed using rules of translation of names to LDAP DN.

3. After translation, like for the Active Directory, attempt of the user registration at the specified LDAP server using determined DN and specified password is performed.

4. After this, like for the Active Directory, LDAP object attributes are read for the determined DN. Attributes and their possible values can be redefined in the configuration file.

5. If undefined values of administrator attributes are found, and inheriting is specified (in the configuration file), the search of needed attributes in the user groups is the same as in the Active Directory.

5.2. Types of Administrators

> This section contains information about administrators, account data of which is stored in the **Enterprise Server** DB.

There are four types of administrator accounts:

◆ Full-rights administrators.

◆ Read-only administrators.

◆ Group administrators with full-rights.

◆ Group administrators with read-only rights.

Full-Rights Administrators

Administrators with full rights have exclusive rights to the administration of **Enterprise 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).

Full-rights Administrator can view and edit the list of current administrator accounts.

Read-Only Administrators

Administrators with read-only rights can only view the settings of the anti-virus network and its separate elements, but cannot modify them.

Group Administrators with Full-Rights

Group Administrators have access to all system group and those custom groups which they are allowed to manage (including nested groups). Group Administrator accounts could be created for custom groups only (see System and User Groups). Only those groups which such administrators are allowed to access are displayed for them in the hierarchical tree.

The list of current administrator accounts is not available for Group Administrators.

Group Administrators with Read-Only Rights

You can grant Group Administrators with full-rights to manage their groups as well as read-only rights.

Default Administrators

After **Server** is installed, the **admin** account for administrator with full rights is created automatically. Access password for this account is specified during the **Server** installation (step 15 in the installation procedure).

5.3. Management of Administrative Accounts

> This section contains information about administrators, account data of which is stored in the **Enterprise Server** DB.

Administrators with full rights can:

◆ Add new and delete already existing administrators accounts.

◆ Edit settings for all administrators of anti-virus network.

Group administrators and administrators with read-only rights can:

◆ Edit some of settings of their account only.

5.3.1. Creating and Deleting Administrators

Creating Administrators

To add administrator account:

1. Select the **Administration** item in the main menu of the **Dr.Web Control Center** and then the **Administrative accounts** item in the control menu.

2. Click the 🧑‍💼 **Create account** icon in the toolbar.

3. A window with account settings similar to the settings, will be opened. Specify the following parameters:

   ◆ In the **Login** field specify administrator account login for the **Dr.Web Control Center** access.

   ◆ In the **Password** and **Retype password** fields set the password for the **Dr.Web Control Center** access.

   ⚠️ It is not allowed to use national characters in administrator password.

   ◆ Set the **Read only** flag to restrict access rights.

   ◆ In the **First name**, **Middle name** and **Last name** fields you can specify administrator's personal data.

   ◆ In the **Interface language** drop-down list, select the language which will be used by the adding administrator.

   ◆ In the **Date format** drop-down list, select the date format which will be used by this administrator during editing settings that contain dates. The following formats are available:

     • European: `DD-MM-YYYY HH:MM:SS`

     • American: `MM/DD/YYYY HH:MM:SS`

   ◆ In the **Description** field, you can set optional description of the account.

   ◆ For group administrator account, set the **Can manage a limited number of groups** flag to specify available groups.

   The **Supervised groups** section become available. In the **Supervised groups** list, specify groups managed by this administrator. To do this, click the group name in the **Known groups** list. To exclude customer groups, managed by this administrator, click the group name in the **Supervised groups** list.

   ⚠️ Values of fields, marked by the * sign, must be obligatory specified.

   ---

4. After you set all necessary parameters, click **Save** to create a new administrator account.

Deleting Administrators

To delete administrator account:

1. Select the **Administration** item in the main menu of the **Dr.Web Control Center** and then the **Administrative accounts** item in the control menu.

2. Select the account you want to delete in the administrators list.

3. Click the **X Remove account** icon in the toolbar.

5.3.2. Editing Administrators

To edit administrator account:

1. Open the account settings section:

   For administrators with full rights, you can do this by one of the following ways:

   ◆ Select the **Administration** item in the main menu of the **Dr.Web Control Center**, in the opened window, select the **Administrative accounts** item in the control menu. In the administrators list, select the account which you want to edit. Click **Edit** on the toolbar.

   ◆ Select the **Preferences** item in the main menu of the **Dr.Web Control Center**, in the opened window, select the **My account** item.

   For group administrators and administrators with with read-only rights, account settings can be opened via the **Preferences** item in the main menu of the **Dr.Web Control Center** only.

2. You can edit settings, which had been specified during adding a new account if necessary.

> ⚠️ Values of fields, marked by the * sign, must be obligatory specified.

> For group administrators and administrators with read-only rights, the list of editing settings is limited.

3. The following settings are read only:
    - ◆ Dates of creation and last modification of the account.
    - ◆ **Status** - network address of the last connection under current account.

4. After changing settings, click **Save**.

5. Click 🔑 **Change password** to set a new password for account access.

> ℹ️ Administrator with full rights can edit password for all other administrators.

> ⚠️ It is not allowed to use national characters in administrator password.

Chapter 6: Groups. Integrated Workstations Management

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

Grouping of antivirus stations allows to perform:

- ◆ Group operations over all stations, included to these groups.

  As for separate group so and for several selected groups, you can launch, view and stop scan tasks on stations, included to this group. In the same way, you can view statistics (including infections, viruses, start/stop, scan and installation errors and etc) and summary statistic for all workstations of the group or several groups.

- ◆ Settings the single parameters for stations via the group, to which these stations are included (see p.).

- ◆ Order (structure) the list of workstations.

It is possible to create nested groups.

6.1. System and User Groups

System Groups

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

Dr.Web ESS has an initial set of system groups. These groups are created during the installation of **Enterprise Server** and may not be deleted. Still the administrator may disable their display, if necessary.

Each system group except **Everyone** contains a set of feature-packed subgroups.

Everyone group

Group containing all stations known to **Enterprise Server**. The **Everyone** group has default settings.

Status

Status group contains subgroups 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.

◆ **Deinstalled** group. Once **Enterprise Agent** software has been deinstalled from a station, the station is transferred to the **Deinstalled** group.

◆ **Deleted** group. Contains stations, which were deleted by an administrator from the **Server**. Such stations can be restored (see p.).

◆ **Offline** group. Contains all workstations not connected at the moment.

◆ **Online** group. Contains all workstations connected at the moment (reacting to **Server** requests).

Operating system

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

◆ **Android** family groups. This family includes a set of groups, that correspond to specific version of Android OS for mobile devices.

◆ **Mac OS X** family groups. This family includes a set of groups, that correspond to specific version of Mac OS X operating

system.

◆ **Netware** group. This group contains stations, that operate under Novell NetWare OS.

◆ **UNIX** family groups. This family includes a set of groups, that correspond to OS of UNIX system-based systems, for example, Linux, FreeBSD, Solaris, etc.

◆ **Windows** family groups. This family includes a set of groups, that correspond to specific version of Windows operating system.

◆ **Windows CE** group. This group contains stations, that operate under Windows Mobile OS for mobile devices.

Transport

The 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.

Ungrouped

This group contains stations, which are not included in any of user groups.

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 the table bellow, 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 of anti-virus components (to be propagated to its stations).

Table 6-1. Groups and supported parameters

Group/group type	Parameter			
	Automatic membership	Membership administration	Primary group	Possibility to have own settings
Everyone	+	−	+	+
Status	+	−	−	−
Transport	+	−	−	−
Operating system	+	−	+	+
Ungrouped	+	−	−	−
User groups	−	+	+	+

Under group administrator account, the user group which he manages will be the root of the hierarchical tree, even if it has the parent group. All nested groups of managing group is available.

6.2. Group Management

6.2.1. Creating and Deleting Groups

Creating Groups

To create a new group:

1. Select: **Add a station or a group** on the toolbar and the **Add a group** in the submenu. A window for creating a group will be opened.
2. The **ID** entry field is filled in automatically. You can edit it during creation, if necessary. The identifier should not contain blank spaces. In the sequel group ID can not be changed.
3. Type the group name in the **Name** entry field.
4. For nested groups, in the **Parent group** field, select a parental group from the drop-down list. For a root group (without a parent), leave this field blank. The group will be added to the root of the hierarchical tree. In this case settings are inherited from the **Everyone** group.
5. Type comments in the **Description** entry field (optional).Click **OK**.

The groups you create are initially empty. Procedure of including workstations to groups is described in the Adding a Station to a Group. Removing a Station from a Group section.

Deleting Groups

To delete a group:

1. Select the user group in the hierarchical list.

2. Click ⭐ **General** → ❌ **Remove selected objects** on the toolbar.

> ℹ️ You cannot delete preinstalled groups.

6.2.2. Editing Groups

To edit group settings:

1. Select the **Network** item in the main menu of the **Dr.Web Control Center**, then select the group in the hierarchical list.
2. Click **Properties** in the control menu (left pane).
3. Window with the group settings will be opened. This window contains **General** and **Configuration** tabs. These settings are described below.

> ℹ️ If you open group permissions via the ⭐ **General** → ✏️ **Edit** item on the toolbar, the **Stations information** section with general information about stations, included to this group, will be also available.

4. Click **Save** to save all changes.

General

In the **General** section, the following fields are listed:

◆ **ID** - group unique identifier. Is read-only.

◆ **Name** - group name. You can change the group name, if necessary.

> For preinstalled groups, **ID** and **Name** fields are read-only.

◆ **Parent group** - parent group in which this group is included and from which group configuration is inherited, if the personal settings is not specified. If the parent group is not specified, settings are inherited from the **Everyone** group.

◆ **Description** - optional filed with group description.

Configuration

> For more details on inheriting of group settings by stations, for which this group is primary, see Using Groups to Configure Stations section.

In the **Configuration** section, the following groups parameters are presented:

◆ 🔒 - setting permissions for the workstations, for which this group is primary. Setting permissions of group is similar to setting permissions of separate workstations (see p. Setting Users Permissions).

◆ 🔟 - changing schedule settings for the workstations, for which this group is primary. Setting schedule of group is similar to setting schedule of separate workstations. Centralized schedule setting described in p. Editing Scheduled Tasks on a Station.

◆ 🔑 - setting the licence key file for the workstations, for which this group is primary.

◆ 🔄 - setting restrictions for anti-virus software updating for the workstation, for which this group is primary (see p. Update Restrictions).

◆ 📦 - installing components list for workstations, for which this group is primary. Setting the components list of group is similar

to setting the components list of separate stations (see p.).

◆ Settings of the anti-virus components - **Dr.Web Scanner for Windows**, **SpIDer Guard for Windows**, **SpIDer Mail for Windows Workstations**, etc. Click the ⚙ button against the correspond item to change its settings. Setting the anti-virus package components of group is similar to setting the anti-virus package components of separate workstations (see also Management of Stations Configuration).

6.3. Adding a Station to a Group. Removing a Station from a Group

There are several ways how to add a workstation to a user group:

1. Change tha station settings.
2. Grag'n'drop a station in the hierarchical list.

To edit the list of groups containing the station via the station settings:

1. In the main menu, select **Network**, then click the name of a workstation in the hierarchical list.

2. Open the station settings by one of the following ways:

   ◆ In the control menu (left pane), select **Properties**.

   ◆ Click the ⭐ **General** → ✏ **Edit** in the toolbar.

3. In the **Station Properties** pane, select the **Groups** section (tab).

   The **Member of** list displays the groups which include the workstation.

   The **Other groups** list displays the groups, in which membership for the workstation is yet available.

4. To add the workstation into a group, click the name of a group in the **Known groups** list. The workstation will be added to the group, and the group name will move into the **Member of**

list.

5. To remove a workstation from the group, click the name of a group in the **Member of** list. The workstation will be removed from the group, and the group name will move into the **Known groups** list.

> i You cannot remove stations from preinstalled groups.

6. To save settings, click **Save**.

In the **Properties** section, you can also set a group as the primary one for the station (for more read p. Inheriting Stations Configuration from Groups. Primary Groups).

To edit the list of groups containing the station via the hierarchical list:

1. In the main menu, select **Network** and unfold the hierarchical list of groups and stations.

2. To add a station to the user group, press CTRL and drag-and-drop a station to the corresponding group.

3. To move a station from one user group to another, drag-and-drop this station from the user group, from which station will be removed, to the user group, to which station will be added.

> i When dragging a station from preinstalled group in both 2 and 3 steps, station is added in the user group and is not removed from preinstalled group.

> ⚠ Drag-and-drop method is not supported under Windows Internet Explorer 7 web browser.

Merging stations

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:

1. Select all repeated names of workstation. Use the CTRL to do this.
2. In the toolbar, select ⭐ **General** → 🌱 **Merge stations**.
3. In the offered list, select the station which will be the main. All other stations will be deleted and their data will be prescribed to the selected station.
4. In the offered list, select the station settings of which will be set for the main station.
5. Click **Save**.

6.4. Using Groups to Configure Stations

Stations settings can be:

1. Inherited from the primary group.
2. Specified personally.

Inherited Settings

For created group, its settings are inherited from the parental group or from the **Everyone** group, if the parental group is not specified.

For created station, its settings are inherited for the primary group.

> For more details, refer the <u>Inheriting Stations Configuration
> from Groups. Primary Groups</u> section.

When viewing or editing workstation configuration inherited from the
primary group, a notification that the settings are inherited from the
primary group will be displayed in correspondent windows.

You can set different configurations for different <u>groups</u> and <u>stations</u>,
by editing corresponding settings.

Personal Settings

To set the personal settings for the station, edit corresponding settings
section (see p. <u>Management of Stations Configuration</u>). In the settings
section, notification that the settings are set personally for the station
will be displayed.

If the personal settings are specified for the station, personal group
settings and their changing will not have any affect on station settings.

You can restore the configuration inherited from the primary group. To
do this, click the **Remove these settings** button in the toolbar
of the **Dr.Web Control Center**, in the corresponding parameters
section or in the station settings section.

6.4.1. Inheriting Stations Configuration from Groups. Primary Groups

Inheriting a Station Settings

When a new workstation is created, its configuration settings are
inherited from one of the groups it belongs to. That group called 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.

It is possible to create nested groups.

Inheritance in nested groups depends on group hierarchy. If a station have no personal settings, it inherits the configuration from parental group, and this process repeats recursively. Therefore the search for group configuration is performed upwards through the hierarchical tree of nested groups, starting from the station primary group and stopping at the root group. If no personal settings are selected for all the nesting groups, then the **Everyone** group settings are inherited.

Example

The structure of the hierarchical list is as follows:

Network
— **Everyone**
— Group1
  — Group2
    — Group3
      — Group4
        — Station1
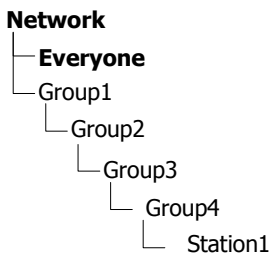
The `Group4` is the primary group for the `Station1`. To determine which settings to inherit for the `Station1`, the search is carried out in the following order: `Station1` → `Group4` → `Group3` → `Group2` → `Group1` → `Everyone`.

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 toolbar in 📑 **Tree settings**, clear the **All groups membership** flag.

Setting the Primary Group

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

To set primary group for station

1. In the main menu, select **Network**, then click the name of a workstation in the hierarchical list.

2. In the control pane (left pane), select **Properties**. In the **Station Properties** window, select the **Groups** tab.

3. In necessary, click a group in the **Membership in** list to set the group as primary.

4. Click **Save**.

To set primary group for several stations

1. In the main menu, select **Network**. In the hierarchical list, click the name of the workstations or groups of workstations for which you want to set a primary group. To select several workstations, press and hold CTRL or SHIFT during selection.

2. On the toolbar, click ⭐ **General** → 🔢 **Set a primary group for the stations**. This opens the window listing the groups which can be set as primary for the selected workstations.

3. In the window, click the name of a group you want to set as primary for the workstations.

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 toolbar, click ⭐ **General** → 🔢 **Become primary**.

6.4.2. 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 propagate settings:

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 the **Propagate these settings** in one of the following locations:

   ◆ 🐞 the editor of anti-virus component configuration,

   ◆ 📅 the schedule editor,

   ◆ 🔄 in the update restrictions window,

   ◆ 🖥 in the installing components window.

   A window of the network catalog will be opened.

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**.

6.5. Comparison of Stations and Groups

You can compare stations and groups by general parameters.

To compare several objects of the anti-virus network:

1. In the main menu, select **Network**, then select the objects you want to compare in the hierarchical list. Use CTRL and SHIFT for this. The following variants are possible:

   ◆ selection of several stations - to compare selected stations;

   - ◆ selection of several groups - to compare selected groups and all nested groups;
   - ◆ selection of several stations and groups - to compare all stations: selected directly in the hierarchical list and included in all groups and their nested groups.

2. In the control menu (left pane), select **Comparison**.

3. The comparison table for selected objects will be opened.

   ◆ Comparative parameters for groups:

   - **Stations** - total number of stations, included in this group.
   - **Stations online** - number of on-line stations.
   - **Primary for** - number of stations for which this group is parental.
   - **Personal configuration** - list of components with personal settings, not inherited from the parental group.

   ◆ Comparative parameters for stations:

   - **Creation time** of this station.
   - **Primary group** for this station.
   - **Personal configuration** - list of components with personal settings, not inherited from the primary group.
   - **Installed components** - list of anti-virus components installed at this station.

Chapter 7: Administration of Workstations

Anti-virus networks operated by **Dr.Web ESS** provide for centralized configuring of anti-virus packages on workstations and allows:

◆ to set the configuration parameters of anti-virus programs,

◆ to schedule tasks on workstations,

◆ launch scanning the computer independently of schedule settings,

◆ 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**.

7.1. Management of Workstation Accounts

7.1.1. New Stations Approval Policy

Procedure of stations adding via the **Control Center** is described in the Creation of a New User Account section.

Possibility of managing authorization of stations at the **Enterprise Server** depends on the following parameters:

1. If during the **Agent** installation, **Automatic** authorization is selected, mode of stations access to the **Server** is defined according to settings specified at the **Server** (used by default).

2. If during the **Agent** installation, **Manual** authorization is selected and **Identifier** and **Password** parameters are specified, when connecting to the **Server**, station will be authorized automatically regardless of **Server** settings (is used by default when installing the **Agent** via the *esinst* installation package - see p. Installation Files).

> Setting the type of the **Agent** authorization during its installation is described in p. Installation of the Dr.Web Enterprise Agent in the Graphical Mode of the Installer (step 6).

To change the access mode of stations to the Dr.Web Enterprise Server:

1. Open the **Server** configuration: select the **Administration** item in the main menu, then click **Configure Dr.Web Enterprise Server** in the control menu.

2. On the **General** tab, in the **Newbie** drop-down list select the necessary option:

   ◆ **Approve access manually** (the mode is specified by default unless changed at the **Servers** installation),

   ◆ **Allow access automatically**,

   ◆ **Always deny access**.

Manual Access Approving

In the **Approve access manually** mode, new stations are placed to the **Unapproved stations** list until administrator submits them.

To access the Unapproved stations list:

1. Select the **Administration** item in the main menu of the **Dr.Web Control Center**, then click **Unapproved stations** in the control menu.

2. In the opened window, the table of stations with installed **Agents** requesting the **Server** access and the following general information about stations are listed: time of request, network name, IP address of a station and OS installed at a station.

3. To specify an access to the **Server**, set flags for corresponding stations or set the flag in the table header to select all stations. On the toolbar, set the action to apply for selected stations:

   ◆ - approve access for selected stations and set the primary group from the offered list,

   ◆ - deny access for selected stations.

Automatic Access Approving

In the **Allow access automatically** mode, all stations that request an access to the **Server** will be approved automatically without requesting the administrator. The **Everyone** group will be set as a primary.

Access Denying

In the **Always deny access** mode, the **Server** denies access for requests from new stations. The administrator should manually create an account for new stations and set access password for them.

7.1.2. Removing and Restoring Stations

To remove a workstation account:

1. Select the **Network** item in the main menu, then click ⭐ **General** → ❌**Remove selected objects** in the toolbar of the opened window.

2. You will be prompts to remove the station. Click **OK**.

After a station is removed from the hierarchical list, it is added to the deleted stations table. You can restore the removed station via the **Dr.Web Control Center**.

To restore a workstation account:

1. Select the **Network** item in the main menu, in the opened window in the hierarchical list select deleted station or several stations you want to restore.

> ℹ️ All deleted stations are located in the **Deleted** subgroup of the **Status** group.

2. On the toolbar, select ⭐ **General** → 🔄 **Restore deleted stations**.

3. The section for station restoring will be opened. You can specify the following station parameters, which will be set during restoring:

   ◆ **Primary group** - select the primary group, in which the station will be added. By default the primary group which was set before station deletion is selected.

> ℹ️ If you restore several stations simultaneously, the **Former primary group** is selected by default. It means that for each selected station its own primary group, in which station was resides before deletion, will be specified. If the definite group is selected, for all restoring stations the same specified group will be set.

◆ In the **Member of** section, you can change the list of groups in which the station will be included. By default, the list of groups in which the station has been included before deletion is set. To include the station in user groups, click names of accessible user groups in the **Groups list** section. To exclude the station from user groups in which it has been included before deletion, click names of corresponding user groups in the **Member of** section.

4. To restore the station with specified parameters, click **Restore.**

7.2. Management of Stations Configuration

Station Settings

To view and edit the properties of a workstation

1. Select the **Network** item in the main menu, then select the station in the hierarchical list and click the ⭐ **General** → ✏️ **Edit** element of the Toolbar.

2. A panel with properties of the station will be opened in the right part of the **Dr.Web Control Center**. This panel contains the following settings: **General**, **Configuration**, **Groups**, **Location**. These settings are described below.

3. To save changes in the settings, click **Save**.

General

In the **General** section, the read-only fields are listed:

◆ **ID** - station unique identifier;
◆ **Name** - station name.

Also you can specify the following fields:

◆ In the **Password** field, specify a password to authorize the station at the **Server** (retype this password in the **Retype password** field). If you change the password, you must repeat this action in the **Agent** connection settings at the station to permit **Agent** connection.

◆ in the **Description** field, add comments.

> **i**   Values of fields, marked by the * sign, must be obligatory specified.

Configuration

In the **Configuration** section, the following stations parameters are presented:

◆ 🔒 - setting permissions for the workstation (see p. <u>Setting Users Permissions</u>).

◆ 📅 - changing schedule settings. Centralized schedule setting described in p. <u>Editing Scheduled Tasks on a Station</u>.

◆ 🔧 - setting the licence key file for the station.

◆ 🔄 - setting restrictions for anti-virus software updating. For more details about update restrictions, see p. <u>Update Restrictions for Workstations</u>.

◆ 📦 - installing components list (see p. <u>Anti-Virus Package Composition</u>).

◆ the settings of the anti-virus components - **Dr.Web Scanner for Windows**, **SpIDer Guard for Windows**, **SpIDer Mail for Windows Workstations**, etc. Click the ⚙ button against the correspond item to change its settings.

Dr.Web Control Center also provides you with option for deleting personal settings of a workstation. These settings are located in the left part of the corresponding options for components configuration options.

When you delete personal settings of a workstation, it inherits settings from the primary group.

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

Meanwhile the **Dr.Web Control Center** 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 manage separate parameters, use the options located on the right from corresponding settings:

to restore the value a parameter had before editing.

to set the default value for a parameter.

◆ to manage set of parameters, use the options located 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 propagate this parameters on other objects (group or several groups and workstations).

- to restore the values all parameters had before editing.

- to restore the default values of all parameters.

- to export parameters to a file of a special format.

- to import parameters from such file.

- to delete the specific configuration of the given workstation (the configuration inherited from the preinstalled groups will be restored, see p.).

◆ Click **OK** to confirm the changes made, or click **Cancel** to restore the state of the configuration before editing.

Groups

In the **Groups** section, you can set the list of groups into which the workstation is included (see Adding a Station to a Group. Removing a Station from a Group)

Also in this section you can change the primary group for the station (see Inheriting Stations Configuration from Groups. Primary Groups).

Security

In the **Security** section, restrictions for network addresses from which **Agents**, network installers and other ("neighboring") **Enterprise Servers** will be able to access the given **Server** are set.

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

To allow any TCP address, include it into the **TCP:Allow** or **TCPv6:Allow** list.

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

To edit an addresses at the list:

1. Specify an address in the corresponding field and click **Save**.

2. To add a new field click the [+] button in the corresponding section.

3. To delete a field click [−].

   Network address specifies in format: *<IP-address>*/[*<prefix>*].

Prefix 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.

Restrictions for IPX addresses can be set similarly.

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

Location

In the **Location** section, you can set information on geographical location of the workstation.

> ℹ️ 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.

Removing Personal Settings

To remove personal settings of a workstation via the Dr.Web Control Center:

1. Select the **Network** item in the main menu, then select the workstation in the hierarchical list and click ⭐ **General →** 🗙
 Remove personal settings in the toolbar. A list of settings for this workstation will be opened. Personal settings will be marked with a flag.

2. To remove settings, clear the flags and click **Save**. Settings of the workstation 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).**

> Starting from version **5.0** anti-virus package includes **SpIDer Gate** and **Office Control** components. For using this components, they must be included in you license **(Antivirus**+**Antispam**), that described in the **Agent** key file.

> **Spam filter**, **SpIDer Gate** and **Office Control** settings are described in the manual **Dr.Web® Anti-Virus for Windows. User Manual**.

7.2.1. Setting Users Permissions

To edit users permissions via the Dr.Web Control Center for administrating the anti-virus package:

1. In the main menu, select **Network**, then click the name of a workstation in the hierarchical list.

2. In the control menu (left pane), select **Permissions**. This opens the permissions configuration window.

3. To change permissions, use the following tabs:

   ◆ **Components** - to change permissions for components management. By default, a user is authorized to launch each component, but prohibited to edit components configuration or stop the operation of components.

   ◆ **General** - to change permissions for **Agent** and its functions management.

      • **Mobile mode and update from Dr.Web GUS** - disables the **Mobile mode** option in the **Agent** context menu.

      • **Create a local schedule** - disables the **Local** option in the **Schedule** submenu of the **Agent** context menu.

      • **Change the local policy** - disables the **Run mode** option and the **Installing components** submenu in the **Agent** context menu.

      • **Change Dr.Web Enterprise Agent settings** - disables in the **Agent** context menu, in the **Settings** submenu, the **Synchronize time** option and **Log level** submenu.

      • **Stop Dr.Web Enterprise Agent interface** - disables the **Exit** option in the **Agent** context menu, if the **Agent** interface has been run under a user without administrative rights.

      • **Disable access to network** - disables the **Network access** option in the **Agent** context menu.

      • **Disable the system protection** - disables the **System protection** submenu of the **Agent** context menu.

- **Disable self-protection** - disables activity of the the **Self-protection** option in the **Agent** context menu.
- **Uninstall Dr.Web Agent** - disables uninstalling of the **Agent** at the station either via the installer or via standard Windows OS services (see the <u>Uninstalling the ESS Software for Windows® OS</u> section). In this case, **Agent** can be uninstalled only via the ⭐ **General** → 🗙 **Uninstall Dr.Web Agent** option on the toolbar of the **Dr.Web Control Center**.

To change (enable or disable) any permission, set or clear the correspondent flag.

> **i** After disabling an option that changes **Agent** settings, the value which has been set at the last time before disabling, will be used.
>
> Actions for the corresponding menu options are described at the **Dr.Web® Agent for Windows. User manual** documentation.

4. To accept the changes in permissions, click **OK**; to reject the changes, click **Cancel**.

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

6. To use the same settings for another object, click 🔒➡ **Propagate these settings to another object**.

7. To export settings to a file, click 📄 **Export settings**.

8. To import settings from a file, click 📄 **Import settings**.

9. To save changes, click **Save**.

> **i** 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**.

7.2.2. Viewing Installed Components List of the Anti-Virus Package

Components

To check which components are installed on a workstation:

1. Select the **Network** item in the main menu, then click the name of a group or workstation in the hierarchical list.

2. Select the **Installed components** item in the control menu (the panel on the left) to open a list of installed components.

> Compound of installed components list depends on:
>
> ◆ Components enabled in the licence key file.
>
> ◆ Workstation OS.
>
> ◆ Settings specified by administrator of anti-virus network at the **Server**. Administrator is able to change the list of anti-virus package components either before **Agent** (see Anti-Virus Package Composition) installation or at any time after its installation.

> It is not recommended to install **SpIDer Gate**, **SpIDer Mail** and **Dr.Web Firewall** components on servers that implement significant network functions (domain controllers, licence distribution servers and etc.) to avoid probable conflicts between network services and internal components of **Dr.Web** antivirus.

Virus Bases

To view virus databases installed on a workstation:

1. In the main menu, select **Network**, then in the hierarchical list click the workstation name. In the control menu (left pane), select **Virus bases** in the **Tables** subsection.

2. This opens a window with information on installed virus databases including information on the file containing a particular database, virus database version, the total number of virus records in the database, the database creation date.

> If the **Virus bases** item is hidden, to view the item, select **Administration** in the main menu, and then select **Configure Dr.Web Enterprise Server** in the control menu of the window. On the **Statistics data** tab, set **Stations status monitoring** and **Virus database monitoring** flags, then restart the **Server**.

7.2.3. Anti-Virus Package Composition

To change the installing components list of the anti-virus package:

1. Open the list of components, select the **Network** item in the main menu, then select the station and click the **Installing Components** item in the control menu (panel on the left).

2. Select an option for necessary components in the drop-down list:

   ◆ **must** - means that a component *must* be present on the workstation. When a new workstation is created, the component is installed with the anti-virus package. If the **must** option is specified for an existing workstation, the component will be added to the available anti-virus package.

◆ **may** - means that the component can potentially be installed. The user decides whether the component is required.

◆ **cannot** - means that installing the component is not allowed. When a new workstation is created, the component will not be installed with the anti-virus package. If the **cannot** option is specified for an existing workstation, the component will be removed from the anti-virus package.

Table 7-1 shows whether the component will be installed on the workstation (+) according to the parameters specified by the user and the settings defined by the **Server** administrator.

Table 7-1.

User parameters	Specified on the Server		
	Must	**May**	**Cannot**
Install	+	+	
Do not install	+		

3. Click **Save** to save the settings and the set of anti-virus package components on the workstation.

The **VadeRetro Antispam** component cannot be installed, if at least one of the listed products is not installed:

◆ **SpIDer Mail**,

◆ **Dr.Web plug-in for MS Outlook**,

◆ **Dr.Web for IBM Lotus Domino**,

◆ **Dr.Web for MS Exchange Server**,

◆ **Dr.Web for Qbik WinGate plug-in**.

7.3. Editing Parameters of the Dr.Web Enterprise Agent for Windows® OS

To view and edit the configuration of the Dr.Web Enterprise Agent for the necessary station:

1. Select the **Network** item in the main menu.
2. Select the workstation or group in the hierarchical list (click name of the station or group).
3. Click the **Dr.Web Enterprise Agent for Windows** item in the control menu (panel on the left).
4. A window for editing the **Agent** settings will be opened.

> ⚠️ 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** settings are made via the **Dr.Web Control Center**, click **Save** button to accept changes in settings.

General Tab

On the **General** tab, you can set genaral parameters of the **Agent**, which were not included in other tabs:

- ◆ In the **Server public key** field, specify the path to the public encryption key of **Enterprise Server** on the user's computer.
- ◆ In the **Local Dr.Web key file** field, specify the path to the local key file of the **Dr.Web** product, if you want to store the license key file at the station either. Otherwise, the key file is stored at the **Server** only.
- ◆ In the **Statistics collection period (minutes)** field, set the value of the time interval in minutes for the **Agent** to send all statistics data, collected at the station.
- ◆ Specify the language for the **Agent** interface in the **Language**

drop-down list.

◆ Set the **Microsoft Network Access Protection** flag to enable the support of *Microsoft® Network Access Protection (NAT)* (for more details see p. NAP Validator).

◆ Set the **Synchronize time** flag to enable system time synchronization on the **Agent** machine with the time on the machine with **Enterprise Server**.

◆ The **Protect the HOSTS system file** flag forbids modifications of the HOSTS file. The operating system uses this file when connecting to the Internet: for translation DNS names of some web-sites to corresponding IP addresses. Changes to this file may indicate virus infection.

◆ The **Protect critical system objects** flag protects critical objects of the operating system such as register etc.

Network Tab

On the **Network** tab, you can find the parameters determining interaction with the **Server**:

◆ In the **Server** field, you can set the address of the **Enterprise Server**. You may leave this field blank, then the **Agent** will use as the address of **Enterprise Server** the value of the parameter set on the user's local machine (the address of the **Server** from which the installation was initiated).

Either one **Server** address or several different **Servers** addresses can be set. To add one more **Server**, click [+] and specify an address to the added field. Format of **Server** network addresses is described in Appendix E. The Specification of Network Addresses.

Server address example:

    tcp/10.4.0.18:2193
    tcp/10.4.0.19
    10.4.0.20

To set several addresses in **Agent** settings, the **Servers** addresses must be separated by space symbol in the **Server** field in the **Settings → Connection** section, which is called from the context menu of the **Agent** icon.

If the **Server** parameter is set incorrectly, the **Agents** will disconnect from the **Server** and will not be able to reconnect. In this case you will have to set the **Server** address on the stations directly.

◆ In the **Number of retries** field, set the parameter determining the number of attempts to find **Enterprise Server** via the connection using the Mulicasting mode.

◆ In the **Search timeout** field, set the interval between attemts to find **Enterprise Server** in seconds via the connection using the Mulicasting mode.

◆ The **Compression mode** and **Encryption mode** fields determine the compression and encryption settings of network traffic correspondingly (also see p. Traffic Encryption and Compression).

◆ In the **Network scanner listen** field, specify the UDP port for the **Dr.Web Control Center** to use when searching for working **Enterprise Agents** in a network. To disable ports listening, enter **NONE**.

This parameter should be specified in the network addresses format described in Appendix E. The Specification of Network Addresses.

By default, the **udp/:2193** is used, which means "all interfaces, port 2193".

Mobility Tab

On the **Mobility** tab, you can set the *Mobile Mode* of the **Agent**:

◆ In the **Update period** field, specify the time interval between anti-vrirus software updates, in seconds.

◆ Set the **Check Internet connection** flag to enable checking if there is a connection to the Internet before starting updating.

◆ Set the **Use proxy server** flag to use an HTTP proxy server to receive updates from the Internet. This will make the fields to set a proxy server available.

Log Control Tab

On the **Log control** tab, you can set the parameters of **Agent** logging:

◆ In the **Log file name** field, specify the path to the log file on the user's machine.

◆ The **Log level** parameter determines the level of detail of logging (see also p. Dr.Web Enterprise Server Logging).

◆ The values of the **Log rotation** fields determine such parameters of logging as the number and size of log files, and old files compression.

◆ The **Updater log files** parameter determines the maximum number of updater log files.

Interface Tab

On the **Interface** tab, you can set the parameters of the **Agent** interface.

In the **Welcome message delay** field, specify the time for which the welcome message should be delayed, in minutes. Set the value to **-1** to disable showing the welcome message.

On the **Interface** tab, you can select the type of events that the user is to be notified of. For this set the respective flag:

◆ **Critical notifications** - receive only critical notifications. Such notifications include periodical messages about:

- updating errors of the anti-virus software or some of the components;
- the necessity to restart a computer after updating.

The notification shows, if the user has administrator rights.

◆ **Virus notifications** - receive only notifications about viruses. This type of notification includes messages about virus(es) detection by one of the anti-virus software components.

◆ **Major notifications** - receive only important notifications. Such notifications include messages about:

- the launching errors of the anti-virus software or some of the components;
- the updating errors of the anti-virus software or some of the components, is displayed right after error of update procedure.
- the necessity to restart a computer after updating, is displayed right after update procedure.
- necessity of message with reboot requirement to finish components installation.

◆ **Minor notifications** - receive only minor notifications. Such notifications include messages about

- the starting of remote scanning;
- the stoping of remote scanning;
- the beginning of updating of the anti-virus software or some of the components;
- the end of successful updating of the anti-virus software or some of the components.

If you want messages of all groups to be sent, set all the four flags. Ohterwise only message of the specified groups will be displayed.

Users can configure all notifications except **Critical notifications**, which are configured by administrators only.

7.4. Editing Scheduled Tasks on a Station

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 **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; **Enterprise Server** does not control this schedule.

Centralized Schedule

Using the **Dr.Web Control Center** 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.

To edit centralized schedule:

1. Open the window for editing the schedule: select the **Network** item in the main menu, then select a group or workstation in the hierarchical list and click the **Schedule** item in the control menu (panel on the left).

2. You can add, remove and edit tasks in the schedule. You can also enable or disable any existing tasks (this is described below).

   By default for stations operated under Windows and Windows Mobile OS, two tasks are available:

   - ◆ **Startup scan** (enabled by default),
   - ◆ **Daily scan** (disabled by default).

3. After editing, click **Save** in the **Dr.Web Control Center** to save changes or a newly created tasks.

> **i** If, when edited, the schedule is empty (without any task), the **Dr.Web Control Center** will offer you to use either the schedule inherited from groups, or the empty schedule. Use empty schedule to override the schedule inherited from the groups.

To add a new task:

1. To create a new task, click 📋 **New job** on the toolbar.

> **i** Values of fields, marked by the * sign, must be obligatory specified.

2. On the **General** tab:

   - ◆ Give a name to the task in the **Name** entry field.
   - ◆ To enable the job, set the flag **Enable execution**.

   To disable the job, clear the flag. The job will remain on the list but will not be executed.

   - ◆ The **Critical job** flag instructs to perform the job at next **Enterprise Agent** launch, if execution of this job is omitted (**Enterprise Agent** is switched off at the due time). If a task is omitted several times within a certain period of time, then it will be performed only once after **Enterprise Agent** has been launched.

> ⚠️ If several scan tasks via the same **Scanner** (**Dr.Web Scanner for Windows** or **Dr.Web Enterprise Scanner**) must be implemented during station startup, only one task will be executed - the first one in the queue.
>
> For example, if **Startup scan** is enabled and critical scan via the **Enterprise Scanner** is omitted, only **Startup scan** will be executed during station startup and omitted critical task will not be done.

3. On the **Action** tab, 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** or **Dr.Web Enterprise Scanner for Windows** and specify the **Scanner** settings, described in the p. Launching and Terminating Anti-Virus Scanning on Workstations.

 ◆ 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. On the **Time** tab, in the **Time** drop-down list set the time mode of the task:

 ◆ Daily,

 ◆ Every N minutes,

 ◆ Hourly,

 ◆ Monthly,

 ◆ Startup,

 ◆ Weekly.

 The parameters of different types of the time modes are described below.

5. When all parameters for the task are specified, click **Save** to

accept changes.

Table 7-2. 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.
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 an existing task, left-click the task to select it in the list. The following actions are similar to adding a new task (see above).

To delete an existing task:

1. Set the flag next to the task.

2. Click the **Remove these settings** button on the taskbar of the **Dr.Web Control Center**.

Local Schedule

To edit 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 **Enterprise Agent** will be opened.

On the **Agent** context menu, the **Schedule** item will contain the **Local** option provided that the **Create local schedule** flag has been set in the station permissions from the **Dr.Web Control Center**.

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

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

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.

7.5. Anti-Virus Scanning of Stations

Users can scan their workstations themselves using **Dr.Web Scanner for Windows**. A **Scanner** 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** malfunction or running Windows OS in the safe mode.

For every station you can:

◆ View the list of all anti-virus components running at present.

◆ Terminate running anti-virus components of a certain type.

◆ Initiate anti-virus scanning and specify its parameters. Scans can be initiated for:

- **Dr.Web Scanner for Windows**,
- **Dr.Web Enterprise Scanner for Windows**,
- **Dr.Web Enterprise Scanner for Mac OS X**,

- **Dr.Web Enterprise Scanner for Unix**.

7.5.1. Viewing and Terminating Running Components

To view the list of running components and terminate some of them manually

1. In the main menu, select **Network**, then click the name of a workstation or group in the hierarchical list. In the control menu (left pane), select **Launched components**.

   Lists of components active at present both run manually by you, or users and scheduled, will be opened.

2. If necessary, set a flag next to a task to terminate and click **Interrupt** on the toolbar. Execution of a task will be terminated, and the tasks will be removed from the list.

7.5.2. Terminating Running Components by Type

> ⚠️ In this mode running scans will be terminated and all monitores except **SpIDer Guard** will be disabled.
>
> Warning! You cannot launch **SpIDer Mail** or **SpIDer Gate** monitors via the **Dr.Web Control Center**.

You can terminate the execution of the components on workstations

- ◆ run manually by you,
- ◆ run by users,
- ◆ scheduled.

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 running components of a certain type

1. In the main menu, select **Network**, then in the hierarchical list select workstations or groups.

2. In the toolbar, click 🔵 **Managing components** and select **Interrupt running components**. This opens the scan type selection window.

3. Set flags against the necessary types. To terminate all types, set the 🔵 **Interrupt running components** flag in the heading.

4. Click **Interrupt**.

7.5.3. Launching Scan on Station

To launch a scan task:

1. In the main menu of the **Dr.Web Control Center**, select **Network**.

2. Click the name of a station or group in the hierarchical list.

3. In the toolbar, click 🔍 **Scan**.

4. In the opened list at the toolbar, select one of the following scan modes:

   🔍 **Dr.Web Scanner for Windows. Express scan**. In this mode the following objects will be scanned:

   - main memory (RAM),
   - boot sectors of all disks,
   - autorun objects,
   - root directory of the boot sector,
   - root directory of the Windows OS installation disk,
   - system directory of the Windows OS,
   - `My documents` folder,
   - temporary directory of the system,
   - temporary directory of the user.

In this mode, **Scanner** uses default values.

Dr.Web Scanner for Windows. Complete scan. In this mode all hard disks and removable disks (including the boot sectors) will be fully scanned. In this mode, **Scanner** uses default values.

Dr.Web Scanner for Windows. Custom scan. In this mode you will be able to choose files and folders to scan. In this mode, the **Scanner** settings window will be opened. Specify scanning parameters and the lists of file system objects to scan (instructions on settings scan parameters are given below) and click **Scan for viruses**.

Dr.Web Enterprise Scanner for Windows. In this mode the scan will be done via the **Dr.Web Enterprise Scanner**. In this mode, the **Scanner** settings window will be opened. Specify scanning parameters and the lists of file system objects to scan (instructions on settings scan parameters are given below) and click **Scan for viruses**.

Dr.Web Enterprise Scanner for Unix. To scan stations which operate under UNIX system-based OS. Specify scanning parameters and the lists of file system objects to scan and click **Scan for viruses**.

Dr.Web Enterprise Scanner for Mac OS X. To scan stations which operate under Mac OS X. Specify scanning parameters and the lists of file system objects to scan and click **Scan for viruses**.

7.5.4. Managing Scanner Settings for Windows® OS

To view and edit Scanner settings, do one of the following:

1. In the main menu of the **Dr.Web Control Center**, select **Network**, then click the name of a station or a group in the hierarchical list. In the opened control menu (panel on the left), click the **Dr.Web Scanner for Windows** item. Scanner settings window opens. This parameters list is the most complete and includes all parameter groups, described below.

2. In the main menu of the **Dr.Web Control Center**, select **Network**, then click the name of a station or a group in the hierarchical list. In the toolbar, click 🔍 **Scan**. In the opened list at the toolbar, select 📇 **Dr.Web Scanner for Windows. Custom scan**. The **Scanner** settings window will be opened on the right pane. This parameter list is shortened and allows to specify only basic settings included in the **General**, **Actions, Log control** and **Miscellaneous** tabs.

3. In the main menu of the **Dr.Web Control Center**, select **Network**, then click the name of a station or group in the hierarchical list. In the toolbar, click 🔍 **Scan**. In the opened list at the toolbar, select 📇 **Dr.Web Enterprise Scanner for Windows**. The **Scanner** settings window will be opened on the right pane. This parameter list is shortened and allows to specify only basic settings included in the **General**, **Actions** and **Excluded paths** tabs.

General Tab

◆ With the **Heuristic analysis** flag set by default, the **Scanner** makes attempts to detect unknown viruses. In this mode the **Scanner** may give false positives though.

◆ The **Check archives** flag is set by default and instructs the **Scanner** to search for viruses in files within archives of different types.

◆ The **Check e-mail files** flag is set by default and instructs to

scan mailboxes.

◆ The **Scan running programs and modules** (**Processes in memory** for the **Enterprise Scanner**) flag is set by default and instructs to scan the processes run in the RAM.

◆ The **Scan programs that run on OS start up** (**Startup processes** for the **Enterprise Scanner**) flag is set by default and instructs to scan the files automatically launched at startup.

◆ The **Scan boot sectors** flag is set by default and instructs 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 **Scan subfolders** flag (it is absent for the **Enterprise Scanner**) is set by default and used in case of scanning the paths. This flag instructs the **Scanner** to scan not only files, but specified nested subfolders.

In case of setting the Scanner parameters via the Dr.Web Scanner for Windows item of the control menu, the following parameters are available:

◆ **Protect the HOSTS system file -** forbid modifications of the HOSTS file. The operating system uses this file when connecting to the Internet. Changes to this file may indicate virus infection.

◆ The **Scan files** item defines the scan mode. Select the mode in the drop-down list:

  • **All files** - scan all files, regardless of their names and extensions.

  • **User masks** - scan only files, which names and extensions are included in the list, specified at the **Mask list** tab.

  • **Selected types** - scan only files, which extensions are included in the list, specified at the **Extensions list** tab.

◆ The **Prompt on any action** flag instructs to show messages about events and **Scanner** action confirmations to the user.

◆ The **Prompt to scan another floppy** flag uses in case of scanning the removable data storages such as floppy or CD/DVD disks, flash drives etc. and instructs to prompt the confirmation for change the current and check the next storage.

In case of setting the Scanner parameters via the Dr.Web Scanner for Windows item of the toolbar, select one of the two alternative modes:

1. **Scan all volumes**.

   For the **Enterprise Scanner**, if **Scan all volumes** is selected, specify what system volumes should be scanned

   - ◆ To scan fixed hard drives, select **Fixed volumes**;
   - ◆ To scan all removable data storages such as floppy or CD/DVD disks, flash drives etc, select **Removable volumes**;

   The paths excluded from search can also be specified in the **Scan all volumes** mode. (Details of path selection are provided below).

2. **Scan specified paths**.

   If **Scan specified paths** is selected, specify the list of scanned paths (how to specify paths is described below);

For the Enterprise Scanner for Windows, also the following flags are available:

- ◆ The **BurstScan technology** flag instructs to use this technology, which considerably increases the scanning speed on modern systems.
- ◆ The **Low priority scan** flag is set by default and ensures lower **Scanner** load on computing recourses of a system. Meanwhile, other processes could have higher priority as compared to when the option is disabled. The load is reduced by dynamical adjustment of thread priorities in the scan process.
- ◆ The **Scan containers** flag instructs the **Scanner** to search for viruses in files within file containers of different types.
- ◆ The **Actions after scan** list instructs to perform specified action automatically when scan completes: shutdown, reboot, set the corresponding mode or do nothing with the station.
- ◆ The **Disable network while scanning** flag instructs to disable network and Internet connections during scanning process.

In the Limitations section, the following settings are available:

◆ **Maximum time for scanning one file** - the maximum file scanning time in milliseconds. When the specified time expires, **Scanner** stops the scan.

◆ **Maximum archive nesting level** - the maximum nesting level for archived files. During scan, **Scanner** proceeds unpacking and scanning the archive until this limit is exceeded.

◆ **Maximum archive size** - if the archive size exceed the limit, **Scanner** neither unpacks, nor scans the archive.

◆ **Maximum compression ratio** - the maximum archives compression rate. If the compression rate of the archive exceed the limit, **Scanner** neither unpacks, nor scans the archive.

◆ **Maximum size of extracted files (KB)** - the maximum file size at unpacking. If the size of extracted files will exceed the limit, **Scanner** neither unpacks, nor scans the archive.

◆ **Compression check threshold** - minimum size of file inside archive beginning from which compression ratio check will be performed.

Actions Tab

On the **Actions** tab, you can configure reactions of **Scanner** to various virus events. For different types of compromised objects, actions are assigned separately.

The following actions for detected virus threats are provided:

◆ **Cure** - instructs **Scanner** to try to restore the original state of an object before infection. If the object is incurable, or the attempt of curing fails, the action set for incurable viruses is applied.

Available for known viruses only except Trojan programs that are deleted on detection, and infected files within complex objectssuch as archives, mail boxes or file containers.

◆ **Delete** - delete the object.

◆ **Quarantine** - move the object to the special **Quarantine**.

◆ **Rename** - rename infected objects according to the rule from the **Pattern used for renaming files** field.

◆ **Report** - report about the detection of a virus (read p. Setting Alerts on how to configure alerts).

◆ **Ignore** - skip the object without performing any action or displaying a notification.

Table 7-3. Reactions of Scanner to various virus events

Action	Object				
	Adware	**Infected archives**	**Infected files**	**Suspicious files**	**Incurable**
Cure			+/*		
Delete	+	+	+	+	+
Quarantine	+	+/*	+	+	+/*
Rename	+	+	+	+	+
Report	+/*	+	+	+/*	+
Ignore	+				

Conventions

+	action is enabled for this type of objects
+/*	action is set as default for this type of object

To set actions on virus threats detection, use the following options:

◆ In the **Pattern used for renaming files** field specify an extension mask applied to renamed files, if you specify **Rename** actions for them. By default, it is #??, i. e. the first character of the extension is replaced with #. The extension can be changed, but standard extensions (EXE, COM, BAT, DOC, PAS, BAS etc.) should not be used instead.

◆ In the **Adware** drop-down list set the **Scanner** reaction to the detection of this type of unsolicited software.

> If you select to **Ignore**, no action is performed as compared to when you select to **Report** user on virus detection, that is, no warning is displayed and detection of an adware program is ignored.

◆ In the same way setting the **Scanner** reaction to the detection of other types of unsolicited software such as

- Dialers;
- Jokes;
- Riskware;
- Hacktools.

◆ In the **Reboot mode** drop-down list, set the mode for restart the computer after the scan.

◆ In the **Infected archives** drop-down list set the **Scanner** 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.

◆ In the **Infected files** drop-down list, set the **Scanner** reaction to the detection of a file infected with a known virus.

◆ The **Suspicious files** drop-down list sets the **Scanner** reaction to the detection of a file presumably infected with a virus (upon a reaction of the heuristic analyzer).

> 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.

◆ The **Incurable files** drop-down list sets the **Scanner** reaction to the detection of a file infected with a known incurable virus (and in case an attempt to cure a file failed).

◆ The **Enable archive deletion** flag allows to delete infected archives and e-mail files. If you set this flag, the **Infected archive** and **Infected e-mail file** lists will contain the **Delete** action. If you clear this flag, only **Quarantine** (by default for archives), **Rename** and **Report** (by default for e-mail files) actions will be acceptable.

Excluded Files and Paths Lists

To edit lists of excluded from scanning files and paths

◆ In an empty line of the **Paths excluded from scanning** or **Files excluded from scanning** list, enter a path to scan for viruses.

◆ To add a new path, click ✚ **Add**, then enter a path in the new line.

◆ To remove a path from the list, click ▬ Remove next to the appropriate line.

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:

1. Direct path in the explicit form to the excluded object. And:

   ◆ 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,

   For example: `C:\Windows` - skip scanning files of the `C:\Windows` folder and all its subfolders.

2. Masks of objects, excluded from the scan. The `?` and the `*` symbols can be used to specify masks.

   For example: `C:\Windows\*\*.dll` - `C:\Windows.` skip scanning all files with the `dll` extension at all subfolders of the `C:\Windows` folder.

3. Regular expression. 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".

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.

Regular expressions briefly described in <u>Appendix K</u>.

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

Extensions List (for setting parameters via the item of the control menu)

To activate the **Extension list** section, set the **Selected types** value for parameter **Scan files** on the **General** tab. Only the files with extensions from this list will be scanned.

While changing extensions list, use the ➕ button to add a new item of a list and the ➖ button to delete present item.

You can use special symbols * and ? in extension list. The list with extensions of executable and archive files are set by default. To restore default values, click the ↩ button.

Mask List (for setting parameters via the item of the control menu)

To activate the **Mask list** section, set the **User masks** value for **Scan files** parameter on the **General** tab. Only the files with names and extensions from this list will be scanned.

While changing mask list, use the ➕ button to add a new item of a list and the ➖ button to delete present item.

You can use special symbols * and ? in extension list. The list with extensions of executable and archive files are set by default. To restore default values, click the ↩ button.

Miscellaneous

At the Miscellaneous tab, set the additional parameters of the **Scanner**:

◆ The **Use disk to make swap file** flag instructs to use the hard drive for swap creation in case of RAM misplace, while scanning large files such as large archives and etc.

◆ The **Restore access date** flag instructs to restore the last date of access to the file after scanning (replace the date on the one before scanning).

◆ The **Auto-save settings** flag instructs to save **Scanner** configuration settings after current session automatically.

◆ In the **Scan priority** list sets thread priorities in the scan process. Select one of the referred:

- **idle** - it is not recommended to set this priority level, to avoid slowing down the **Scanner** operating and considerable increasing of scanning time,

- **lowest**,

- **below normal**,

- **normal** - recommended scan priority,

- **above normal**,

- **highest**,

- **time-critical** - it is not recommended to set this priority level, to avoid intense loading of operating system by the **Scanner** during scan.

Log Control

At the **Log control** tab you can set the parameters of **Scanner** log file. To do this, set the **Write report to file** flag and configure necessary parameters.

Sound Control (for setting parameters via the item of the control menu)

At the **Sound Control** tab you can set the sound files for events of certain types. To do this, set the **Play sounds** flag and specify the names of the sound files for listed events.

7.6. Viewing Statistics

Via the control menu of the **Network** section, you can view the following information:

 ◆ Tables - to view tabular data on anti-virus components functioning at the stations, stations and anti-virus components status.

 ◆ Charts - to view charts with information on infections, detected at the stations.

 ◆ Summary Data - to view and save the reports, that contains all statistic data or selective statistic tables.

 ◆ Quarantine - to view and remotely manage station **Quarantine** contents.

7.6.1. Tables

To view tables:

1. Select the **Network** item in the main menu.

2. Click the name of the station or group in the hierarchical list and select a necessary item in the **Tables** section of the control menu (panel on the left).

The **Tables** section contains the following items:

 ◆ **Summary data** - view and save the reports, that contains all statistic data or selective statistic tables (see Summary data section).

◆ **Infections** - view information on virus events (list of infected objects, viruses, actions, etc.).

◆ **Errors** - view a list of scanning errors on the selected workstation during a certain period.

◆ **Statistics** - view statistics on the operation of anti-virus facilities on a workstation (see Statistics section).

◆ **Start/End** - view a list of components which operated on the workstation.

◆ **Viruses** - view information on viruses detected on a workstation (grouped by type).

◆ **Status** - view information on unusual (and possibly action-demanding) status of the workstation during a certain period (see Status section).

◆ **Jobs** - view the list of tasks set for a workstation during a certain period.

◆ **Full statistics** - view full statistics which is not divided into sessions.

◆ **Virus bases** - view details on the **Dr.Web** virus databases installed including information on the file containing a particular database, virus database version, the total number of virus records in the database, the database creation date.

◆ **Modules** - view detailed information on all **Dr.Web** modules including module description and function, the corresponding executable file, the full module version etc.

◆ **All network installations** - view a list of software installed on a workstation.

> To show hidden items, select **Administration** in the main menu, then select **Configure Dr.Web Enterprise Server** in the control menu. On the **Statistics data** tab, set corresponding flags, then click **Save** and restart the **Server.**

Table 7-4. Correspondence between items of Tables section and flags of Statistics data section

Tables section items	Flags
Infections	Infection in DB

Tables section items	Flags
Errors	Errors of scanning in DB
Statistics	Statistics of scanning in DB
Start/End	Information on the start/end of the components in DB
Viruses	Infection in DB
Status	Station status monitoring
Jobs	Station jobs execution log
Full statistics	Statistics of scanning in DB
Virus Bases	Station status monitoring
	Virus databases monitoring
	Station jobs execution log
Modules	List of the station modules in DB
All network installations	Information about installations in DB

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.

Below are several examples for viewing the statistics via the **Dr.Web Control Center**.

Statistics

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

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

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

2. Select **Statistics** item from the **Tables** section of the control menu (panel on the left).

3. The Statistics window will be opened. The statistics for last 24 hours are displayed by default.

4. To view the data for certain time period, specify the certain time period relatively today in the drop-down list, or select the arbitrary date range on the toolbar. To select the arbitrary date range, enter required dates or click the calendar icons next to the date fields. To load data, click **Refresh**. The tables with statistics will be loaded.

5. In the **Summary statistics** section, the summary data is displayed:

   ◆ if the stations are selected - by selected stations;

   ◆ if the groups are selected - by selected groups. If several groups are selected, only non-empty groups will be displayed;

   ◆ If both the stations and groups are selected - separately by all stations, including stations from selected non-empty groups.

6. To view the detailed statistics of anti-virus components, click the station name in the table. If groups were selected, click the group name in the summary statistics table, then click the station name in the displayed table. A windows (or a section of current window) with detailed statistics will be opened.

7. You can open the settings window of the anti-virus component from the statistic table of station or group components. To do this, click the name of the component in the statistic table.

8. To sort the data in columns of a table, click the certain point (decrease or increase) in the header of the table.

9. 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**.

10. To view the summary statistics not split in sessions, click **Summary statistics** in the control menu. A window of summary statistics will be opened.

11. To view the statistics as a charts, click **Charts** in the control menu. A statistics charts window will be opened (described below).

Status

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

1. On the control menu, in the **Tables** section, select **Status**.

> **i** To show the **Status** item in the control menu, select **Administration** → **Configure Dr.Web Enterprise Server**. On the **Statistics data** tab, clear the **Station Status monitoring** flag, then restart the **Server**.

---

2. Status information displays automatically in compliance with parameters, specified on the toolbar.

3. To view only data of certain severity, specify the severity level by selecting the respective level in the **Severity** drop-down list. 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 of the **Severity** list. In case of excess of this count, situation is rated as critical and it will displays in the **Status** section.

5. You can format the way the data are presented just like in the statistics window above.

> **i** To view operation results and statistics for several workstations, select those workstations in the network catalog.

7.6.2. Charts

Infection Charts

To view general charts with information on detected infections:

1. In the main menu, select **Network**, then in the hierarchical list click the station or group name.

2. In the control menu (left pane), in the **General** section, select **Charts**. This opens a window with the following charts:

   ◆ **Top 10 viruses** - lists top ten widespread viruses that infected the most number of files. The chart displays numerical data on infected objects per a virus.

   ◆ **Daily virus activity** - displays the total number of viruses detected per day at all selected workstations and groups during the selected time period.

   ◆ **Infection classes** - displays numerical data on objects with the specified types of infections.

   ◆ **Infected stations in the group** - displays numerical data on infected stations in each group, that contains such stations.

   ◆ **Infection treatment** - displays numerical data on infected objects which were processed by anti-virus.

3. To view data for a certain time slot, specify it in the drop-down list on the toolbar: view the certain day or month. Or you can select the arbitrary date range. To do this, enter required time and date or click the calendar icons to set the time period and then click **Refresh**.

Total Statistics Charts

Graphical data is displayed in the **Charts** entry of the **General** section and in some entries of the **Table** section.

Depending on the object, selected in the hierarchical list (station or group), different collections of charts are displayed. In the table below, charts and sections of the control menu, in which these charts are displayed, are listed.

**Table 7-5. Correspondence between charts, items
selected in the hierarchical list and sections of the control menu**

Charts	For groups	For stations	Sections
Top 10 viruses	+	+	Infection Viruses Charts
Stations having the maximum of the reported infections	+		Infection
Infection Types	+	+	Viruses
Installations results			All network installations
Average infection activity	+		Statistics
Having the maximum of errors	+	+	Errors
Components errors	+	+	Errors
Job resolutions	+	+	Jobs
Infection classes	+	+	Charts
Infection treatment	+	+	Charts
Daily virus activity	+	+	Charts
The most infected stations of the group	+		Charts

◆ **Stations having the maximum of the reported infections** - displays the list of 10 stations, which are infected by the most number of infected objects. Chart displays numerical data on number of objects, founded at these stations.

◆ **Infection Types** - pie chart, that displays the number of detected infected objects by the type of these objects.

◆ **Installations results** - pie chart, that displays the number of all installations, launched from this **Server**, divided by

installation result. For the failed installations - with error reasons. Chart is displayed for all installations from this **Server**, not depending on the objects, selected in the hierarchical list.

◆ **Average infection activity** - displays average of infection activity at stations from selected group. This value is calculated as a sum of all detected infections divided on number of scanned objects at each station.

◆ **Having the maximum of errors** - displays the list of stations, on which errors of anti-virus components operation are detected. Chart displays the number of errors for each station.

◆ **Components errors** - displays the list of anti-virus components installed at stations, with errors of operation. The pie chart displays the total number of errors for each component.

◆ **Job resolutions** - displays the list of jobs, that have been launched on selected objects. Chart displays the number of launches of jobs.

7.6.3. Summary Data

To view Summary data:

1. In the main menu, select **Network**, then in the hierarchical list click the station or group name. Select **Summary data** item from the **Tables** section of the control menu (panel on the left).

2. The window with report table data will be opened. To include specific data in the report, click **Summary data** on the toolbar and select necessary types in the drop-down list: **Statistics**, **Infections**, **Jobs**, **Start/End**, **Errors**. Statistics from this report sections are similar to statistics from the corresponding items of the **Table** section. To view the report with selected tables, click **Refresh**.

3. To view the data for certain time period, specify the certain time period relatively today in the drop-down list, or select the arbitrary date range on the toolbar. To select the arbitrary date range, enter required dates or click the calendar icons next to the date fields. To load data, click **Refresh**.

4. To save the report 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**.

7.6.4. Quarantine

> ⚠️ To manage the **Quarantine** from the **Server**, stations with **Quarantine** module must be operated by OS, on which the installation of **SpIDer Guard G3** is available (see p. System Requirements).
>
> Otherwise, remote control is impossible. **Quarantine** also will not be able to manage files from the `Infected.!!!` folder and information on **Quarantine** contents will not be sent to the **Server**.

Quarantine Content

Files can be added to the **Quarantine**:

◆ by one of anti-virus components, e.g. **Scanner**,

◆ manually by user via the **Quarantine** Manager.

After moving to **Quarantine**, files are automatically rescanned. This affords:

◆ clarifies the status of infection: presence of infection and its type (because in manual moving to **Quarantine**, information on files infection status is unavailable),

◆ infection names and their type are cast to a common view.

Also, user can rescan files in **Quarantine** via the **Control Center** or via the **Quarantine** Manager at the station.

To view and manage Quarantine files, do the following:

1. Select the **Network** item in the main menu, then click the name of the station or group in the hierarchical list and select **Quarantine** in the control menu (panel on the left).

2. A new window with table that contains **Quarantine** current state opens. If you selected one workstation, a table in the window displays objects in **Quarantine** at this station. If you selected more than one stations or one or more groups, the windows displays a set of tables with quarantined objects for each station.

3. To filter files by time when they were quarantined, set a time slot on the toolbar and click **Refresh**.

4. To manage files in **Quarantine**, set the flag for the corresponding file, group of files or for all files in the **Quarantine** (at the table header). On the toolbar, select one of the following actions:

   ◆ 🔋 - Restore the files from the **Quarantine**.

   > ⚠️ Use this option only then, when you are sure that the objects are not harmful.

   Select one of the options from the drop-down list:

   a) 📦 - Restore the original location of the file, i.e. restore the file to the folder where it had resided before it was moved to the **Quarantine**.

   b) 📁 - Restore the file to the folder specified by the administrator.

   ◆ 🗑 **Remove files** - delete the file from the **Quarantine** and from the system.

   ◆ 🔍 **Scan files** - scan selected in **Quarantine** file one more time.

   ◆ 📤 **Export** - copy and save selected in **Quarantine** files.

   After moving suspicious files to the local **Quarantine** on user's computer, you can copy these files via the **Control Center** and save them via the web browser, e.g. to send files to the **Dr.Web virus laboratory** ulteriorly. For saving, set the flags for the needed files and click **Export**.

◆ Export data about the **Quarantine** state to a file in one of the following formats:

- CSV format,

- HTML format,

- XML format.

7.7. Setting Some of Anti-Virus Components

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

Sections below describe settings of some anti-virus components, which are differ from settings, available at the station.

7.7.1. Configuring Office Control for Access to Resources and Web Sites under Windows® OS

You can centralized restrict access to certain local resources and Web sites. For this, the **Dr.Web Office Control** component is used.

To adjust Office control via the Dr.Web Control Center:

1. To open the settings window select the **Network** item in the main menu, then click the name of the station or group in the hierarchical list and select **Dr.Web® Office Control** in the control menu (panel on the left).

2. Select the blocking settings in the **General** tab and specify resources (files and folders) access to which you wish to restrict:

◆ Set the **Enable blocking** flag to activate blocking of local resources and removable devices.

◆ Set the **Block removable devices** flag to restrict access to removable devices.

◆ Set the **Protect files and folders** flag to restrict access to specified resources. You can specify paths to resources which you wish to block in the **Block access to files** field. To add a new path click the 🞢 button.

> If no path to a restricted file is specified, the default path is used (`%system32%`). For the user, such files are displayed with the `c:\windows\system32` prefix in the **Office Control** settings.

3. On the **Access** tab, set the **WWW filter** flag to configure access to Internet domains. Set the **Block all sites** flag to completely block access to the Internet. List the domains you want to block/allow in the respective fields. To create a new entry click the 🞢 button and specify the necessary value.

In the bottom of the window, set the flags against the content categories you want to block. This flags activate build-in filters which block Web sites from the predefined black lists.

4. Click **Save**, when you finish adjusting the settings. New settings will take effect after confirming the new configuration of a workstation.

Dr.Web Office Control does not allow you to restrict access to the following critical system folders (including their parental folders):

◆ %SYSTEMROOT%

◆ %USERPROFILE%

◆ %PROGRAMFILES%

Note, that you can resctrict access to specific subfolders of these folders.

Dr.Web Office Control cannot restrict access to network resources.

You can allow users to change Parental Control settings (see Setting Users' Permissions for details) and configure access to local resources. **Server** settings have priority over user-defined settings. To update access configuration at the station, connect to **Enterprise Server**, edit and reapply **Office Control** settings for the station.

If you limit access to a critical system folders or enter incorrect path to the resource, **Office Control** settings will be updated at the station, but incorrect access right will be ignored. No warning is displays in case of this error.

7.7.2. Configuring MailD Component for Email Protection Under UNIX® System-Based OS and Mac OS

When running **Agents** under UNIX system-based and Mac OS operating systems, you can specify 15, 30, or 50 email addresses to protect from viruses using the **Dr.Web MailD** component.

To check the maximum number of protected emails addresses, check your **Agent** key file (agent.key).

To specify the list of protected e-mails:

1. Select the workstation or group in the hierarchical list and click **Emails list** in the control menu (panel on the left).

2. In the opened window, enter one email address you want ot protect.

3. To add a new address, click ➕. Each address must be specified in a new line.

4. To remove an address from the list, click ➖ next to the corresponding item.

5. Click **Save** to save changes.

7.8. Sending Notifications to Users

The system administrator may send the users informational messages including:

◆ message text;

◆ hyperlinks to Internet resources;

◆ company logo (or any other graphic presentation);

◆ exact date of message receipt in the title of the window.

These messages are displayed on user's PC as popup windows (see figure).
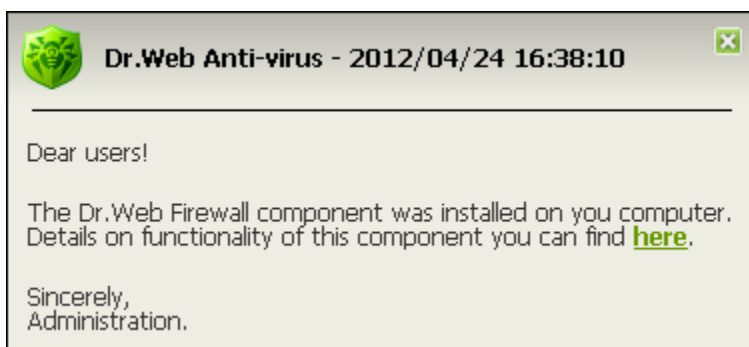
Figure 7-1. Message window on user's PC

To send a message to a user

1. Select the **Network** item in the main menu.
2. Select the workstation or group in the hierarchical list and click the ⭐ **General** → 🖥️ **Send message** button on the toolbar.

Fill in the following fields in the opened window:

◆ **Message text** – an obligatory field containing the message itself.

◆ **Show the company logotype in the message** – set this flag, if you want a graphical object to be displayed in the message window title. To load the file of the object from the local resource, click the **Browse** button to the right of the **Logotype file** field and select the necessary object in the opened file system explorer.

You can also set the title of the message or the company name in the **Name** field. This text will be displayed in the message window title (to the right of the logo). If you leave the field blank, a text about the **Agent** will be displayed in its place instead.

In the **URL** field, specify the link to an Internet resource, witch opens by clicking the logo (also by clicking the message title, if it will be specified in the **Name** field).

If the logo is not set or the size of the logo exceeds the allowable limits (see Logo File Format, p. 3), **Enterprise Agent** logo will be displayed in its place instead.

If the **Show the company logotype in the message** flag is set, the **Use transparency** flag will become active. Set the flag, to apply transparency to the logo image (see Logo File Format, p. 4).

◆ **Show link in the message** – set the flag, to use hyperlinks to web resources in messages to users. To insert a link:

1. In the **URL** field, insert a link to an Internet resource.

2. In the **Text** field, type the name of the link, a text shown instead of the link in the message.

3. In the **Message text** field, put the {link} tag in all places where you want the link to appear. In the resulting message the link with the specified parameters will be shown instead of the tag. You may use an unlimited number of {link} tags in a text, all of them having the same parameters (from the **URL** and **Text** fields correspondingly).

For example:

To send the message displayed in figure 7-1, the following parameters were set for the link:

Message text:

```
Dear users!

The Dr.Web Firewall component was installed
on you computer.
Details on functionality of this component
you can find {link}.


Sincerely,
Administration.
```

URL: `http://drweb.com/`

Text: `here`

◆ **Show delivery status** – set the flag, to be notified of message delivery to the user.

Logo File Format

A file with graphics (logo) inserted in a message should comply with the following requirements:

1. File graphic format: bmp.

2. Bit depth: any (8 - 24 bit).

3. Maximum size of the visible part of a logo: 120x90 px (width x height). Additional 2x2 px are allowed for a border of transparency pixels (see p. 4), i.e. the full maximum size of an image makes up 122x92 px (see figure 7-2).
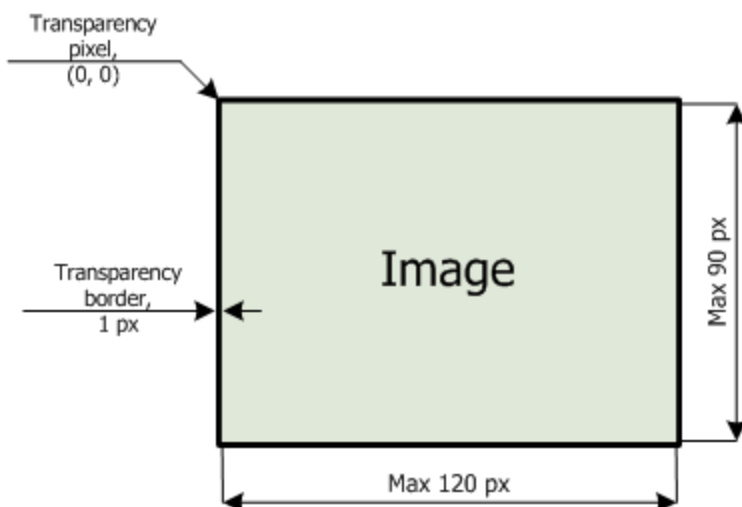
Figure 7-2. Logo file format

4. In case the **Use transparency** option was selected when sending a message, the first pixel in the position (0,0) is

declared *transparent*. All pixels of the same color as the initial color of this pixel will become transparent, the window background will be displayed instead.

If you enable the **Use transparency** option for a rectangular logo, it is recommended to make a rectangular border to avoid erroneous transparency of the pixels of the image itself.

Enabling the **Use transparency** option will be useful in case of a nonstandard (non-rectangular) form of the logo, helping to remove the undesirable background, which supplements the informative part of the image to a rectangular shape. For example, if the image shown in figure 7-3 is used as a logo, the purple background will be removed (become transparent).

Figure 7-3. Nonstandard form Logo

Before sending a message to user(s) (especially to multiple users), it is recommended to send it first to any computer with an installed **Agent** to check the adequacy of the result.

Chapter 8: Configuring the Dr.Web Enterprise Server

8.1. Setting the Dr.Web Enterprise Server Configuration

To set the configuration parameters of the Dr.Web Enterprise Server:

1. Select the **Administration** item in the main menu.
2. Click **Dr.Web Enterprise Server Configuration** in the control menu.
3. A window for setting the **Server** configuration will be opened.

> **i** Values of fields, marked by the * sign, must be obligatory specified.

General Tab

The **Name** parameter sets the name of the **Server**. If it is not specified; the name of the computer where **Enterprise Server** software is installed is used.

The **Threads** parameter sets number of **Server** threads which are serving **Agents**. Change the default setting on advice of the technical support only.

The **DB connections** parameter sets number of database connections with the **Server**. Change the default setting on advice of the technical support only.

The **Authorization queue** parameter sets the maximum number of workstations which can be added to the **Server** authorization queue.

Any natural number is allowed.

In the **Updates bandwidth** drop-down list, the maximal network traffic bandwidth for updates from Server to Agents is set:

◆ If this parameter is set to **Unlimited**, updates for Agents will be transferred without limitation of network traffic bandwidth.

◆ If this parameter is variant from **Unlimited** (has a numerical value), updates for Agents will be transferred in ranges of specified bandwidth of summary network traffic for all Agents updates.

In the **Newbie** drop-down list, the connection policy for new workstations can be set (for more, read p. <u>New Stations Approval Policy</u>). The **Reset unauthorized to newbie** flag instructs to reset the parameters of connection with Server for unauthorized workstations which have not passed authorization check. This option can be helpful when you change Server settings (such as public key) or change the DB. In such cases workstations will not be able to connect to the Server and will need to get the new parameters to assess to the Server.

The **Statistics** flag instructs to send statistics on the operation of **Enterprise Server** for analysis to the Internet server at <u>http://stat.drweb.com/</u>. 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.

To configure statistics via the **Dr.Web Control Center**, use the **Settings** tab.

In the **Encryption** and **Compression** drop-down lists the policy of traffic encryption and compression between **Enterprise Server** and **Enterprise Agents** is selected (for more, read p. <u>Traffic Encryption and Compression</u>).

You can also use the following options:

◆ Set the **Show host name** flag to log host names instead of workstations IP addresses.

◆ Set the **Replace NetBios name** flag to display host names

instead of workstation 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** flags are cleared by default. If the DNS service is not set up properly, enabling these boxes may considerably slow down the **Server** operation. When using any of these options, it is recommended to enable cashing names on the DNS server.

> ℹ️ If the **Replace NetBios name** flag is set and anti-virus network contains the **Proxy server**, when for all stations connected to the **Server** via the **Proxy server**, in the **Dr.Web Control Center**, the name of computer on which the **Proxy server** is installed, will be shown instead of stations names.

◆ **Synchronize the station description** - sets the synchronization of the station description with the description in the **Dr.Web Control Center**. If the station description in the **Dr.Web Control Center** is absent, the user description will be set to this field. If descriptions differ, the description in the **Dr.Web Control Center** will be replaced by the user description.

Statistics Data Tab

On the **Statistics data** tab you can configure statistics information to write in the log file and to the **Server** data base.

To add corresponding type of information to the DB, set the following flags:

◆ **Quarantine** - logs stations **Quarantine** state.

◆ **List of the station modules in DB** - logs the list of the **Anti-virus** modules at the station.

◆ **List of installed components in DB** - logs the list of **Anti-virus** components (**Scanner**, **Monitors**, etc) that are installed at the station.

◆ **Information on the start/end of the components in DB** - logs the information about starting and stopping events of **Anti-virus** components (**Scanner**, **Monitors**, etc) at stations.

◆ **Infection in DB** - logs the statistic data about infections, detected at the stations.

◆ **Errors of scanning in DB** - logs information about all errors, occurring during scanning at the stations.

◆ **Statistics of scanning in DB** - logs the results of stations scanning.

◆ **Information about installations in DB** - logs the information about **Agent** installations at the stations.

◆ **Station jobs execution log** - log results of tasks execution on workstations and store the log in the DB.

◆ **Station status monitoring** - log status changes for workstations and store the log in the DB.

◆ **Virus databases monitoring -** log changes in virus databases status and contents on workstations and store the logs in the DB.

To view statistics information:

1. Select the **Network** option of the main menu.
2. Select a station or a group in the hierarchical list.
3. Open the corresponding section of the control menu (see the table below).

Detailed information about statistic data is described in the Viewing the Statistics section.

The table below describes correspondence between flags in the **Statics data** tab of the **Server** settings and items of the control menu on the **Network** page.

If you clear flags on the **Statistics data** tab, corresponding items of the control menu become hidden.

Table 8-1. Correspondence between flags of Statistics data section and items of the control menu

Server parameters	Menu options
Quarantine	General → Quarantine
List of the station modules in DB	Tables → Modules
List of installed components in DB	General → Installed components
Information on the start/end of the components in DB	Tables → Start/End
Infection in DB	Tables → Infections
	Tables → Viruses
Errors of scanning in DB	Tables → Errors
Statistics of scanning in DB	Tables → Statistics
	Tables → Full statistics
Information about installations in DB	Tables → All network installations
Station jobs execution log	Tables → Jobs
	Tables → Virus Bases
Station status monitoring	Tables → Status
	Tables → Virus Bases
Virus databases monitoring	Tables → Virus Bases

Statistics Tab

On the **Statistics** tab you can configure sending of the statistics on virus events to the **Doctor Web** company.

Set the **Statistics** flag, to activate the sending process. The following fields will become available:

- ◆ **Interval** - an interval in minutes for sending the statistics;
- ◆ **Server** - an IP-address or DNS name and a port of statistics server (by default, `stat.drweb.com:80`);
- ◆ **URL** - a path to the catalog on the statistics server (by

default, `/update/se`);

◆ **ID** - an MD5 key of the **Server** (located in the `enterprise.key` **Server** key file);

◆ **User** - a user name for identification of the sent statistics (contact the **Dr.Web Technical Support Service** for your user name);

◆ **Password** - a password for authentication of the sent statistics (contact the **Dr.Web Technical Support Service** for your password);

◆ **Proxy** - (if necessary) the address of a proxy server for sending the statistics;

◆ **Proxy user** - (if necessary) the name of a user of the proxy server (is not required for anonymous assess);

◆ **Proxy password** - (if necessary) a password to assess the proxy server (is not required for anonymous assess).

Server and **Interval** are the only obligatory fields.

Click **Save**, to accept changes in settings.

Security Tab

On the **Security** tab, restrictions for network addresses from which **Agents**, network installers and other ("neighboring") **Enterprise Servers** will be able to access the given **Server** are set.

To manage **Server** audit log, use the following flags:

◆ **Audit operations** allows to log operations of administrator with the **Dr.Web Control Center** and writing the log into the DB.

◆ **Audit server internal operations** allows to log **Enterprise Server** internal operations and writing the log into the DB.

> ℹ️ To view the audit log, select the **Administration** option in the main menu, then **Audit log** item in the control menu.

The **Agents**, **Installations** 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:

1. Go to the correspondent tab (**Agents**, **Installations** or **Neighbors**).
2. To allow all connections, clear the **Use this ACL** flag.
3. To make the list of allowed or denied addresses, set the **Use this ACL** flag.
4. To allow any TCP address, include it into the **TCP:Allow** or **TCPv6:Allow** list.
5. To deny any TCP address, include it into the **TCP:Deny** or **TCPv6:Deny** list.

To edit the address list:

1. Specify the address in the corresponding field and click **Save**.

2. To add a new field, click the ➕ button in the corresponding section.

3. To delete a field, click ➖.

   The network address is specified as: *<IP-address>*/[*<prefix>*].

> ⓘ Lists for TCPv6 addresses will be available, if the IPv6 interface is installed on the computer.

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.*.*.*`

The addresses not included into any of the lists are allowed or denied depending on whether the **Deny priority** flag is set. If the flag is set, 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 ESS** 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 **Enterprise 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 description will be used by the service detecting the **Server** of **Agents**, etc.

In the **Address** field, specify the address of the interface which **Server** uses for interaction with the **Agents** on the workstations.

In the **Cluster address** field, specify the address of the interface which **Server** uses for interaction with the **Agents** and **Network Installers** while searching for an active **Enterprise Servers**. See the Dr.Web Enterprise Server Detection Service section for more details.

This parameters should be specified in the network addresses format described in Appendix E. The Specification of Network Addresses.

Modules Tab

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

By default, the interaction is enabled for the:

 ◆ **Enterprise Agents**,
 ◆ **NAP Validator** component,
 ◆ **Agent Network Installers**.

The interaction of the **Enterprise Server** with other **Enterprise Servers** is disabled. For a multi-server network configuration (read p. Peculiarities of a Network with Several Dr.Web Enterprise Servers), enable this protocol by setting the correspondent flag.

Location Tab

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

8.1.1. Traffic Encryption and Compression

The **Dr.Web ESS** anti-virus allows encrypting the traffic between **Enterprise Server** and **Enterprise Agents**, between **Enterprise**

Server and the **Network Installer** (**s**), and between **Enterprise 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 ESS** anti-virus. Settings of other components should be compatible with the settings of the **Server**.

To set the encryption and compression policies for the workstations on the Dr.Web Enterprise Server:

1. Select the **Administration** item in the main menu.
2. Click **Dr.Web Enterprise Server Configuration** in the control menu.
3. On the **General** tab, select the necessary variant in the **Encryption** and **Compression** drop-down lists:
   - ◆ **Yes** — enables obligatory traffic encryption (or compression) for all components (is set by default for encryption, if the parameter has not been modified during the **Server** installation),
   - ◆ **Possible** — instructs to encrypt (or compress) traffic with those components whose settings do not prohibit it,
   - ◆ **No** — encryption (or compression) is not supported (is set by default for compression, if the parameter has not been modified during the **Server** installation).

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

Table 8-2 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 8-2. Compatibility of the encryption policy settings

Component settings	Server 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 **Network Installer**-**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.

> ℹ️ By default, **Enterprise 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 **Enterprise Servers**, can be considerable, the **Dr.Web ESS** 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**.

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

8.1.2. Setting the Mode of Operation with Databases

> You can get the structure of the **Enterprise Server** DB via the `init.sql` script, located in the `etc` subfolder of the **Enterprise Server** installation folder.

To specify parameters of operating with the Database:

1. Select the **Administration** item in the main menu.
2. Click **Dr.Web Enterprise Server Configuration** in the control menu.
3. Go to the **Database** tab and select the type of DB in the **Database** drop-down list:

   ◆ **IntDB** – internal DB (a component of **Enterprise Server)**,

   ◆ **MS SQL CE** – external DB, for **Servers** running under Windows OS,

> ⚠ The **MS SQL CE** is a low-production external DB and it is inferior to the internal DB in this parameter.
>
> It is not recommended to use this DB, if more than 30 stations are connected to the **Server**.
>
> But the **MS SQL CE** DB can be successfully used to create reports using API ADO.NET. If you do not need this feature, it is recommended to use an internal DB or any other external DB.

   ◆ **ODBC** (for **Servers** running under Windows OS) or **PostgreSQL** (for **Servers** operated by UNIX system-based OS) – external DB,

   ◆ **Oracle** – external DB (for all platforms except FreeBSD).

> ⚠️ 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**.

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.

> ⚠️ An internal DB can be used, if at most 200-300 stations are connected to the **Server**. If the hardware configuration of the computer with **Enterprise Server** and the load level of other executing tasks are permissible, up to 1000 stations can be connected.
>
> Otherwise, you must use an external DB.
>
> If you use an external DB and more than 10 000 stations are connected to the **Server**, it is recommended to perform the following minimal requirements:
>
> ◆ 3 GHz processor CPU,
>
> ◆ RAM at least 4 Gb for the **Enterprise Server** and at least 8 Gb for the DB server,
>
> ◆ UNIX system-based OS.

> ℹ️ It is possible to perform transactions connected with clearing the database used by **Enterprise 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, open the Server schedule and add a corresponding job.

8.1.3. Setting Alerts

To set the mode of sending alerts about the events connected with the operation of the Dr.Web ESS anti-virus:

1. Select the **Administration** item in the main menu and click **Dr.Web Enterprise Server Configuration** in the control menu.

2. Go to the **Alerts** tab and select the necessary mode of alerts in the **Alert sender** drop-down list:

   ◆ **None** – do not send messages (default mode),

   ◆ **eMail** – send by e-mail,

   ◆ **Windows network message** – send through **Windows Messenger** (for **Servers** under Windows OS only).

E-Mail Notifications

To send notifications by e-mail, specify:

◆ **From** – address of message sender.

◆ **To** – address or addresses of message receivers. To add a new receiver, click .

◆ **SMTP server**, **Port** – address and port of the SMTP server, to send e-mails.

◆ **User**, **Password** (**Enter password again**) – if necessary, set a user name and a password for authorization on the SMTP server.

Set the following flags, is necessary:

◆ **Debug mode** – get detailed log of the SMTP-session.

◆ **Use TLS/SSL encoding** – use *TLS/SSL* encoding to encrypt traffic when sending e-mail notifications.

◆ **Allow plain text authorization** – use *plain text* authentication on mail server.

◆ **Allow CRAM-MD5 authorization** – use *CRAM-MD5* authentication on mail server.

In the **Allowed messages** section, set flags against the events on which the notifications should be sent.

Windows Network Message

⚠️   Windows network message system functions only under Windows OS with Windows Messenger (Net Send) service support.

       Windows Vista OS and later do not support Windows Messenger service.

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

In the **Allowed messages** section, set flags against the events on which notifications should be sent.

To add a new field, click the 🞤 button and enter the computer name; to delete a field, click 🞢.

Message Templates

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 network components. Available variables are listed in Appendix D. The Parameters of the Notification Templates.

It is strongly recommended to use the **Dr.Web Control Center** templates editor for editing the templates. To do this:

1. Select the **Administration** item in the main menu and click **Edit templates** in the control menu.

2. A window for editing templates will be opened. 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.

   To add variables, use drop-down lists in the message header.

3. To save edited template, click **Save**.

⚠ 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**.

8.2. Dr.Web Enterprise Server Logging

Enterprise Server logs the events connected with its operation. Its name is drwcsd.log.

The log file resides by default:

◆ Under **UNIX** OS:

  • for Linux: /var/opt/drwcs/log/drwcsd.log;

  • for FreeBSD and Solaris: /var/drwcs/log/drwcsd.log.

◆ Under **Windows** OS: in the var subfolder of the **Server** installation folder.

It is a plain text file (see Appendix L. Log Files Format).

> i The **Server** log helps to detect the problem in case of an abnormal operation of the **Dr.Web ESS** anti-virus.

8.3. Setting the Dr.Web Enterprise Server Schedule

To schedule tasks for the Dr.Web Enterprise Server via the Dr.Web Control Center:

1. Select the **Administration** item in the main menu and click **Dr.Web Enterprise Server Schedule** in the control menu. The list with the current tasks of the **Server** will be opened.

2. To remove a task from the list, set the flag against it and click **Remove these settings** in the toolbar.

3. To edit a task, select it in the list. This will bring up the **Job editor** window which is described below.

4. To add a new task to the list, click the **New job** item in the toolbar. This will bring up the **New job** window where you should specify necessary parameters described below and click **Save**.

5. You can also enable or disable certain tasks.

6. To export the schedule to a special file, click the button in the toolbar.

7. To import the schedule from a file, click the button in the toolbar.

> i Values of fields, marked by the * sign, must be obligatory specified.

To edit the parameters of a task:

1. On the **General** tab:

   ◆ In the **Name** entry field assign a name to the task, which will be displayed in the schedule.

   ◆ To enable the job, set the **Enable execution** flag.

   To disable the job, clear the flag. The job will remain on the list but will not be executed.

   ◆ The **Critical job** flag instructs to perform the job at next **Enterprise Server** launch, if execution of this job is omitted (the**Enterprise Server** is switched off at the due time). If a task is omitted several times within a certain period of time, then it will be performed only once after the **Enterprise Server** has been launched.

2. On the **Action** tab, 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 in Table 8-3).

3. On the **Time** tab, 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. Editing Scheduled Tasks on a Station above).

4. Click **Save**.

Table 8-3. 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. The name of the procedure must correspond to the name of the executable lua-script (with no extension), located at the `var/extensions` folder of the **Server** installation folder (see also scripts description at the Appendix M).
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.

Type	Description
	Set the **Execute synchronously** flag for the synchronization with **Server** - wait while task finishes before executing other tasks with **Run** type. If the **Execute synchronously** flag is cleared, the **Server** logging only the start of the program. If the **Execute synchronously** flag is set, the **Server** logging the start of the program, the returned code and the time of the program shutdown.
License expiration reminder	Select the period till the license expiration when to execute the task (licenses of **Server** and **Agent** either).
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.
	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 H5.5. 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 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 old stations	Specify the time period (90 days is by default).
	Stations, which do not visit the **Server** during specified period, will be considered outdated and deleted.
Purge old data	Specify number of days after which statistic data about workstations (but not stations themselves) should be considered outdated and be deleted.

Type	Description
	Periods for deleting statistics data for different types of records are set separately.

> ℹ️ 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 network components will be less representative. If you decrease the value, the **Server** may need more resources.

8.4. Administration of the Dr.Web Enterprise Server Repository

8.4.1. Introduction

The *repository* of **Enterprise 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** 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 **Enterprise Server** from the product update site (via HTTP),

> ⚠️ For **Server 5.0** and later versions, updates are not supplied, regardless of repository settings for the **Server** software.

> To upgrade the **Server**, use the installer of corresponding version and make the upgrade procedure according to general rules, described in <u>Upgrading Dr.Web ESS for Windows® OS</u> or <u>Upgrading Dr.Web ESS for UNIX® System-Based Systems</u>.

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

c) from **Enterprise 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 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** repository deals with the following products:

◆ **Enterprise Server**,

◆ **Enterprise Agent** (the **Agent** software and the **Scheduler**, the anti-virus package for workstations),

◆ the **Dr.Web Control Center**,

◆ virus databases.

For more about the repository, please refer to <u>Appendix F. Administration of the Repository</u>.

8.4.2. Checking the Repository State

To check current repository state or update the **Dr.Web Enterprise Security Suite** components, select the **Administration** item in the main menu of the **Dr.Web Control Center** and click **Repository state** in the control menu.

In the opened window, the **Dr.Web Enterprise Security Suite** components list, their last revision date and current state are displayed.

To check updates availability and download available components updates from the **GUS**, click the **Check for updates** button.

8.4.3. Editing the Configuration of the Repository

A repository configuration editor allows to specify the repository configuration parameters common to all products.

> After repository settings have been changed, you must update the repository to change its state according new settings.

To edit the configuration of the repository, select the **Administration** item in the main menu and click **Configure repository** in the control menu.

Dr.Web GUS Setup

On the **Dr.Web GUS** tab, you can set parameters of the **Global Update System**.

The Dr.Web Control Center allows you to:

◆ Remove a server from the list (select one or more servers necessary object, and on the toolbar, click **Remove servers from list** 📱✖).

> **i** To select several elements of the list, press and hold CTRL or SHIFT during selection.

◆ Add a new server to the list (on the toolbar, click **Create server** 📱➕ and select server properties as described below).

◆ Select a proxy server (set the **Use proxy server** flag. Proxy server settings are similar to those of the **Update servers**).

◆ Change the server address and user authorization parameters (click the server icon).

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

To configure the Update servers

1. Click the icon of certain the server.

2. Fill the **Server** entry fields with the server address and the port of the server.

3. Fill in the **User** and the **Password** entry fields. If authorization on the server is not required, leave these fields empty.

4. To save changes in the settings, click **Save**.

You can set a proxy server to access all update servers.

To add the proxy server:

1. Set the **Use proxy server** flag.
2. In the opened window of a proxy-server settings, specify the parameters, that a similar to update server parameters.
3. Click **Add**.
4. Click **Save**.

> ⚠️ Pay attention to the authorization type when you configure a proxy-server.
>
> The current **Dr.Web Enterprise Security Suite** version supports only base HTTP authentication, proxy-HTTP authentication and RADIUS authentication.

If it is necessary to disconnect the update server from the proxy server, clear the **Use proxy server** flag.

Dr.Web Enterprise Agent Update Setup

Configuration of repository update for the **Agent** and anti-virus package software is set separately for different OS versions, on which this software is installed:

◆ On the **Dr.Web Enterprise Agent for Windows** tab in the group of radio buttons, specify whether all components, which are installed on workstations under Windows OS, or virus databases only should be updated.

◆ On the **Dr.Web Enterprise Agent for Unix** tab in the group of radio buttons, specify for which UNIX system-based OS update of components, which are installed on workstations, is required.

Dr.Web Enterprise Server Update Setup

On 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 or none should be updated.

> For **Server 5.0** and later versions, updates from the **GUS** servers are not supplied, regardless of settings of this section.
>
> To upgrade the **Server**, use the installer of corresponding version and make the upgrade procedure according to general rules, described in Upgrading Dr.Web ESS for Windows® OS or Upgrading Dr.Web ESS for UNIX® System-Based Systems.

8.5. Peculiarities of a Network with Several Dr.Web Enterprise Servers

Dr.Web ESS allows to build an anti-virus network with several **Enterprise 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).

8.5.1. Building a Network with Several Dr.Web Enterprise Servers

Several **ESS Servers** can be installed in an anti-virus network. Each **Enterprise 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 ESS allows to connect such anti-virus networks by transferring data between **Enterprise 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 **Enterprise Servers** in case the parent **Enterprise Server** is inaccessible. This will allow the **Agents** connected to a subordinate **Enterprise Server** to receive updated virus databases and program modules. For more, read p. Editing the Configuration of the Repository.

◆ information on virus events, statistics, etc.

The program provides for two types of connections between the Dr.Web Enterprise 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 8-1.

![icon](.)	**Dr.Web Enterprise Server**	─────	TCP, IPX, NetBIOS network
![icon](.)	Protected computer	─────	Transfer of updates via HTTP
![icon](.)	**Dr.Web GUS**	──▶	Sending information on events
		◀───	Interserver transfer of updates
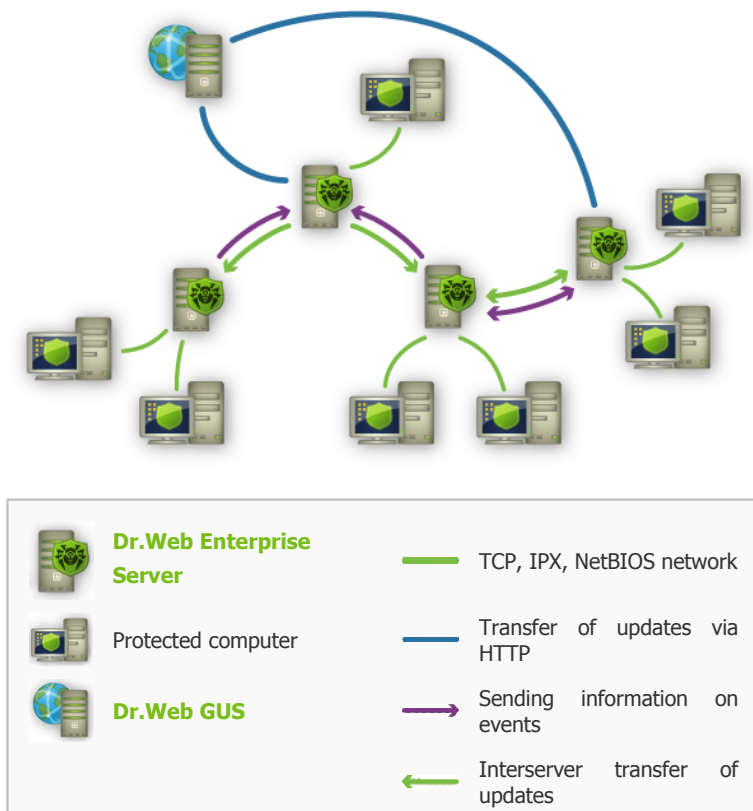
Figure 8-1. A multi-server network

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

◆ receipt of updates from the **Dr.Web GUS** servers by one principle **Enterprise 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 **Dr.Web Control Center** connected to such **Server**.

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

8.5.2. Setting Connections between Several Dr.Web Enterprise Servers

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, each **Server** included into the network connections with any "neighboring" **Servers** ("neighbors" have at least one dataflow between them) should be set up. After that, for each **Server** included into the network, you should set up connections with "neighboring" **Servers** ("neighbors" have at least one data flow between them).

Example: Configure a connection between Parent and Child Dr.Web Enterprise Servers

> Values of fields, marked by the * sign, must be obligatory specified.

1. Make sure that both **Enterprise Servers** operate normally.

2. Make sure that each of the **Enterprise Servers** uses different keys `enterprise.key`.

3. Connect to each of the **Enterprise Servers** by means of the **Dr.Web Control Center** and give them "meaningful" names, as it will help prevent mistakes while connecting and administering the **Enterprise Servers**. You can change the

names through the **Dr.Web Control Center** 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 **Enterprise Servers**, enable the **server** protocol. To do this, on the **Dr.Web Control Center** **Administration** menu, select **Configure Dr.Web Enterprise Server**. On the **Modules** tab, set the **Dr.Web Enterprise Server** flag (see p. Setting the Dr.Web Enterprise Server Configuration).

> **i** If the server protocol is disabled, the message about enabling this protocol will be shown and the link to the corresponding section of the **Dr.Web Control Center** will be given during creation of new connection.

5. Restart both **Enterprise Servers**.

6. Connect the **Dr.Web Control Center** to the Child **Server** (AUXILIARY) and add the Parent **Server** (MAIN) to the list of neighbor **Servers** of the Child **Server**. To do this, select **Neighborhood** item in the main menu. A window with the hierarchical list of the anti-virus network **Servers** "neighboring" with the given **Server** will be opened. To add a **Server** to the list click the **Create neighbor** ![icon] in the toolbar.

A window to describe the connection between the current **Server** and the new **Server** will be opened (see). 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 **View** and specify the drwcsd.pub key of the Parent **Server**. In the **Address** field type the address of the Parent **Server**.

You can browse the list of **Servers**, available in the network. To do this:

   a) Click the arrow on the right of the **Address** field.

b) In the opened window, specify networks in the following format: with a hyphen (for example, `10.4.0.1–10.4.0.10`), separated by a comma with a whitespace (for example, `10.4.0.1–10.4.0.10, 10.4.0.35–10.4.0.90`), with a network prefix (for example, `10.4.0.0/24`).

c) Click ![icon] to browse the network for available **Servers**.

d) Select the **Server** in the list of available **Servers**. Its address will be set to the **Address** field to create connection.

In the **Administrative console web address** field specify the address of a start web page for the **Dr.Web Control Center** of the main **Server** (see p.).

Flags in **Updates** and **Events** sections are set according to *parent-child* type of connection and can not be changed:

◆ main **Server** sends updates to child **Servers**;

◆ main **Server** receives information about events from child **Servers**.

Click **Save**.

Figure 8-2.

As a result, the Parent **Server** (MAIN) will be included to the **Parents** and **Offline** folders (see Figure 8-3).
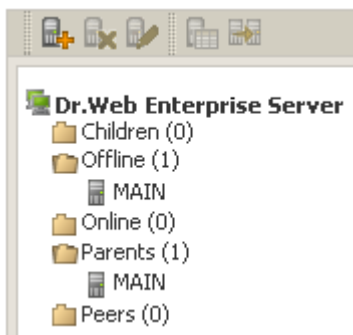

Figure 8-3.

7. Connect the **Dr.Web Control Center** to the Parent **Server** (MAIN) and add the Child **Server** (AUXILIARY) to the list of neighbor **Servers** of the Parent **Server**. To do this, select **Neighborhood** item in the main menu. A window with the

hierarchical list of the anti-virus network **Servers** "neighboring" with the given **Server** will be opened. To add a **Server** to the list click the **Create neighbor** in the toolbar.

In the opened window (see) 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 **View** and specify the drwcsd.pub key of the Child **Server**.

In the **Administrative console web address** field specify the address of a start web page for the **Dr.Web Control Center** of the child **Server** (see p.).

Flags in **Updates** and **Events** sections are set according to *parent-child* type of connection and can not be changed:

- ◆ child **Server** receives updates from main **Server**;
- ◆ child **Server** send information about events to main **Server**.

Click **Save**.

Figure 8-4.

As a result, the Child **Server** (AUXILIARY) will be included to the **Children** and **Offline** folders (see Figure 8-5).
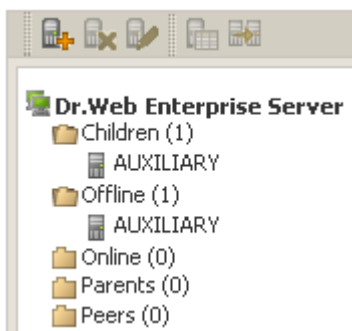

Figure 8-5.

8. Wait until the connection between the **Servers** has been established (usually it takes not more than a minute). Click F5 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 8-6).
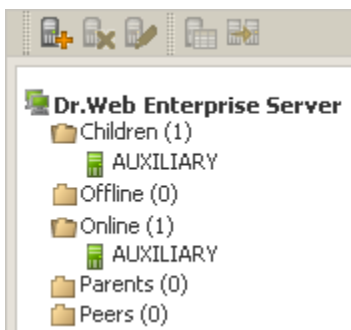
Figure 8-6.

9. Connect the **Dr.Web Control Center** to the Child **Server** (AUXILIARY) to make sure that the Parent **Server** (MAIN) is connected to the Child **Server** (AUXILIARY) (see Figure 8-7).
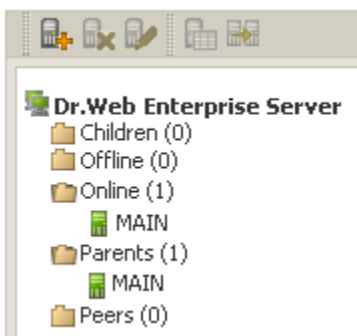

Figure 8-7.

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

You may not connect several **Servers** with the same pare of parameters: password and the drwcsd.pub public key.

> For peer to peer connections between **Servers**, it is recommended to set **Server** address in the settings for one of them only.
>
> It will not take effect on the **Servers** interconnection, but allows to avoid messages like `Link with the same key id is already activated` in the **Servers** log files.

Connection between two Dr.Web Enterprise Servers can be failed because of:

◆ Network problems.

◆ Wrong address of the main **Server** was set during connection setup.

◆ Wrong `drwcsd.pub` encryption public key at one of connecting **Servers**.

◆ Wrong access password at one of connecting **Servers** (passwords on connecting **Servers** are not matched).

◆ The same `enterprise.key` license key on both **Servers**.

◆ License key (`enterprise.key`) of connecting child **Server** matches with the license key of the child **Server** already connected to the main **Server**.

> While creating connections between **Servers**, you can specify update restrictions for the connected **Servers**. To do this, click ⊡ in the **Update restrictions** pane while creating the connection. The window for editing update modes opens. See Update restrictions for details.

8.5.3. Using an Anti-Virus Network with Several Dr.Web Enterprise Servers

The peculiarity of a multi-server network is that updates from the **Dr.Web GUS** servers can be received by a part of **Enterprise 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 Dr.Web Enterprise 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 ESS** 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 Dr.Web Enterprise Servers linked to the current Dr.Web Enterprise Server:

1. Select **Neighborhood** item in the main menu of the **Dr.Web Control Center**.

2. In the opened window in the **Tables** item of the control menu, select the **Summary data** option to view the data on the total number of entries on events at neighbour **Servers**. In the table with statistic data on neighbour **Servers**, the following data is displayed:

    ◆ **Infections** - infections which are detected at stations, connected to the neighbour **Servers**.

    ◆ **Errors** - scanning errors.

    ◆ **Statistics** - statistics on detected infections.

    ◆ **Start/Stop** - the launch and termination of scan tasks.

    ◆ **Status** - status of anti-virus software on stations.

    ◆ **All network installations** - network installations of the **Agent**.

3. To view the page with detailed tabular information on events at neighbour **Servers**, click the number of entries on demand

event at the table in **Summary data** section.

4. Also, to view the page with detailed tabular information on events at neighbour **Servers**, select the corresponding item (see step 2) in the **Tables** section of the control menu.

5. To view the data for certain time period, specify the certain time period relatively today in the drop-down list, or select the arbitrary date range on the toolbar. To select the arbitrary date range, enter required dates or click the calendar icons next to the date fields. To load data, click **Refresh**.

6. 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**.

8.5.4. Using Several Dr.Web Enterprise Servers with One Database

For creation of the anti-virus network with several **Servers** and one DB, the following prescriptions must be implemented:

1. All **Servers** must have the same `drwcsd.pub`, `drwcsd.pri` encryption keys, `certificate.pem`, `private-key.pem` certificates and the `agent.key` **Agent** key file.

2. In the `webmin.conf` **Server** configuration file the same DNS-name of the **Server** must be specified in the `ServerName` parameter for all **Servers**.

3. At the network DNS server, the common cluster name must be registered for each **Server** and load balancing must be set.

4. Each **Server** must have its own `enterprise.key` key file with the `ID1` unique identifier.

5. In the `drwcsd.conf` **Servers** configuration files the same external DB must be specified for all **Servers**.

6. In the **Server** schedule the **Purge Old Data**, **Prepare and send fiscal report periodic job**, **Backup sensitive data**, **Purge old stations**, **Purge expired stations**, **Purge old data**, **Purge unsent IS events** tasks must be specified only for one **Server** (the most productive, if the configuration is differ).

Chapter 9: Updating the Dr.Web Enterprise Security Suite Software and Its Components

> ⚠️ Before updating **Dr.Web ESS** 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**.

> ℹ️ 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. Editing the Configuration of the Repository).

9.1. Upgrading Dr.Web Enterprise Security Suite

9.1.1. Upgrading Dr.Web Enterprise Server for Windows® OS

Two modes of upgrading the **Server** to **6.0.4** version are available:

1. Automatic. Upgrading the **Server** of **5.0** and **6.0.0** versions can be done automatically by using the installer.

> ⚠️ Automatic upgrade is supported for **Servers** with the same bitness only.

> In other cases, it is necessary to delete the old **Server** and install the new **Server** manually.

2. Manual. To upgrade **Server** software of **4.XX**, **6.0.2** and later versions, delete **Server** software of current versions and install the new **Server**.

Saving Configuration Files

During deleting of the **Server** manually or upgrading by using the installer, the following files will be backed up automatically:

File	Description	Default folder
dbinternal.dbs	internal database	var
drwcsd.conf (the name may vary)	**Server** configuration file	etc
drwcsd.pri	private encryption key	
drwcsd.pub	public encryption key	• Installer • webmin\install
enterprise.key (the name may vary)	**Server** license key file	etc
agent.key (the name may vary)	**Agent** license key file	
certificate.pem	SSL certificate	
private-key.pem	RSA private key	

If necessary, copy other critical files you want to preserve to another folder, other than **Server** installation folder. For instance, copy the **Dr.Web Control Center** configuration file (webmin.conf) and report templates which are stored in the \var\templates folder.

Saving Database

Before upgrade **Dr.Web Enterprise Security Suite** software, it is recommender to backup database.

To backup database:

1. Stop the **Server**.
2. Export DB to the file:
```
"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 <backup_folder>\esbase.es
```

For **Servers** with external DB, it is recommended to use standard tools supplied with the database.

> ⚠ Make sure, that **Dr.Web ESS** DB export completed successfully. If DB backup copy is not available, the **Server** could not be restored in emergency case.

Important Notes

> ⚠ Starting from version **5.0** anti-virus package includes **SpIDer Gate** and **Office Control** components. For using this components, they must be included in you license **(Antivirus+Antispam)**. If you license does not include this components, it is recommended to perform the actions described below.
>
> If the **Agent** with an active self-protection is installed on **Sever** computer, the wizard prompts you to disable **Dr.Web SelfPROtect** during update process. Disable self-protection in the **Agent** settings to continue updating the **Server**.

If you are using the ODBC for Oracle as an external database, select the **Custom** option and in the opened window disable the installation of Oracle client in the **Database support** - **Oracle database driver** section in the installer settings during the **Server** upgrading (or reinstallation).

Otherwise, Oracle DB functioning will fail because of the libraries conflict.

Automatic Upgrading Dr.Web Enterprise Server from 5.0 and 6.0.0 Versions

Dr.Web Enterprise Server can be upgraded from **5.0** and **6.0.0** versions to version **6.0.4** automatically by using the installation wizard.

To upgrade the Dr.Web Enterprise Server to version 6.0.4 run the installation file and follow instructions of the Wizard

1. The **Dr.Web Enterprise Server Upgrade Notes** window displays, which notifies you on the previous **Enterprise Server** version installed. The installation wizard locates the **Server** installation folder automatically.

2. On the following steps, the wizard displays locations of the preserved files (see above) which will be used during installation of the **6.0.4 Server**. You can change locations if necessary.

   For the external **Server** database, also select **Use existing database** during upgrade. After subsequent selection of existing **Server** configuration file and private encryption key, a further update will be proceeded automatically.

3. To remove the previous version and launch the installation process, click **Install**.

> During upgrade of the **Server** software, contents of the repository are removed and new version is installed.

> If after **Server** upgrade from the **5.0** and earlier versions, the repository has not been removed, it is necessary to remove its contents and renew it manually.

> For a network with several **Severs**, from the main **Server** with **6.0.4** version to child **Servers** with **5.0** and earlier versions, only virus bases are transmitted.
>
> To transmit all software and **Agent** updates, upgrade child **Servers** to **6.0.4** version (for repositories compatibility).

After upgrading of Dr.Web Enterprise Server to 6.0.4 version:

Do the following to ensure normal operation of **Dr.Web Control Center**:

1. Clear cache of the Web browser that is used to connect to **Dr.Web Control Center**.
2. Upgrade the **Dr.Web Browser-Plugin**.

Manual Upgrading Dr.Web Enterprise Server from 4.XX, 6.0.2 and Later Versions

Dr.Web Enterprise Server does not support upgrade from **4.XX** versions or **6.0.2** and later versions to **6.0.4** version automatically. To upgrade **Server**, delete the current **Server** software and install the new **Server**.

> ⚠️ In case of upgrade from **4.XX** version, if your licence on anti-virus software of **6.0.4** version does not include **SpIDer Gate** and **Office Control** components **(Antivirus +Antispam)**, it is recommended to perform the actions described below.

To upgrade the Dr.Web Enterprise Server, do the following

1. Stop the **Server** (see Start and Stop the Dr.Web Enterprise Server).
2. In case of using external DB, save DB via SQL server loots.

3. If you plan to use any files (besides files which are copied automatically during **Server** uninstall at step **4**), backup these files manually. For instance, copy the report templates to a backup folder.

4. Remove the **Enterprise Server** software.

5. Install new **Server** (see p.).

   In case of using external DB, specify to create a new DB.

   In case of using internal DB, specify saved `dbinternal.dbs` file.

6. Stop the **Server** (see).

7. In case of manual backup, replace the files in the same folders from which you copied the files before new install.

8. In case of using external DB, restore the DB on the new **Server** and specify the path to this DB in the configuration file `drwcsd.conf`.

   Run the `drwcsd.exe` with `upgradedb` switch for DB upgrading. The command line will look as follows:

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

9. Start the **Server** (see).

*In upgrading procedure of Dr.Web Enterprise Server from
4.XX version to 6.0.4 version, it is recommend to do the
following:*

1. Before upgrading disable the use of communication protocols
   with **Enterprise Agent** and the **Network installer**. To do
   this, select the **Administration** item in the main menu and
   click **Configure Dr.Web Enterprise Server** in the control
   menu, go to the **Modules** tab and clear the **Protocol Dr.Web
   Enterprise Agent** and the **Protocol Dr.Web Network
   Installer** flags. Click **Save**. A request to restart the **Server**
   will be opened. Click **Yes**.

2. Upgrade the **Server** to version **6.0.4** as described above
   (using preserved **Server** configuration file).

3. After upgrading the **Server**, configure the set of components
   installed at the workstations (see p. Anti-Virus Package
   Composition), in particular if you do not have **Antispam**
   license, the **cannot** option for the **SpIDer Gate** and **Office
   Control** components must be set.

4. Update the components of **Dr.Web ESS**. To do this, select
   the **Administration** item in the main menu and click
   Repository state in the control menu. In the opened window
   click **Check for updates**. Beforehand configure the proxy
   servers settings for **GUS** updating if necessary.

5. If necessary, configure ports that is using by the **Agents** for
   communication with the **Server**. To do this, use the
   **Administration → Configure Dr.Web Enterprise Server
   → Transport** tab.

6. Enable the use of communication protocols with **Enterprise
   Agent** and the **Network installer**, disabled at step **1**.

7. Upgrade the workstations software.

> ⚠️ After the **Server** upgrading from the **4.XX** version to **6.0.4**
> version, the `transport` parameter must be present in
> the `drwcsd.conf` configuration file of the **Server**:
>
> ```
> Transport   "drwcs"  "tcp/0.0.0.0:2193"
> "udp/231.0.0.1:2193"
> ```

where the `drwcs` is a **Server** name.

If this parameter is not specified, add it manually and restart the **Server**.

9.1.2. Upgrading Dr.Web Enterprise Server for UNIX® System-Based OS

Upgrading the **Server** software over the previous version is possible not for all UNIX system-based OS. Thus, under UNIX system-based OS, in which upgrading is not supported, it is recommended to delete the **Server** software of previous versions and install the **6.0.4** version.

Saving Configuration Files

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

File	Description	Default folder
`dbinternal.dbs`	internal database	• for Linux OS: /var/opt/drwcs/ • for Solaris and FreeBSD OS: /var/drwcs/
`drwcsd.conf` (the name may vary)	**Server** configuration file	• for Linux OS: /var/opt/drwcs/etc • for Solaris and FreeBSD OS: /var/drwcs/etc
`webmin.conf`	**Dr.Web Control Center** configuration file	
`common.conf`	configuration file (for some UNIX system-based OS)	
`enterprise.key` (the name may vary)	**Server** license key file	
`agent.key` (the name may vary)	**Agent** license key file	
`certificate.pem`	SSL certificate	
`private-key.pem`	RSA private key	

File	Description	Default folder
drwcsd.pri	private encryption key	
drwcsd.pub	public encryption key	for Linux and Solaris OS: • /opt/drwcs/Installer/ • /opt/drwcs/webmin/ install for FreeBSD OS: • /usr/local/drwcs/ Installer/ • /usr/local/drwcs/ webmin/install

Saving Database

Before upgrade **Dr.Web Enterprise Security Suite** software, it is recommender to backup database.

To backup database:

1. Stop the **Server**.
2. Export DB to the file:
    *   For FreeBSD OS:
        ```
        # /usr/local/etc/rc.d/drwcsd.sh exportdb /
        var/drwcs/etc/esbase.es
        ```
    *   For Linux OS:
        ```
        #   /etc/init.d/drwcsd   exportdb   /var/opt/
        drwcs/etc/esbase.es
        ```
    *   For Solaris OS:
        ```
        #   /etc/init.d/drwcsd   exportdb   /var/drwcs/
        etc/esbase.es
        ```

For **Servers** with external DB, it is recommended to use standard tools supplied with the database.

Make sure, that **Dr.Web ESS** DB export completed successfully. If DB backup copy is not available, the **Server** could not be restored in emergency case.

Important Notes

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

During **Server** update to **6.0.4** version from **5.0** and earlier versions, it is necessary to delete the repository and install the new repository.

For a network with several **Severs**, from the main **Server** with **6.0.4** version to child **Servers** with **5.0** and earlier versions, only virus bases are transmitted.

To transmit all software and **Agent** updates, upgrade child **Servers** to **6.0.4** version (for repositories compatibility).

Starting from version **5.0** anti-virus package includes **SpIDer Gate** and **Office Control** components. For using this components, they must be included in you license (**Antivirus**+**Antispam**). If you license does not include this components, it is recommended to perform the actions described below.

Automatic Upgrade

If you update the **Server** from **5.XX** version to **6.0.4** version for **Linux** OS, instead of deleting old version and installing new version of the **Server**, you can use the following commands to update the **Server**:

- ◆ for **rpm**: rpm -U *<package_name>*
- ◆ for **dpkg**: dpkg -i *<package_name>*
  for upgrading deb packages, the /root/drwcs catalog must be empty or absent.

All automatically saved <u>files</u> will be stored in corresponding directories and manual replacement is not required.

During upgrade of package for **rpm** distribution kits of **5.0** or **6.0 Server**, if before **Server** upgrade, the `webmin.conf` **Control Center** configuration file had been changed, the `webmin.conf` file is saved form the old version, and the new file is created with the `webmin.conf.rpmnew` name.

If you want to use functional, provided by changed parameters of configuration file (and also, the **Agent** installer could be available at <u>http://<*server_name*>:9080/install</u> page, see <u>Installation Files</u>), copy all changed settings from the old file to the new file and rename the `webmin.conf.rpmnew` new file to the `webmin.conf` with replace.

Manual Upgrade

If using an internal database:

1. Stop the **Enterprise Server**.

2. If you plan to use any files (besides <u>files</u> which are copied automatically during **Server** uninstall at step **4**), backup these files manually. For instance, copy the report templates to a backup folder.

3. Remove the contents of the repository.

4. Remove **Enterprise Server** software (see <u>Uninstalling the Dr.Web Enterprise Server Software for UNIX system-based OS</u>). You will be prompt to create backup copies, for this specify a folder where to store the backup or accept the default folder.

5. Install **Enterprise Server** version **6.0.4** (see <u>Installing the Dr.Web Enterprise Server for UNIX system-based OS</u>).

6. After new install, you can replace automatically created files with the backup copies from the previous installation. In case of automatic backup, replace the files in the following folders:

Files	Paths under OSes		
	Linux	**Solaris**	**FreeBSD**
drwcsd.pub	/opt/drwcs/Installer/		/usr/local/drwcs/Installer/
	/opt/drwcs/webmin/install		/usr/local/drwcs/webmin/install
dbinternal.dbs	/var/opt/drwcs/	/var/drwcs/	
drwcsd.conf drwcsd.pri enterprise.key agent.key certificate.pem private-key.pem	/var/opt/drwcs/etc	/var/drwcs/etc	

> ⚠ **Dr.Web Control Center** configuration file
> (`webmin.conf`) of versions, that is earlier than **6.0.2**, is
> not compatible with the **6.0.4** version software. After
> upgrading the **Server** of version, that is earlier than **6.0.2**,
> you cannot replace a new configuration file with a backup
> copy of the **4.XX** configuration file and have to make all
> necessary changes manually.

In case of manual backup, replace the files in the same folders
from which you copied the files before new install.

> ⚠ For all backup files from the previous **Server** version (see
> step **6**) assign the user, selected at the installation of the
> new **Server** version (**drwcs** by default), as files owner.

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

8. Launch **Enterprise Server**.

9. Set up repository upgrade and perform the upgrade.

10. Restart the **Server**.

If using an external database:

1. Stop **Enterprise Server**.

2. If you plan to use any files (besides [files](#) which are copied automatically during **Server** uninstall at step **4**), backup these files manually. For instance, copy the report templates to a backup folder.

3. Remove the contents of the repository.

4. Remove **Enterprise Server** software (see the [Uninstalling the Dr.Web Enterprise Server Software for UNIX system-based OS](#) section). You will be prompt to create backup copies, for this, specify a folder where to store the backup or accept the default folder.

5. Install **Enterprise Server** version **6.0.4** (see p. [Installing the Dr.Web Enterprise Server for UNIX system-based OS](#)).

6. Move the automatic saved files (see [above](#)) to:

   ◆ for **Linux** OS: to `/var/opt/drwcs/etc`, except for the public key. The latter must be saved to `/opt/drwcs/Installer/` and to `/opt/drwcs/webmin/install`

   ◆ for **FreeBSD** OS: to `/var/drwcs/etc`, except for the public key. The latter must be saved to `/usr/local/drwcs/Installer/` and to `/usr/local /drwcs/webmin/install`

   ◆ for **Solaris** OS: to `/var/drwcs/etc`, except for the public key. The latter must be saved to `/opt/drwcs/Installer/` and to `/opt/drwcs/webmin/install`

   In case of manual backup, replace the files in the same folders from which you copied the files before new install.

For all backup files from the previous **Server** version (see step **6**) assign the user, selected at the installation of the new **Server** version (**drwcs** by default), as files owner.

7. To upgrade the databases, execute the following commands:

   - for **Linux** OS and **Solaris** OS:

     ```
     /etc/init.d/drwcsd upgradedb
     ```

   - for **FreeBSD** OS:

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

8. Launch **Enterprise Server**.

9. Set up repository upgrade and perform the upgrade.

10. Restart the **Server**.

In upgrading procedure of the Dr.Web Enterprise Server to version 6.0.4, it is recommend to do the following:

1. Before upgrading disable the use of communication protocols with **Enterprise Agent** and the **Network installer**. To do this, select the **Administration** item in the main menu and click **Configure Dr.Web Enterprise Server** in the control menu, go to the **Modules** tab and clear the **Protocol Dr.Web Enterprise Agent** and the **Protocol Dr.Web Network Installer** flags. Click **Save**. A request to restart the **Server** will be opened. Click **Yes**.

2. Upgrade the **Server** to version **6.0.4** as described above (using preserved **Server** configuration file).

3. After upgrading the **Server**, configure the set of components installed at the workstations (see p. Anti-Virus Package Composition), in particular if you do not have **Antispam** license, the **cannot** option for the **SpIDer Gate** and **Office Control** components must be set.

4. Update the components of **Dr.Web ESS**. To do this, select the **Administration** item in the main menu and click **Repository state** in the control menu. In the opened window click **Check for updates**. Beforehand configure the proxy servers settings for **GUS** updating if necessary.

5. If necessary, configure ports that is using by the **Agents** for

communication with the **Server**. To do this, use the
**Administration → Configure Dr.Web Enterprise Server
→ Transport** tab.

6. Enable the use of communication protocols with **Enterprise Agent** and the **Network installer**, disabled at step **1**.

7. Upgrade the workstations software.

The upgraded anti-virus program is ready for operation.

> ⚠️ After the **Server** upgrading from the **4.XX** version to **6.0.4** version, the transport parameter must be present in the drwcsd.conf configuration file of the **Server**:
>
> Transport   "drwcs"   "tcp/0.0.0.0:2193"
> "udp/231.0.0.1:2193"
>
> where the drwcs is a **Server** name.
>
> If this parameter is not specified, add it manually and restart the **Server**.

9.1.3. Upgrading Dr.Web Browser-Plugin

To upgrade **Dr.Web Browser-Plugin** (is used by the **Dr.Web
Control Center**), delete **Dr.Web Browser-Plugin** software of
current versions and install the new version.

Deletion of the the **Dr.Web Browser-Plugin** is described in the
Uninstalling the ESS Software for Windows® OS or Uninstalling the
Dr.Web Enterprise Server Software for UNIX® System-Based OS
sections.

Installation is described in the Installing the Dr.Web Browser-Plugin
section.

9.1.4. Upgrading Dr.Web Enterprise Agent

After upgrading **Server** software, **Agents** connected to this **Server** will be upgraded automatically.

> Recommendations on upgrading the **Agents**, installed at the stations that implement significant LAN functions, specified in the Upgrading Dr.Web Enterprise Agents on the LAN servers section.

9.1.5. Upgrading Proxy Server

Upgrading Proxy Server for Windows OS

Automatic update of **Proxy server** is not supported.

When you run the installer on a PC with installed **Proxy server**:

◆ If the installer has the same bit depth as an installed **Proxy server**, notification about impossibility of installation is shown.

◆ If the bit depth of installer differs from bit depth of installed **Proxy server**, the **Proxy server** is installed in the folder different from the folder of installed version.

> Installation of two **Proxy servers** on the same PC and configuring them to operate via the same port leads to inoperability of both **Proxy servers**.

To upgrade Proxy server:

1. If on a computer with installed **Proxy server**, the **Agent** with enabled self-protection is installed, disable the **Dr.Web SelfPROtect** component via the **Agent** settings.

2. Uninstall the **Proxy server** according to the standard procedure (see Removing Proxy Server).

> ⚠️ During **Proxy server** uninstallation, the `drwcsd-proxy.xml` configuration file is deleted. If necessary, save configuration file manually before **Proxy server** uninstallation.

3. Install a new version of **Proxy server** according to the standard procedure (see Installing Proxy Server).

4. If necessary, replace configuration file with manually saved one from the previous version.

5. If you disabled the **Dr.Web SelfPROtect** component at step 1, enable it via the **Agent** settings.

Upgrading Proxy Server for UNIX System-Based OS

To upgrade Proxy server, perform the following:

For Proxy server under		Command
FreeBSD OS Solaris OS		Perform uninstallation and repeated installation according to the standard procedures, described in Removing Proxy Server and Installing Proxy Server.
Linux OS	deb package	`dpkg -i drweb-esuite-proxy`
	rpm package	`rpm -U drweb-esuite-proxy`
	generic package	Unpack installation package with the following command: `tar -xjf` *<distribution_file>*`.tar.bz2` After that, replace files from the **Proxy server** installation folder with files from unpacked archive manually.

9.2. Manual Updating of the Dr.Web ESS Components

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

Checking for Updates

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

1. Select the **Administration** item in the main menu and click **Repository state** in the control menu.

2. In the opened window information about all components are listed, also last revision date and its current state is specified. Click **Check for updates**.

3. 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).

4. After the check updated components will have current date in the **Last revision since** column.

Updating the Software

To update the software of an anti-virus station through the Dr.Web Control Center

1. Select the **Network** item in the main menu, then click the name of the station or group in the hierarchical list.

2. In the toolbar, click 🧊 **Managing Components**. In 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;

◆ 🟢 **Update all components** instructs to force the update of all components, including those updated successfully.

ⓘ After forced update of all components, two reboots of a station required. Follow the **Agent** instructions.

The same operation can be carried out with the help of **Enterprise Agent**.

To update the software of an anti-virus station through the Dr.Web Enterprise Agent

1. Permit the user of the given workstation to change the local policy (for information on how to do it, read p. <u>Setting Users' Permissions</u>).

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.

Critical Updating Error

In case of a critical error occurs during the operation of Dr.Web Enterprise Agent

1. Initiate a forced update of the workstation (see p. <u>Manual Updating of the Dr.Web ESS Components</u>).

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** installation folder.

3. Remove the cause of the error.

4. Run a forced update of the workstation again.

9.3. Scheduled Updates

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

To schedule product updates on the Dr.Web Enterprise Server:

1. Select the **Administration** item in the main menu and click **Dr.Web Enterprise Server Schedule** in the control menu. The list with the current tasks of the **Server** will be opened.

2. To add a task, click 🎁 **New job** in the toolbar.

3. In the opened window assign a name to the task in the **Name** field.

4. Go to the **Action** tab and select the **Update** action in the drop-down list.

5. In the drop-down list, select the component 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

   ◆ **All Dr.Web Enterprise Products**, if you want to set a task for updating all **Dr.Web ESS** components.

⚠️ For **Server 5.0** and later versions, updates from the **GUS** servers are not supplied.

To upgrade the **Server**, use the installer of corresponding version and make the upgrade procedure according to general rules, described in Upgrading Dr.Web ESS for Windows® OS or Upgrading Dr.Web ESS for UNIX® System-Based Systems.

6. Go to the **Time** tab and 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. Editing Scheduled Tasks on a Station above).

7. Click **Save** to accept the changes.

9.4. 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 **ESS Server**, which has been updated normally.

This way is not meant for upgrading.

For **Server 5.0** and later versions, updates for the **Server** itself from the **GUS** servers are not supplied.

To upgrade the **Server**, use the installer of corresponding version and make the upgrade procedure according to general rules, described in Upgrading Dr.Web ESS for Windows® OS or Upgrading Dr.Web ESS for UNIX® System-Based Systems.

To update the anti-virus software, do the following:

1. Install the anti-virus **Server** software on another computer connected to the Internet as described in p. Installing the Anti-Virus Server.

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. Fully replace the content of repository catalog on the main (working) **Server** by the content of correspondent catalog of the **Server** connected to the Internet. Usually it is:

   ◆ `var\repository` under **Windows** OS,

   ◆ `/var/drwcs/repository` under **FreeBSD** OS and **Solaris** OS,

   ◆ `/var/opt/drwcs/repository` under **Linux** OS.

> ⚠️ If the **Agent** with an active self-protection is installed on **Sever** computer, you must disable **Dr.Web SelfPROtect** component in the **Agent** settings before starting the repository update.

5. If the main **Server** is runing 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**.

> ⚠️ If **Dr.Web SelfPROtect** component was disabled before the repository update, it is recommended to enable this component after updating.

9.5. Update Restrictions for Workstations

Via the **Dr.Web Control Center** you can enable or disable the update mode for **Dr.Web ESS** at workstations in particular time slots. To do this:

1. Select the **Network** item in the main menu, then click the name of a station or group in the hierarchical list and select **Update restrictions** in the control menu (panel on the left).

2. In the opened table, the update mode is specified using the following colors:

    ■ green - update is enabled,

    ■ red - update is disabled.

    The restrictions are set separately for each 15 minutes of each day of the week.
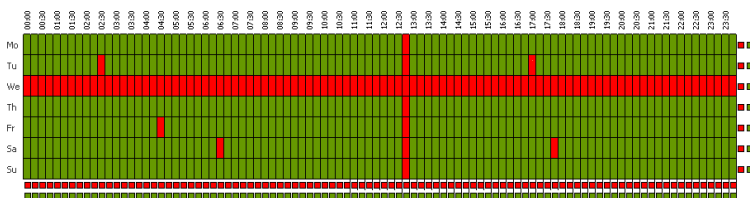
3. To change the update mode, click the corresponding block of the table.

    To change the update mode for a row (full day), click the corresponding color in the right part of the table row.

To change the update mode for a column (a particular 15 minutes interval of each day of the week), click the corresponding color under the table column.

4. After editing, click **Save** to accept changes.

In the toolbar, the following options are available:

 Propagate these settings to another object - copy the update settings of the current station or group to the settings of other station or group.

 Remove these settings - set the update settings to the default values (all updates are enabled).

 Export shown settings to file - save the update settings in a file of special format.

 Import settings from file - load the update settings from a file of special format.

9.6. Updating Mobile Dr.Web Enterprise Agents

If your computer (laptop) has no connection to the **Enterprise 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 →
Enabled**. 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 permissions (for more, read p. Setting Users' Permissions).

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

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, set the **Only when connected to Internet** flag.

When using a proxy server, set the **Use proxy to transfer updates** flag 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**.

The **Start update** option is disabled, if connection to the **Server** is active.

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

9.7. Replacing Old Key Files with New Ones

During the installation of the **Dr.Web ESS** anti-virus you will be asked to provide files containing the **Server** key and the key for workstations (read p. Installing the Dr.Web Enterprise Server; 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 ESS** anti-virus, you should obtain and import new key files.

There are two ways to install new key files which depend on whether the `ID` parameter in the new key file is the same as the previous key file. Open both key files (`enterprise.key`) with a text editor, find the `[Enterprise]` section and compare the values in the `ID1` parameter.

> ⚠️ The key file has a write-protected format using a digital signature. Editing the key file makes it invalid. To avoid this, do not modify the key file and/or save it when closing the text editor.
>
> If the **Agent** with an active self-protection is installed on **Sever** computer, you must disable **Dr.Web SelfPROtect** component in the **Agent** settings before replacing a key files.

The Same ID1 Parameters

> ℹ️ To specify the new key files for the anti-virus network components, use the License Manager.

To install new key files in Dr.Web ESS:

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 **Dr.Web Control Center**).
3. Import the new **Agent** key for the **Everyone** group. To do this, in the catalog of the anti-virus network select the **Everyone** group, and click ⭐ **General** → 🔑 **Import key** in the toolbar.

4. In the next window select the new key file for workstations (agent.key) and click **OK**.

Different ID1 Parameters

To install new key files in Dr.Web ESS:

1. Disable the protocols of the **Agent** and **Network Installer**. To do this, select the **Administration** item in the main menu and click **Configure Dr.Web Enterprise Server** in the control menu, go to the **Modules** tab and clear the **Protocol Dr.Web Enterprise Agent** and the **Protocol Dr.Web Network Installer** flags. Click **Save**. A request to restart the **Server** will be opened. Click **Yes**.

2. Export the **Enterprise Server** timetable. To do this, select the **Administration** item in the main menu and click **Dr.Web Enterprise server schedule** in the control menu. Click   **Export shown settings to file** in the toolbar.

3. To free space in the database, remove the **Enterprise Server** schedule. To do this, select the **Administration** item in the main menu and click **Dr.Web Enterprise server schedule** in the control menu. Click **Remove these settings** in the toolbar.

4. In case of a multi-server network:

   a) If you need to save statistic information of neighbour **Servers**, you must export statistic tables, because after connections deletion this information will be lost.

   b) Remove all interserver connections. This can be done via the **Administration** menu → **Neighborhood** item.

5. Specify the new key files for the anti-virus network components:

   ◆ Use the License Manager.

   ◆ To replace keys manually, use the procedure described above.

6. Enable the protocols of the **Agent** and **Network Installer** which were disabled in step **1**.

7. Set up a new schedule for the **Server** or import the old one

which was exported in step **2**.

8. In case of a multi-server network, set up all the necessary interserver connections which were removed in step **4**.

9. Restart the **Server**.

Chapter 10: Configuring the Additional Components

10.1. Proxy Server

The anti-virus network may consist of one or several **Proxy servers**.

The main function of a **Proxy server** is to establish a connection between **Enterprise Server** and **Enterprise Agents** in cases when it is impossible to set up direct access (e.g. if **Enterprise Server** and **Enterprise Agents** are located in separate networks which do not have packet routing between them).

General Functions

A proxy server performs the following functions:

1. Network listening and receipt of connections according to the specified protocol and port.
2. Protocol translation (supported protocols: TCP/IP, IPv6, IPX and NetBIOS).
3. Data transmission between **Enterprise Server** and **Enterprise Agents** according to the **Proxy server** settings.
4. Caching of **Agent** and anti-virus package updates, which are translated by the **Server**. In case of using cache of the **Proxy server** to translate updates, following are provided:
   ◆ reducing of network traffic,
   ◆ reducing of **Agent** updates receiving time.

> **Proxy servers** can be composed to hierarchical structure.

The general diagram of the anti-virus network when a **Proxy server** is used is illustrated in the figure 10-1.

	Dr.Web Enterprise Server		LAN, Internet
	Proxy Server		Router
	Protected computer		
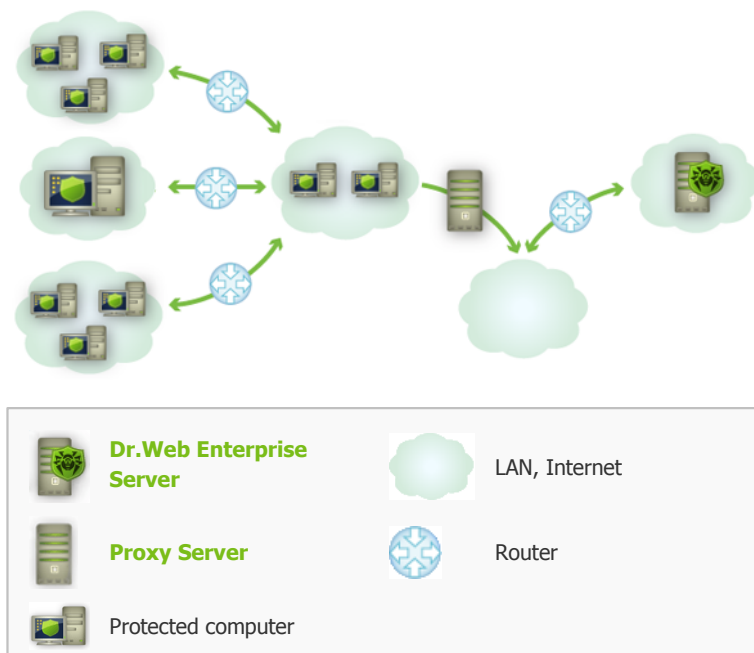
Figure 10-1. Diagram of the anti-virus network when a proxy server is used

Principle of Operation

When a proxy server is used, the following operations are performed

1. If the address of the **Server** is not specified on the **Agent**, the **Agent** sends a multicast request according to the protocol of the network.

2. If the **Proxy server** is set up to translate connections (the `discovery="yes"` parameter), a message about the availability of an operating **Proxy server** is sent to the **Agent**.

3. The **Agent** sets the received **Proxy server** parameters for

Enterprise Server. Further intercommunication is performed transparently for the **Agent**.

4. The **Proxy server** listens specified ports for incoming connections via given protocols according to the configuration file.

5. For each incoming connection from the **Agent** (or **Enterprise Server**) the **Proxy server** establishes a connection with **Enterprise Server** (or **Agent**).

The forwarding algorithm for the list of Enterprise Servers

1. **Proxy server** loads to RAM the list of **Enterprise Servers** from the `drwcsd-proxy.xml` configuration file (see Appendix G4).

2. The **Enterprise Agent** connects to the **Proxy server**.

3. **Proxy server** forwards the **Enterprise Agent** to the first **Server** from the **Enterprise Servers** list loaded in the RAM.

4. **Proxy server** rotate the list in the RAM and moves the **Enterprise Server** from the first position to the end of list.

> **Proxy Server** does not save changed order of **Servers** to its configuration file. After restart of **Proxy server**, the list of **Enterprise Servers** is loaded to the RAM in original version, which is stored in the configuration file.

5. When the next **Agent** connects to the **Proxy server**, procedure is repeated from the step 2.

6. If the **Enterprise Server** disconnects from the antivirus network (e.g., gets offline or denies of service), the **Agent** connects to the **Proxy server** repeatedly and procedure is repeated from the step 2.

> Network scanner which is launched from an external network (in respect to the **Agents**) is unable to locate the installed **Agents**.

If the **Replace NetBios name** flag is set and anti-virus network contains the **Proxy server**, when for all stations connected to the **Server** via the **Proxy server**, in the **Dr.Web Control Center**, the name of computer on which the **Proxy server** is installed, will be shown instead of stations names.

Traffic Encryption and Compression

Proxy server supports traffic compression. Transferred data is processed regardless of whether traffic is compressed or not.

Proxy server does not support traffic encryption. It analyzes transferred data and if traffic between **Enterprise Server** and **Agent** is encrypted, **Proxy server** switches to the transparent mode, i.e. transfers all traffic between **Server** and **Agent** without any data analyzing.

If encryption between **Server** and **Agent** is enabled, **Proxy server** do not caching updates.

Caching

Proxy server supports traffic caching.

Products are cached by revisions. Each revision stores in separate directory. Directories with all next revisions contain *hard links* on existing files from old revisions and originals for changed files. Thus, files for each version are stored on a hard drive in a single exemplar, all directories for next revisions contain only links on unchanged files.

Outdated revisions are cleared ones in an hour. Not outdated are 3 last revisions only. All other revisions are deleted.

In addition, unused *memory mapped* files are unloaded each 10 minutes.

Settings

The **Proxy server** does not have a GUI. Its settings are adjusted via a configuration file. The format of the configuration file is described in Appendix G4.

> ⚠️ Only user with administrative rights on the computer can manage settings (edit configuration file) of **Proxy server**.
>
> For proper operation of **Proxy server** under Linux system-based OS after computer reboot, you must edit system network configuration without Network manager.

Starting and Stopping

To start and stop the **Proxy server** under Windows OS, open **Control Panel** → **Administration** → **Services**, then double-click `drwcsd-proxy` and select a necessary action in the opened window.

To start and stop the **Proxy server** under a UNIX-based OS, use the `start` and `stop` commands with scripts created during installation of the **Proxy server** (see Installing the Proxy Server).

To start the **Proxy-server** under both Windows OS and UNIX system-based OS, you can run the `drwcsd-proxy` executable file with corresponding switches (see the Appendix H10. Proxy Server).

10.2. NAP Validator

Overview

Microsoft® Network Access Protection (NAP) is a policy enforcement platform built into Windows OS that allows you to better protect network assets by enforcing compliance with system health

requirements.

With NAP, you can create customized health requirement policies to
validate computer health in the following cases:

◆ before allowing access or communication,

◆ automatically update compliant computers to ensure ongoing
compliance,

◆ optionally confine noncompliant computers to a restricted
network until they become compliant.

Detailed description of NAT technology specified at http://
www.microsoft.com/windowsserver2008/en/us/nap-product-
home.aspx.

NAP in Dr.Web Enterprise Security Suite

Dr.Web ESS allows you to use the NAP technology to check health of
Dr.Web anti-virus software on protected workstations. This
functionality is provided by use of **Dr.Web NAP Validator**.

Means of Health Validation

◆ A NAP health policy server which is installed and configured in
the network.

◆ The **Dr.Web NAP Validator** which is an implementation of
NAP System Help Validator (SHV) with use of **Dr.Web** custom
policies plug-ins. This component is installed on the computer
where the NAP server resides.

◆ System Health Agents (SHAs) which are installed automatically
on the workstations during installation of **Enterprise Agents**.

◆ The **Dr.Web Enterprise Server** which serves as the NAP
remediation server and ensures health of anti-virus software on
workstations.
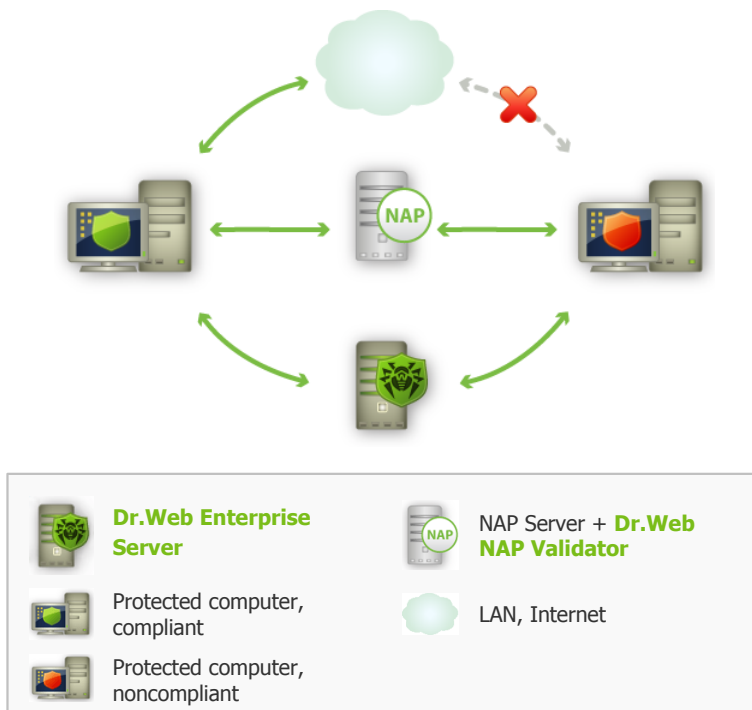
Figure 10-2. Diagram of the anti-virus network when NAP is used

Workstation Validation Procedure

1. Validation is activated when you configure the corresponding settings of the **Agent**. For more information, see Editing the Parameters of the Dr.Web Enterprise Agent.

2. The SHA connect to the **Dr.Web NAP Validator** installed on the NAP server.

3. The **Dr.Web NAP Validator** determines compliance of workstations against the health requirement policies as described below. To determine health compliance, **NAP Validator** checks workstation anti-virus state against the corresponding health requirement policies, and then classifies the workstation in one of the following ways:

◆ Workstations which meet the health policy requirements are classified as compliant and allowed unlimited access and communication on the network.

◆ Workstations which do not meet at least one requirement of the health policy are classified as noncompliant and have their access limited to **Enterprise Server** only. The **Server** allows noncompliant workstations to update the system with the necessary anti-virus settings. After update, the workstations are validated again.

Health Policy Requirements

1. **Enterprise Agent** must be started and running (**Agent** health).
2. **Dr.Web** virus databases must be up-to-date, i.e. databases on the workstation must be similar to those on the **Server**.

Setting NAP Validator

You need to configure **Dr.Web NAP Validator** after installing it on a computer where a NAP server resides. For more information on installation, see Installing NAP Validator.

To configure Dr.Web Nap Validator

1. To open NAP server configuration component, run the `nps.msc` command.
2. In the **Policies** section, select **Health Policies**.
3. Configure the **NAP DHCP Compliant** policy:

   ◆ To enable the policy, select **Dr.Web System Health Validator** in the settings window.

   ◆ To classify workstations as compliant only when all health policy requirements are met, select **Client passed all SHV checks** in the drop-down list.

4. Configure the **NAP DHCP Noncompliant** policy:

   ◆ To enable the policy, select **Dr.Web System Health Validator** in the settings window.

◆ To classify workstations as noncompliant if any of the health policy requirements are not met, select **Client failed one or more SHV checks** in the drop-down list.

Appendices

Appendix A. The Complete List of Supported OS Versions

For the Dr.Web Enterprise Server

UNIX system-based OS:

ALT Linux School Server 5.0
ALT Linux School Server 5.0 x86_64
ASP Linux 12
ASP Linux 14
Debian/GNU Linux Lenny
Debian/GNU Linux Lenny x86_64
Debian/GNU Linux Sid x86_64
Debian/GNU Linux Squeeze
Debian/GNU Linux Squeeze x86_64
FreeBSD 7.3
FreeBSD 7.3 amd64
FreeBSD 7.4
FreeBSD 7.4 amd64
FreeBSD 8.1
FreeBSD 8.1 amd64
FreeBSD 8.2
FreeBSD 8.2 amd64
Linux glibc2.7
Linux glibc2.7 x86_64
Linux glibc2.8
Linux glibc2.8 x86_64

Linux glibc2.9
Linux glibc2.9 x86_64
Linux glibc2.10
Linux glibc2.10 x86_64
Linux glibc2.11
Linux glibc2.11 x86_64
Linux glibc2.12
Linux glibc2.12 x86_64
Linux glibc2.13
Linux glibc2.13 x86_64
Mandriva Linux 2010
Mandriva Linux 2010 x86_64
Mandriva Linux Corporate Server 5.1
Mandriva Linux Corporate Server 5.1 x86_64
openSUSE 11
openSUSE 11 x86_64
RedHat Enterprise Linux 5.3
RedHat Enterprise Linux 5.3 x86_64
RedHat Enterprise Linux 6
RedHat Enterprise Linux 6 x86_64
RedHat Fedora 8
RedHat Fedora 8 x86_64
RedHat Fedora 9
RedHat Fedora 9 x86_64
RedHat Fedora 10
RedHat Fedora 10 x86_64
RedHat Fedora 11
RedHat Fedora 11 x86_64
RedHat Fedora 12
RedHat Fedora 12 x86_64
RedHat Fedora 13
RedHat Fedora 13 x86_64
RedHat Fedora 14

RedHat Fedora 14 x86_64

RedHat Fedora 15

RedHat Fedora 15 x86_64

SUSE Linux Enterprise Server 10

SUSE Linux Enterprise Server 10 x86_64

SUSE Linux Enterprise Server 11

SUSE Linux Enterprise Server 11 x86_64

Sun Solaris 10 x86

Sun Solaris 10 Sparc 32bit (Sparc V9 processor; UltraSparc or later)

Sun Solaris 10 Sparc 64bit (Sparc V9 processor; UltraSparc or later)

Ubuntu 8.04

Ubuntu 8.04 x86_64

Ubuntu 10.04

Ubuntu 10.04 x86_64

Ubuntu 10.10

Ubuntu 10.10 x86_64

Ubuntu 11.04

Ubuntu 11.04 x86_64

Ubuntu 11.10

Ubuntu 11.10 x86_64

Windows OS:

- 32 bit:

Windows 2000 Professional (SP4)

Windows 2000 Server (SP4)

Windows XP Professional (SP3)

Windows XP Home (SP3)

Windows Server 2003 (SP2)

Windows Vista (also with SP1 and later)

Windows Server 2008 (also with SP1 and later)

Windows 7

Windows 8

- 64 bit:

Windows Server 2003 (SP2)

Windows Vista (also with SP1 and later)

Windows Server 2008 (also with SP1 and later)

Windows Server 2008 R2

Windows 7

Windows Server 2012

Windows 8

For the Dr.Web Enterprise Agent and Anti-Virus Package

UNIX system-based OS:

Linux glibc 2.7 and later

FreeBSD 7.3 and later

Sun Solaris 10 (only for Intel platform)

Windows OS:

- 32 bit:

Windows 98

Windows Millennium Edition

Windows NT4 (SP6a)

Windows 2000 Professional (SP4 also with Update Rollup 1)

Windows 2000 Server (SP4 also with Update Rollup 1)

Windows XP Professional (also with SP1 and later)

Windows XP Home (also with SP1 and later)

Windows Server 2003 (also with SP1 and later)

Windows Vista (also with SP1 and later)

Windows Server 2008 (also with SP1 and later)
Windows 7
Windows 8

- 64 bit:

Windows Server 2003 (also with SP1 and later)
Windows Vista (also with SP1 and later)
Windows Server 2008 (also with SP1 and later)
Windows Server 2008 R2
Windows 7
Windows Server 2012
Windows 8

SelfPROtect, Spider Gate, Office Control, FireWall

- 32 bit:

Windows 2000 Professional (SP4 also with Update Rollup 1)
Windows 2000 Server (SP4 also with Update Rollup 1)
Windows XP Professional (also with SP1 and later)
Windows XP Home (also with SP1 and later)
Windows Server 2003 (also with SP1 and later)
Windows Vista (also with SP1 and later)
Windows Server 2008 (also with SP1 and later)
Windows 7
Windows 8

- 64 bit:

Windows Server 2003 (also with SP1 and later)
Windows Vista (also with SP1 and later)
Windows Server 2008 (also with SP1 and later)
Windows Server 2008 R2
Windows 7
Windows Server 2012
Windows 8

Windows Mobile OS

Windows Mobile 2003

Windows Mobile 2003 Second Edition

Windows Mobile 5.0

Windows Mobile 6.0

Windows Mobile 6.1

Windows Mobile 6.5

Novell NetWare OS

Novell NetWare 4.11 SP9

Novell NetWare 4.2

Novell NetWare 5.1

Novell NetWare 6.0

Novell NetWare 6.5

Mac OS X

Mac OS 10.4 (Tiger)

Mac OS 10.4 Server (Tiger Server)

Mac OS 10.5 (Leopard)

Mac OS 10.5 Server (Leopard Server)

Mac OS 10.6 (Snow Leopard)

Mac OS 10.6 Server (Snow Leopard Server)

Mac OS 10.7 (Lion)

Mac OS 10.7 Server (Lion Server)

Android OS

Android 1.6

Android 2.0

Android 2.1

Android 2.2
Android 2.3
Android 3.0
Android 3.1
Android 3.2
Android 4.0.

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

> You can get the structure of the **Enterprise Server** DB via the init.sql script, located in the etc subfolder of the **Enterprise Server** installation folder.

As a database for **Enterprise Server** you can use the following variants:

◆ internal DBMS (IntDB);
◆ external DBMS.

Internal DBMS

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

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

Name	Default value	Description
DBFILE	dbinternal.dbs	Path to the database file
CACHESIZE	2000	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.

External DBMS

The following database management systems may be used to arrange the external database for **Enterprise Server**:

- ◆ Oracle. The settings are given in Appendix B2. Setting Up the Database Driver for Oracle.
- ◆ Microsoft SQL Server Compact Edition (SQL CE). The settings are given in Appendix B3. Setting Up the Database Driver for SQL CE.
- ◆ PostgreSQL. The settings necessary for PostgreSQL are given in Appendix B4. Using the PostgreSQL DBMS.
- ◆ Microsoft SQL Server/Microsoft SQL Server Express. To access these DBMS, an ODBC driver may be used (setting up the parameters of the ODBC driver for Windows is given in Appendix B1. Setting Up the ODBC Driver).

> With Microsoft SQL Server 2005 it is necessary to use the ODBC driver supplied with this DBMS.
>
> Using of Microsoft SQL Server 2005 (SP4) and later is supported.
>
> It is strongly recommended to install latest service packs for used DB server.
>
> Microsoft SQL Server Express DB is not recommended for anti-virus network with a large number of stations (from 100 and more).

Comparison Characteristics

> An internal DB can be used, if at most 200-300 stations are connected to the **Server**. If the hardware configuration of the computer with **Enterprise Server** and the load level of other executing tasks are permissible, up to 1000 stations can be connected.

Otherwise, you must use an external DB.

If you use an external DB and more than 10 000 stations are connected to the **Server**, it is recommended to perform the following minimal requirements:

◆ 3 GHz processor CPU,

◆ RAM at least 4 Gb for the **Enterprise Server** and at least 8 Gb for the DB server,

◆ UNIX system-based OS.

When choosing between an internal and external database, take into account the following peculiar parameters of DMBS:

◆ In large anti-virus networks (of over 200-300 stations), it is recommended to use an external DB, which is more fault-resistant than internal DBs.

◆ The internal DBMS (IntDB) is considerably faster than the external analogs and is recommended mainly for the typical use of databases.

◆ You may use an external database in case it will be necessary to work through a DBMS and access the DB directly. To facilitate access, standard APIs may be used, such as OLE DB, ADO.NET or ODBC. Though it is to be noted that there is no ODBC driver for Microsoft SQL CE at present. Still, working in applications with this DBMS may be facilitated by implementing ADO.NET technologies and the LINQ language, which allows using all the possibilities of the .NET Framework platform including the report generation system CrystalReports.

Appendix B1. Setting Up the ODBC-driver

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

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

Name	Default value	Description
DSN	Drwcs	Data set name

Name	Default value	Description
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 on transactions isolation see in documentation on corresponding DBMS.

> To exclude encoding problems, you must disable the following parameters of ODBC-driver:
>
> - ◆ **Use regional settings when outputting currency, numbers, dates and times** - may cause errors during numerical parameters formatting.
>
> - ◆ **Perform translation for character** - may cause illegal characters displaying in the **Dr.Web Control Center** for parameters, which are came from the DB. This parameter sets symbols displaying dependence on the language parameter for programs, which do not use the Unicode.

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 **Enterprise 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 be opened. Go to the **System DSN** tab.

2. Click **Add**. A window for selecting a driver will be opened.

3. Select the item of the corresponding ODBC-driver for this DB in the list and click **Finish**. The first window for setting access to the DB server will be opened.

> ⚠ If an 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 ODBC driver supplied with Windows OS. Except databases, supplied by Microsoft without ODBC-driver.

4. Enter access parameters to the data source (the same as in the settings of **Enterprise Server**). If the DB server is not installed on the same computer as **Enterprise Server**, in the **Server** field specify its IP address or name. Click **Next**. The next window will be opened.

5. Specify the necessary DB access settings in this window. Click **Client configuration**. A window for selecting and setting the network protocol will be opened.

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 be opened.

7. Check that the **Only when you disconnect** option, the **Use ANSI quoted identifiers** and the **Use ANSI nulls**, **paddings** and **warnings** flags are set. Click **Next.** The last window for setting access will be opened.

> ℹ 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 be opened.

9. To test the specified settings, click **Test Data Source**. After you see a notification of a successful test, click **OK**.

Appendix B2. Setting Up the Database Driver for Oracle

General Description

The Oracle Database (or Oracle DBMS) is an object-relational DBMS. Oracle may be used as an external DB for **Dr.Web ESS**.

> ⚠️ The **Dr.Web Enterprise Server** may use the Oracle DBMS as an external database on all platforms except FreeBSD (see Installation and supported versions).

To use the Oracle DBMS:

1. Install an instance of Oracle DB and set up the AL32UTF8 encoding. Also you may use existence instance which is configured to use the AL32UTF8 encoding.

2. Set up the database driver to use the respective external database. You can do this in configuration file or via **Dr.Web Control Center**: **Configure Dr.Web Enterprise Server**, **Database** tab.

> ⚠️ If you are going to use the ODBC for Oracle as an external database, select the **Custom** option and in the opened window disable the installation of Oracle client in the **Database support** - **Oracle database driver** section in the installer settings during the **Server** installation (or upgrade).
>
> Otherwise, Oracle DB functioning will fail because of the libraries conflict.

Installation and Supported Versions

To use Oracle as en external DB, you must install the instance of the Oracle DB and set up `AL32UTF8` (`CHARACTER SET AL32UTF8 / NATIONAL CHARACTER SET AL16UTF16`) encoding. This can be done in one of the following ways:

- ◆ Using an Oracle installer (use an external mode of instance installation and configuration);
- ◆ Using the `CREATE DATABASE` SQL command.

For more information on creating and configuring Oracle instances, see Oracle documentation.

> ⚠️ In case of using a different encoding, national symbols may be displayed incorrectly.

A client to access the database (Oracle Instant Client) is included in the installation package of **Dr.Web ESS**.

Platforms supported by the Oracle DBMS are listed on the web site of the vendor http://www.oracle.com/technology/software/tech/oci/instantclient/index.html.

Dr.Web ESS supports the following versions of the DBMS: Oracle9i Database Release 2: 9.2.0.1 - 9.2.0.8 and higher.

Parameters

To adjust access to the Oracle DBMS, use the parameters described in Table B-3.

Table B-3. Parameters of the Oracle DBMS

Parameter	Description
drworacle	Driver name

Parameter	Description
User	Database user name (obligatory)
Password	User password (obligatory)
ConnectionString	Database connection string (obligatory)

The format of the connection string to the Oracle DBMS is as follows:

`//<host>:<port>/<service name>`

where:

- ◆ *<host>* - IP address or name of the Oracle server;
- ◆ *<port>* - port 'listening' to the server;
- ◆ *<service name>* - name of the DB to connect to.

For Example:

`//myserver111:1521/bjava21`

where:

- ◆ `myserver111` - name of the Oracle server.
- ◆ `1521` - port 'listening' to the server.
- ◆ `bjava21` - name of the DB to connect to.

An Example of the drwcsd.conf Configuration File

If you deploy Oracle, it is necessary to change the definition and the settings of the database driver by one of the following ways:

- ◆ in the **Control Center**: **Administration** item in the main menu → **Dr.Web Enterprise Server Configuration** item in the control menu → **Database** tab → select in the **Database** drop-down list, the **Oracle** type, and set parameters according to the format listed below.
- ◆ in the **Server** configuration file. Fragment of configuration file with corresponding parameters is listed below:

```
...
;Database definition. Mandatory.
;Only one definition is allowed.
database

;DB driver (DLL or shared object name)
drworacle  ; Oracle DB, unix & windows

;load library from this path; empty - use default
from ""
using "User=DRWCS Password=root
ConnectionString=//192.168.0.1:1521/ORADB"
```

Appendix B3. Setting Up the Database Driver for SQL CE

> If you do not need the direct operation with the DB via the ADO.NET, it is recommended to use an internal DB instead of SQL SE DB. Internal DB is more stable and productive in comparison with the SQL CE.

General description

Microsoft SQL Server Compact Edition (SQL CE) is a relational database produced by the Microsoft company.It is an embedded database engine for desktop applications and mobile devices. SQL CE may be used as an external database for **Dr.Web ESS**.

To use SQL Server CE:

1. Install the SQL CE server.

2. Set up the database driver to use the respective external database. You can do this in configuration file or via the **Dr.Web Control Center**: **Configure Dr.Web Enterprise Server**, **Database** tab.

Installation and Supported Versions

> ⚠ The SQL CE DBMS is compatible only with Windows 2000 OS and higher (x32 and x64 versions).
>
> **Dr.Web Enterprise Security Suite** supports Microsoft SQL Server Compact of 3.5 SP1/SP2 for x86 and x64 platforms. Compatibility with all later versions of SQL CE DB is not guaranteed.

If you want to deploy SQL Server Compact Edition, you need to download the installation package from the web site of the manufacturer http://www.microsoft.com/sqlserver/2005/en/us/compact-downloads.aspx and install the corresponding version of the server (see also System requirements for 3.5.).

> ⚠ It is not recommended to install more than one version of Microsoft SQL Server Compact on the same computer due to possible compatability issues.
>
> Microsoft SQL Server Compact 3.1 does not support encryption. Databases created on servers running under this version of Microsoft SQL Server may not be compartible with Microsoft SQL Server Compact 3.5 servers. Use the **Dr.Web Enterprise Security Suite** exportdb and importdb commands to import data from SQL Server Compact 3.1 databaes to SQL Server Compact 3.5 databases.

A client to access the database is included in the installation package of **Dr.Web ESS**.

Parameters

To adjust access to the SQL CE DBMS, use the parameters described in Table B-4.

Table B-4. Parameters of the SQL CE DBMS

Parameter	Description
drwsqlce	Driver name
DBFILE	Database name (by default mssqlce.sdf)
PASSWORD	Database encryption password

> The PASSWORD parameter is an encryption key and bears no relation to the user/password system.
>
> By default, the password is empty (the database is not encrypted).

An Example of the drwcsd.conf Configuration File

If you deploy SQL CE, it is necessary to change the definition and the settings of the database driver in the configuration file of the **Server**. See a fragment of the configuration file with corresponding parameters below:

```
...
;Database definition. Mandatory.
;Only one definition is allowed.
database


;DB driver (DLL or shared object name)
drwsqlce ; sql server compact, windows only

```

```
;load library from this path; empty - use default
from ""
;parameters describing database connection
;defaults (DBFILE: varroot/mssqlce.sdf)
;using "DBFILE=mssqlce.sdf PASSWORD=drwcs"
using "DBFILE=mssqlce.sdf PASSWORD=drwcs"
```

Appendix B4. Using the PostgreSQL DBMS

General Description

PostgreSQL is an object-relational DBMS distributed as a freeware unlike such commercial DBMS as Oracle Database, Microsoft SQL Server, etc. The PostgreSQL DBMS may be used to arrange an external DB for the **Dr.Web Enterprise Server** in large anti-virus networks.

To do this:

1. Install the PostgreSQL server.
2. Set up the ODBC driver.
3. Set up the **Dr.Web Enterprise Server** to use the respective external database. You can do this in configuration file or via the **Dr.Web Control Center**: **Configure Dr.Web Enterprise Server**, **Database** tab.

Installation and Supported Versions

Please download the latest available version of this free product (the **PostgreSQL** server and correspondent ODBC-driver), otherwise do not use the version earlier than **8.2.**

> ⚠️ PostgreSQL DMBS is compatible with the following platforms: Linux, Solaris/OpenSolaris, Win32, MacOS X, FreeBSD.

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

For more information about installation of **Enterprise Server** using external database see step 10 in p. Installing the Dr.Web Enterprise 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.

Installation for 64-bit systems

PsqlODBC driver for x64 systems is not supplied by an official developer. However, according to the PostgreSQL DBMS official web-site, prerelease installation packages can be installed. You can download these packages, for instance, using following links:

- ◆ http://www.enterprisedb.com/products/pgdownload.do#windows
- ◆ http://code.google.com/p/visionmap/wiki/psqlODBC
- ◆ http://www.geocities.jp/inocchichichi/psqlodbc/index.html

> ℹ️ After installation of the ODBC-driver on 64-bit OS, to get access to drivers, use administrative management panel, resides in: `C:\WINDOWS\SYSWOW64\odbcad32.exe`.

Parameters

When setting access to PostgreSQL, use the parameters described below.

Table B-5. PostgreSQL parameters (only in the version for UNIX OS)

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

More information can be found at http://www.postgresql.org/docs/manuals/.

Dr.Web Enterprise Server and PosrtgreSQL DB Interaction via the UDS

If the **Enterprise Server** and the PostgreSQL DB are installed on the same computer, their interaction can be set via the UDS (UNIX domain socket).

To set interaction via the UDS:

1. In the postgresql.conf PostgreSQL configuration file, specify the following directory for the UDS:

   ```
   unix_socket_directory = '/var/run/postgresql'
   ```

2. Restart the PostgreSQL.

Appendix C. The Description of the Notification System Parameters

When setting the system of alerts for events connected with the program 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

> ⚠️ Windows network message system functions only under Windows OS with Windows Messenger (Net Send) service support.
>
> Windows Vista OS and later do not support Windows Messenger service.

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** component named the templates processor on the basis of the templates files.

> Windows network message system functions only under Windows OS with Windows Messenger (Net Send) service support.
>
> Windows Vista OS and later do not support Windows Messenger service.

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:

- ◆ {*<VAR>*} – substitute the current value of the *<VAR>* variable.
- ◆ {*<VAR>*:*<N>*} – the first *<N>* characters of the *<VAR>* variable.
- ◆ {*<VAR>*:*<first>*:*<N>*} – the value of *<N>* characters of the *<VAR>* variable that go after the first *<first>* characters (beginning from the *<first>*+1 symbol), if the remainder is less, it is supplemented by spaces on the right.
- ◆ {*<VAR>*:*<first>*:−*<N>*} – the value of *<N>* characters of the *<VAR>* variable that go after the first *<first>* characters (beginning from the *<first>*+1 symbol), if the remainder is less, it is supplemented by spaces on the left.

◆ {*<VAR>*/*<original1>*/*<replace1>*[/*<original2>*/ *<replace2>*]} – replace specified characters of *<VAR>* variable with given characters: *<original1>* characters are replaced with *<replace1>* characters, *<original2>* characters are replaced with *<replace2>* characters, etc.

There is no limitation for the number of substitution pairs.

Table D-1. Notation of variables

Variable	Value	Expression	Result
SYS.TIME	10:35:17:456	{SYS.TIME:5}	10:35
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	10:35:17:456	{SYS.TIME/10/99/35/77}	99:77:17.456

Conventions

° - whitespace.

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**),

◆ SYS.SERVER — product name (**Dr.Web Enterprise Server**).

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 (Dr.Web Enterprise Server 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 — **Dr.Web Control Center** network address;

Approved_Newbie:

- ◆ MSG.AdminName — administrator name,
- ◆ MSG.AdminAddress — **Dr.Web Control Center** 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 is launched 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 the last visit;

Processing_Error:

- ◆ `MSG.Component` — component name,
- ◆ `MSG.RunBy` — component is launched 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 **Dr.Web Control Center** address;

Station_Already_Logged_In:

- ◆ `MSG.ID` — station UUID,
- ◆ `MSG.StationName` — name of the station,
- ◆ `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 **Dr.Web Control Center** 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 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.

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/127.0.0.1:2193
```

means a TCP protocol, port `2193` on an interface `127.0.0.1`.

```
2.tcp/[::]:2193
```

means a TCP protocol, port `2193` on an IPv6 interface `0000.0000.0000.0000.0000.0000.0000.0000`

```
3.localhost:2193
```

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/00000000.000000000001:2193`

  means socket SPX loopback `0x2193.`

UDS Addresses

  ◆ Connection-oriented protocol:

  `unx/`*<file_name>*

  ◆ Datagram-oriented protocol:

  `udx/`*<file_name>*

Examples:

1. `unx/tmp/drwcsd:stream`
2. `unx/tmp/drwcsd:datagram`

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.

Datagram-Oriented Protocol

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

Examples:

1.`udp/231.0.0.1:2193`

  means using a multicast group `231.0.0.1:2193` on an interface depending on the application by default.

2.`udp/[ff18::231.0.0.1]:2193`

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/0.0.0.0:2193`

  which means "all interfaces (excluding those with IPv6 addresses), port `2193`";

- ◆ `tcp/[::]:2193`

  which means "all IPv6 addresses, port `2193`";

- ◆ `spx/00000000.000000000001:2193`

  which means "all interfaces, port `0x2193`";

- ◆ `nbs/drwcs:23:0`

  which means using NetBIOS stream protocol, port `23`, computer `drwcs`.

Dr.Web Enterprise Server Location Service

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

By default, depending on *<datagram-protocol>*:

- ◆ `udp/231.0.0.1:2193-0.0.0.0`

  which means using a multicast group `231.0.0.1:2193` for all interfaces;

- ◆ `udp/[ff18::231.0.0.1]:2193-[::]:0`

  which means using a multicast group `[ff18::231.0.0.1:2193]` on all interfaces;

- ◆ `ipx/00000000.FFFFFFFFFFFF:2193-` `00000000.000000000000`

  which means receipt of broadcasting messages on socket `0x2193` 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 Dr.Web Enterprise Server

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

By default, depending on *<connection-protocol>*:

- ◆ `tcp/127.0.0.1:2193`

  means loopback port `2193`,

- ◆ `tcp/[::]:2193`

  means loopback port `2193` for IPv6;

- ◆ `spx/00000000.000000000001:2193`

means loopback socket `0x2193`.

<drwcs-name> Dr.Web Enterprise 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/231.0.0.1:2193−0.0.0.0`

location of a **Server** with the `drwcs` name for a TCP connection using a multicast group `231.0.0.1:2193` for all interfaces,

◆ `drwcs@ipx/00000000.FFFFFFFFFFFF:2193−` `00000000.000000000000`

location of a **Server** with the `drwcs` name for an SPX connection using broadcasting messages on socket `0x2193` 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 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 .config Configuration File

Formal grammar based on the Extended Backus-Naur Form (EBNF) notation is used for description of the **Server** configuration file. It uses the following symbols:

- ◆ (...) — group of symbols (fragment of the configuration file);
- ◆ '...' — terminal symbol;
- ◆ <...> — nonterminal symbol;
- ◆ | – symbol for selecting one of the given elements;
- ◆ (...)? – symbol (or group of symbols) to the left of the operator is not obligatory (may occur 0 or 1 time);
- ◆ (...)* – symbol (or group of symbols) to the left of the operator may be repeated any number of times (or may be omitted);
- ◆ (...)+ – symbol (or group of symbols) to the left of the operator may occur 1 or more times;
- ◆ [...] – any symbol from the specified range;
- ◆ period at the end — a reserved character which indicates completion of a rule.

```
<line> := <instruction>? (<separator>+ <comment>?)*.


<instruction> := <name> "{"? <parameter>* "}"?.

<name> := "description" | "sync-with" |
          "sync-delay" | "sync-only" |
          "sync-ignore" | "state-only" |
          "state-ignore" | "notify-only" |
          "notify-ignore" | "notify-off".

<parameter> := <text>.

<text> := <word> <separator>*.

<word> := (<symbol> | <sign>)+.

<symbol> := [a-zA-Z] | [0-9].

<sign> := """ | "/"| "\" | "*" | "^" | "." | "-"| "$".


<separator> := \r | \t | \n | \s.


<comment> := ";"<text> | "#"<M1><symbol>+<M1> | "'"<M2><text>+<M2>.

<M1> := <symbol>+.
```

```
<M2> := <sign>+.
```

The configuration file is a sequence of words separated by separators. A separator is any sequence of the following characters: space ($\backslash s$), tab ($\backslash t$), carriage return ($\backslash r$), line feed ($\backslash n$).

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.

F2. The Meaning of .config File Instructions

The Description Instruction

The description instruction sets a product name which is displayed in the **Dr.Web Control Center**. 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 **Dr.Web Enterprise Security Suite** version supports only base HTTP authentication, proxy-HTTP authentication and RADIUS 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 }
}
```

If using the proxy server

```
sync-with{
 http-proxy{  10.3.0.74   auth   user:pass   http
{ esuite.msk7.drweb.com /update  } }
 http-proxy{  10.3.0.74   auth   user:pass   http
{ esuite.jp.drweb.com   /update  } }
 http-proxy{  10.3.0.74   auth   user:pass   http
{ esuite.msk5.drweb.com /update  } }
 http-proxy{  10.3.0.74   auth   user:pass   http
{ esuite.msk6.drweb.com /update  } }
 http-proxy{  10.3.0.74   auth   user:pass   http
{ esuite.msk.drweb.com  /update  } }
 http-proxy{  10.3.0.74   auth   user:pass   http
{ esuite.us1.drweb.com  /update  } }
 http-proxy{  10.3.0.74   auth   user:pass   http
{ esuite.msk3.drweb.com /update  } }
 http-proxy{  10.3.0.74   auth   user:pass   http
{ esuite.msk4.drweb.com /update  } }
 http-proxy{  10.3.0.74   auth   user:pass   http
{ esuite.us.drweb.com   /update  } }
```

```
 http-proxy{    10.3.0.74    auth    user:pass    http
{ esuite.fr1.drweb.com  /update  } }
}
```

where:

- ◆ `10.3.0.74` - IP-address of the proxy server;
- ◆ `user` - name of the user to access the proxy server (may be absent, if the proxy do not require authentication);
- ◆ `pass` - password to access the proxy server (may be absent, if the proxy do not require authentication).

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 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 **Enterprise Agent**:

◆ german, polish and spanish interface languages should not be received (others - will 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.).

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 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 folder, except for the `.id` and the `.config` files,

◆ write `0` to the `.id` file,

◆ launch the **Server**,

◆ update the product.

> **i** `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:

1. Stop the **Server**.
2. Write `0` to the `.id` file.
3. Comment the `sync-with` instruction in the `.config`, file to disable synchronization.
4. Restart the **Server**.
5. Update the product.

Shift from the "frozen" status to a new version:

1. Replace the content of the `.id` file

   <new_revision> <previous_revision> `frozen`

   with

   <new_revision>,

2. Restart the **Server**.
3. 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.

> **i** At future attempts to synchronize to the *<new revision>*, the repository will go into the "frozen" status again. Saving an <old revision> with updates rejecting is reasonable when a suitable revision is available, for example, after successful tests in the lab.

Appendix G. Configuration Files

This section describes the format of the following files:

◆ `drwcsd.conf` configuration file of the **Enterprise Server**;

◆ `drwcsd-proxy.xml` configuration file of the **Proxy server**;

◆ `webmin.conf` configuration file of the **Dr.Web Control Center**;

◆ `download.conf` configuration file.

> ⚠️ If on the computer with corresponding component, the **Agent** with enabled self-protection is installed, before editing configuration files, disable the **Dr.Web SelfPROtect** component via the **Agent** settings.
>
> After you save all changes, it is recommended to enable the **Dr.Web SelfPROtect** component.

G1. Dr.Web Enterprise 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).

To manage the Dr.Web Enterprise Server configuration file manually, do the following:

1. Stop the **Server** (see Start and Stop the Dr.Web Enterprise Server).

2. Disable self-protection (in case of installed **Agent** with the active self-protection - in the **Agent** context menu).

3. Manage the **Server** configuration file.

4. Start the **Server** (see Start and Stop the Dr.Web Enterprise Server).

Dr.Web Enterprise Server Configuration File Format

Formal grammar based on the Extended Backus-Naur Form (EBNF) notation is used for description of the **Server** configuration file. It uses the following symbols:

- ◆ `(...)` — group of symbols (fragment of the configuration file);
- ◆ `'...'` — terminal symbol;
- ◆ `<...>` — nonterminal symbol;
- ◆ `|` – symbol for selecting one of the given elements;
- ◆ `(...)?` – symbol (or group of symbols) to the left of the operator is not obligatory (may occur 0 or 1 time);
- ◆ `(...)*` – symbol (or group of symbols) to the left of the operator may be repeated any number of times (or may be omitted);
- ◆ `(...)+` – symbol (or group of symbols) to the left of the operator may occur 1 or more times;
- ◆ `[...]` – any symbol from the specified range;
- ◆ period at the end — a reserved character which indicates completion of a rule.

Format of the Server configuration file

```
<instruction> := (<parameter> '"'<value>'"')? (';'<comment>)?.
<parameter> := <word>.
<value> := (<word> <separator>*)*.
<word> := ([a-zA-Z] | [0-9] | <reserved_character>)+.
<reserved_character> := '&&' | '&r' | '&t' | '&n' | '&v' |
'&f' | '&b' | '&e' | '&l' | '&s'.
<separator> := \s | \t | \r | \n | \f.
```

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 **Dr.Web**

Control Center. 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.

◆ `MaximumAuthorizationQueue` *<value>*

Specify the maximum number of workstation in the **Server** authorization queue. 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 **ESS** 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` (default is `Yes`). For more read p. Traffic Encryption and Compression.

◆ Compression *<mode>*

Traffic compression mode. Possible values: `Yes`, `No`, `Possible` (default is `No`). For more read p. Traffic Encryption and Compression

◆ `InstallAccess`, `AgentAccess` and `LinksAccess` parameters are not displayed in the configuration file unless the **Use this ACL** flag is set (for more see p. Setting the Dr.Web Enterprise Server Configuration). If this flag is set, 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. <u>Setting the Mode of Operation with Databases</u>.

> **i** 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. <u>Setting Alerts</u>.

> **i** 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 <u>Appendix D. The Parameters of the Notification System Templates</u>.

◆ 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. The SERVER protocol is disabled by default. Read more in p. Setting the Dr.Web Enterprise Server Configuration.

---

i   Disabling unnecessary protocols saves system resources.

◆ `Disable Plugin` *<module>*

Disable the use of plug-ins for the **Server**. Legitimate value: WEBMIN. For details see Setting the Dr.Web Enterprise Server Configuration.

◆ `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`.

◆ The `Organization`, `Department`, `Country`, `Province`, `City`, `Street`, `Floor`, `Room`, `Latitude` and `Longitude` parameters define additional information about the location of the workstation.

◆ `TrackAgentJobs` *<value>*

Enable writing the results of task completion for workstations to the DB. Possible values: `Yes` or `No`.

◆ `TrackAgentStatus` *<value>*

Enable accounting of the workstation status changes and writing information to the DB. Possible values: `Yes` or `No`.

◆ `TrackVirusBases` *<value>*

Enable accounting of the workstation virus database status (composition, changes) and writing information to the DB. Possible values: `Yes` or `No`.

◆ `TrackAgentModules` *<value>*

Enable writing to the DB the list of the **Anti-virus** modules at the station. Possible values: `Yes` or `No`.

◆ `TrackAgentComponents` *<value>*

Enable writing to the DB the list of **Anti-virus** components **(Scanner**, **Monitors**, etc) that are installed at the station. Possible values: `Yes` or `No`.

◆ `KeepRunInformation` *<value>*

Enable writing to the DB information on starting and stopping events of **Anti-virus** components (**Scanner**, **Monitors**, etc) at stations. Possible values: `Yes` or `No`.

◆ `KeepInfections` *<value>*

Enable writing to the DB statistic data about infections, detected at the stations. Possible values: `Yes` or `No`.

◆ `KeepScanErrors` *<value>*

Enable writing to the DB information on all errors, occurring during scanning at the stations. Possible values: `Yes` or `No`.

◆ `KeepScanStatistics` *<value>*

Enable writing to the DB results of stations scanning. Possible values: `Yes` or `No`.

◆ `KeepInstallation` *<value>*

Enable writing to the DB information on **Agent** installations at the stations. Possible values: `Yes` or `No`.

◆ `Quarantine` *<value>*

Enable writing to the DB stations **Quarantine** state. Possible values: `Yes` or `No`.

◆ `UpdatesBandwidth` *<value>*

Maximal network traffic bandwidth in KB for updates from **Server** to **Agents**. 0 value means unlimited bandwidth.

◆ `Audit` *<value>*

Enable audit logging of the operations performed by the administrator on the **Dr.Web Control Center** and writing the log to the DB. Possible values: `Yes` or `No`.

◆ `AuditInternals` *<value>*

Enable audit logging of the **Server** internal operations and writing the log to the DB. Possible values: `Yes` or `No`.

G2. Dr.Web Control Center Configuration File

The **Dr.Web Control Center** configuration file (`webmin.conf`) is located in the `etc` subdirectory of the **Server** root directory.

Formal grammar based on the Extended Backus-Naur Form (EBNF) notation is used for description of the **Server** configuration file. It uses the following symbols:

◆ `(...)` — group of symbols (fragment of the configuration file);

◆ `'...'` — terminal symbol;

◆ `<...>` — nonterminal symbol;

◆ `|` – symbol for selecting one of the given elements;

◆ `(...)?` – symbol (or group of symbols) to the left of the operator is not obligatory (may occur 0 or 1 time);

◆ `(...)*` – symbol (or group of symbols) to the left of the operator may be repeated any number of times (or may be omitted);

◆ `(...)+` – symbol (or group of symbols) to the left of the operator may occur 1 or more times;

◆ `[...]` – any symbol from the specified range;

◆ period at the end — a reserved character which indicates completion of a rule.

The format of the Dr.Web Control Center configuration file:

```
<instruction> := <parameter>* (';'<comment>)?.


<parameter> := <single> | <block>.
<single> := <name> <value>.
<group> := <name> '{' (<value>' ')+ '}'.
<block> := <prefix>? <name> '{' <single>* | <group>* | <access>?
| <auth>? '}'.


<prefix> := 'Static' | 'Handler' | 'Scripts' | 'Mixed'.
<access> := 'Access {'
              'Secure {'
                 'Priority ' <priority>?
                 ('Allow {' <value>* '}')?
                 ('Deny {' <value>* '}')?
              '}'
              'InSecure {'
                 'Priority ' <priority>?
                 ('Allow {' <value>* '}')?
                 ('Deny {' <value>* '}')?
              '}'
            '}'.
<priority> := 'deny' | 'allow'.


<auth>:= 'Authorization {' <single>+ | <group>+ '}'.


<name> := <word>.
<value> := <word> <separator>*.
<word> := ( [a-zA-Z] | [0-9] | <sign> )+.
<separator> := \s | \t | \r | \n | \f.
<sign> := '/' | '*' | ':' | '.' | '-' | '?' | '^'| '[' |
']'.
```

The configuration file has a text format. The main units in the file are words with separators: spaces (`\s`), tabs (`\t`), carriage shunting (`\r`), line end (`\n`), format change (`\f`).

Comments begin with a semicolon and continue to the end of the line.

Settings of the **Server** are specified in the configuration file via instructions each consisting of:

- ◆ a parameter which includes the parameter name (one word) and its value(s) (one or several words),
- ◆ a block of parameters which includes the block name (one word) followed by values in braces ("`{...}`"):
  - • simple parameters consisting of the parameter name (one word) and its value(s) (one or several words),
  - • groups of parameters consisting of the parameter name (one word) followed by a set of values in braces (one or several words for each value),
  - • the `Access` group of parameters which defines the rules for access to specified resources of the **Server** (see below),
  - • the `Authorization` group of parameters which defines authorization parameters for access to specified resources (see below).

Before the name of a block you can specify a prefix (one word) which defines how this block should be processed.

Some of the possible instructions are described below. The order of instructions is irrelevant.

Most simple (single) parameters are specified with default values and do not require any changes. However, it may be necessary to set the values for some of them:

- ◆ `ServerName` *<DNS_name>*:*<port_number>* – defines name and port number of the **Server**. It is used for connection requests to the **Server**. It is necessary to specify the correct values after installing the **Server** (see Installing the Dr.Web Enterprise Server).

◆ Listen *<protocol> <interface>*:*<port_number>* – defines the parameters of interfaces which are being listened to. It is used to set up access to the **Dr.Web Control Center**.

Blocks of parameters consist of the the following groups and parameters:

◆ The prefix (Static, Script, Handler or Mixed) is specified before the name of the parameter block and defines how corresponding user requests are processed.

   • The Static prefix defines a static processing method which implies that a user is given the final value - the requested file without changes (e.g. an image which is stored on the **Server**).

   • The Handler prefix defines a processing method which implies execution of a script specified in the parameters of the block upon receiving the user request (paths specified in the request do not have to be correct). It is necessary to have the Script *<script_name>* instruction in the body of the instruction block.

   • The Scripts prefix defines a processing method which implies execution of all files from the user request as scripts.

   • The Mixed prefix defines a mix of Static and Scripts processing methods. It is necessary to have the Scripts { *<script_extension>* } instruction in the body of the instruction block which defines executable scripts (according to extension). Other files, which do not comply with the values of the given group of parameters, will be passed on statically (without any processing).

◆ The Access group of parameters contains access rights for the resources of the **Server** when processing the received user requests.

   • The Secure group defines access rights for protected connections via HTTPS.

   • The InSecure group defines access rights for unprotected

connections via HTTP.

- o The `Priority` *<priority>* parameter defines the priority for processing lists of allowed and forbidden connections. If you specify the `deny` value, all addresses which are not included into both groups (`Allow and Deny`) will be forbidden. If you specify `allow` - they will be allowed.
- o The `Allow` group list of parameters defines addresses, access to which is allowed from the **Server**.
- o The `Deny` group list of parameters defines addresses, access to which is forbidden from the **Server**.

Addresses are added to the allowed/forbidden lists in the following format:

for TCP/IP: `tcp/`*<IP-address>*`[/`*<prefix>*`]`;

for SPX: `spx/`*<network_number>*`[.`*<station_address>*`]`.

◆ The `Authorization` group of parameters defines the necessary parameters for user authorization when the **Server** is accessed to process a corresponding request.

G3. Download.conf Configuration File

The download.conf file purposes:

1. During creating and operating of **Enterprise Servers** cluster system, the file allows to distribute the load between the **Servers** of a clusters when connecting a large number of new stations.
2. If a custom port is used at the **Enterprise Server**, the file allows to specify this port during generating installation file of the **Agent**.

The `download.conf` file is used during generating the installation file for a new station of the antivirus network. Parameters of this file allows to specify address of the **Server** and the port, which are used to connect the **Agent** Installer to the **Server**, in the following format:

```
download = { server = '<Server_Address>'; port =
```

<port_number> }

where:

◆ *<Server_Address>* - IP address or DNS name of the **Server**.

During generating of the **Agent** installation file, the **Server** address is taken from the download.conf file first. If the **Server** address is not specified in the download.conf file, when value of the ServerName parameter from the webmin.conf file is taken. Otherwise, the name of the computer, returned by an operating system is used.

◆ *<port_number>* - port to connect the **Agent** Installer to the **Server**.

If the port is not specified in the download.conf file, 2193 port is used by default (sets in the **Administration → Dr.Web Enterprise Server configuration → Transport** tab in the **Control Center**).

By default, the download parameter is disabled in the download.conf file. To use the download.conf file, uncomment this parameter by deleting the "--" in the start of the line, and specify corresponding values of an address and a port of the **Server**.

G4. Proxy Server Configuration File

The drwcsd-proxy.xml configuration file of the **Proxy server** is presented in the XML format and located in:

◆ For Windows OS: **Proxy server** installation folder.
◆ For UNIX system-based OS: etc subfolder of the **Proxy server** installation folder or in the current user's work directory.

The <cache-root /> element

The `<drwcsd-proxy />` root element may contain non-obligatory `<cache-root />` element which defines the path to the cache directory of the **Proxy server**. If `<cache-root />` element has not been specified, caching data will be saved in the temporary directory of OS user.

The <listen /> element

The `<drwcsd-proxy />` root element contains one or several obligatory `<listen />` elements which define basic settings of the **Proxy Server** for receiving connections. A `<listen />` element contains one obligatory attribute `spec`, attributes of which define an interface to "listen" incoming client connections and whether the `discovery` mode is enabled on this interface. The spec attribute contains following properties:

- ◆ `protocol` – type of the protocol for receiving incoming connections. Address which the **Proxy server** listens is set as an attribute.
- ◆ `port` – port which the **Proxy server** listens.
- ◆ `imitation mode` – the mode of **Server** imitation. Allows detection of the **Proxy server** as **Enterprise Server** by the **Network scanner**.
- ◆ `multicast` – multicast group where the **Proxy server** is located.

Properties values of the `spec` attribute and their parameters are specified in the table G-1.

Table G-1. Properties of the spec element

Property	Obliga-tory	Possible values	Parameters of possible values	
			Allowed	**Default**
protocol	yes	`ip,` `ipx,` `netbios`		`0.0.0.0` `-` `-`
port	no	`port`		`2193`
imitation mode	no	`discovery`	`yes, no`	`no`
multicast	no	`multicast`		`231.0.0.1`

The `spec` attribute contains one obligatory `protocol` property and three non-obligatory properties, which are: `port`, `imitation mode` and `multicast`. Depending on value of the `protocol` property, the list of non-obligatory properties in the `spec` attribute may vary.

The G-2 table contains the list of non-obligatory properties, which can be set (+) or can not be set (-) in the `spec` attribute, depending on value of the `protocol` parameter.

Table G-2. Presence of non-obligatory properties in dependence of the value of protocol parameter

Protocol	Attribute presence		
	port	**discovery**	**multicast**
`ip`	+	+	+
`ipx`	+	+	–
`netbios`	+	+	–

The <forward /> element

Redirection of incoming connections is adjusted via the <**forward** /> element which is a child element of <**listen** />. The <**forward** /> element contains one or more obligatory to attributes whose values define addresses of **Enterprise Servers** where the connection should be redirected to. An address of **Enterprise Server** is specified according to the The Specification of Network Addresses, in particular, in the following format: tcp/<*DNS_name>*:<*port>*.

The <**forward** /> element is obligatory. Each <**listen** /> element can contain several <**forward** /> elements.

The forwarding algorithm for the list of Enterprise Servers

1. **Proxy server** loads to RAM the list of **Enterprise Servers** from the drwcsd-proxy.xml configuration file.

2. The **Enterprise Agent** connects to the **Proxy server**.

3. **Proxy server** forwards the **Enterprise Agent** to the first **Server** from the **Enterprise Servers** list loaded in the RAM.

4. **Proxy server** rotate the list in the RAM and moves the **Enterprise Server** from the first position to the end of list.

> **Proxy Server** does not save changed order of **Servers** to its configuration file. After restart of **Proxy server**, the list of **Enterprise Servers** is loaded to the RAM in original version, which is stored in the configuration file.

5. When the next **Agent** connects to the **Proxy server**, procedure is repeated from the step 2.

6. If the **Enterprise Server** disconnects from the antivirus network (e.g., gets offline or denies of service), the **Agent** connects to the **Proxy server** repeatedly and procedure is repeated from the step 2.

Example of drwcsd-proxy.xml configuration file

```xml
<?xml version="1.0"?>
<drwcsd-proxy>
  <!-- Specify path to cahe directory, if not specified
will create directory in user temp -->
  <cache-root>C:\Work\es_head\build\a-x86\bin\var</cache-
root>

  <!-- property: ip, ipx, netbios, unx: define protocol
family and address of addapter -->
  <!-- property: port: define port to listen on. Default
2193 or 23 for netbios -->
  <!-- property: name: define discovery name. Default
drwcs -->
  <!-- property: discovery: define should proxy run
discovery server too -->
  <!-- property: multicast: define should proxy enter to
multicast group -->

  <!-- For example -->
  <!-- Listen on IN_ADDR_ANY port 2193, run discovery on
231.0.0.1 -->
  <listen spec="ip(), multicast()">
    <!-- one or more forward tags-->
    <forward to="tcp/server1.isp.net:2193"/>
    <forward to="tcp/server2.isp.net:2193"/>
  </listen>

  <!-- Listen on ipv6 IN6_ADDR_ANY, port 2194, run
discovery on ff18::231.0.0.1 -->
  <listen spec="ip([]), port(2194), multicast()">
    <forward to="tcp/server1.isp.net:2193"/>
    <forward to="tcp/server2.isp.net:2193"/>
  </listen>

  <!-- Listen on default ipx, port 2194, run simple
discovery -->
  <listen spec="ipx(), discovery()">
    <forward to="tcp/server1.isp.net:2193"/>
    <forward to="tcp/server2.isp.net:2193"/>
  </listen>

  <!-- Listen on default netbios, port 23, lana 0, run
simple discovery -->
  <listen spec="netbios(), discovery()">
    <forward to="tcp/server1.isp.net:2193"/>
```

```
    <forward to="tcp/server2.isp.net:2193"/>
  </listen>
</drwcsd-proxy>
```

Appendix H. Command Line Parameters of the Programs Included in Dr.Web Enterprise Security Suite

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. Dr.Web Enterprise Agent Interface Module

The **Agent** 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 start instruction format:

```
drwagnui [<switches>]
```

Possible switches:

◆ `-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** 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. Dr.Web Enterprise 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.

> **i**   **Agent** parameters which are set directly at the station are reset with parameters received from the **Server**.
>
> If the list of **Servers** to which the **Agent** connects, is set as empty at the **Server**, the list of **Servers** which is set at the station is used.

Enterprise Agent is run by the system as a service and is administrated through **Control Panel**.

The start instruction format:
`drwagntd [<switches>] [<servers>]`

Switches

Possible switches:

◆ `-compression=<mode>` — the compression mode of the traffic with the **Server**. Possible values are yes, no, possible, the default value is possible.

◆ `-control=`*<action>* — administrating the state of the **Agent** service.

Possible actions:

- `install` — install the service,
- `uninstall` — uninstall the service,
- `start` — run the service (only Windows NT OS and later),
- `stop` — terminate the service (only Windows NT OS and later),
- `restart` — restart the service (only Windows NT OS and later).

◆ `-crypt=`*<mode>* — the encryption mode of the traffic with the **Server**. Possible values are yes, no, possible, the default value is yes.

◆ `-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.

◆ `-help` — generate help on the format of the instruction and its parameters. The same is for -help of the interface module, read Appendix H2. Dr.Web Enterprise Agent Interface Module.

◆ `-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`.

◆ `-log=`*<log_file>* — **Agent** log file. By default it resides in the logs subfolder of the **Agent** installation folder. When uninstalling the **Agent** software, the deinstallation log is saved to the system temporary folder.

◆ `-retry=`*<quantity>* — the number of attempts to locate the **Server** by sending multicast-requests (if **Server** search is used) before the failure is reported. **3** is set by default.

◆ `-rotate=`*<N><f>,<M><u>* - **Agent** log rotation mode,

where:

- *<N>* - total number of log files (including current log file);
- *<f>* - log files storage format, possible values: `z` (gzip) - compress file, uses by default, or `p` (plain) - do not compress files.
- *<M>* - file size;
- *<u>* - unit measure, possible values: `k` (kilo), `m` (mega), `g` (giga).

By default, it is `10,10m`, which means storing of 10 files 10 megabytes each, use compression. Alternatively you can use the `none` format (`-rotate=none`), which means "do not use rotation, always write to the same file of unlimited size".

In the rotation mode, log file names are generated as follows: `file.<N>.log` or `file.<N>.log.dz`, where *<N>* - sequence number: 1, 2, etc.

For example, the log file name is set to `file.log` (see the `-log` switch above), then

- `file.log` — current log file,
- `file.1.log` — previous log file,
- `file.2.log` and so on — the greater the number, the older the version of the log.

◆ `-save` *<IP_address>* — verifies **Server** IP address value and saves parameters in registry.

◆ `-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.

◆ `-timeout=`*<time>* — the waiting limit of each reply in seconds for **Server** searching. Reply messages reception will be active, while the reply waiting time is not exceed the timeout value. **5** is set by default.

◆ `-trace` — to log in detail the location of error origin.

◆ `-verbosity=`*<details_level>* — log level of detail. `INFO` is

by default. Allowed values are: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. The `ALL` and `DEBUG3` values are synonyms (see also Appendix L. Log Files Format).

> **i** 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.
>
> The `-verbosity` and `-log` switches are position-relative.
>
> In case of using these keys simultaneously, the `-verbosity` switch must be set before the `-log` switch: the `-verbosity` switch redefines detail level of logs, that reside in folder, specified in the following switch.

Servers

<servers> — list of **Servers**. By default - `drwcs@udp/231.0.0.1:2193`, which instructs to search the drwcs **Server** using multicast requests for group `231.0.0.1` `port 2193`.

H4. Network Installer

The start instruction format:
`drwinst [<switches>] [<variables>] [<servers>]`

Switches

Possible switches:

◆ `-key=`*<public_key>* — full path to the **Server** public key file. 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 (see the `-script` switch). If the script is not explicitly provided, the internal script will be executed.

If such switch is missing (equals to `-no-uninstall`), installation is performed.

◆ `-script=<script_name>` — sets a file with the executable script. It is used with the `-uninstall` switch for the anti-virus software deinstallation.

◆ `-interactive` — run the installer in the interactive mode.

The **Agent** installation in the installer interactive (graphical) mode is described in the Installing the Dr.Web Enterprise Agent section.

If the `-interactive` switch is not set, the **Agent** installation will be launched in the background mode of the installer (see the Installing the Dr.Web Enterprise Agent section). But the interactive graphical mode of the installer can be displayed, if installation error or launch installation error is occurred.

> When installing **Agent** software remotely through the **Dr.Web Control Center**, this key will not work.
>
> The `-interactive` key can not be used with variables simultaneously. If variables are set, they will be ignored.

◆ `-retry=<quantity>` — similar to **Agent**.

◆ `-timeout=<time>` — similar to **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.

◆ `-id=<station_id>` — sets identifier for the station on which **Agent** will be installed.

◆ -log=*<log_file>* — the folder for the installation and deinstallation logs. Full path to the installation log file (it is set for the **Agent** installation) or deinstallation log file (it is set for the **Agent** unistallation).

By default, installation logs are saved to the logs subfolder set by -home for installation.

By default, deinstallation logs are saved to the folder selected by the user for storage of temporary files.

> **i** If the -log switch is not set, 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.

> **i** 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.
>
> The -verbosity and -log switches are position-relative.
>
> In case of using these keys simultaneously, the -verbosity switch must be set before the -log switch: the -verbosity switch redefines detail level of logs, that reside in folder, specified in the following switch.

◆ -regagent — register the **Agent** in the list **Add or Remove Programs**.
◆ -platforms=p1,p2,p3... – platforms load order (it is standard by default, read Appendix J. Using the Script of Dr.Web Enterprise Agent Initial Installation).
◆ -pwd=*<password>* — set the **Agent** password for access to the **Server**.
◆ -help — offer help. Similar to the **Agent** interface module.
◆ -trace — to log in detail the location of error origin.

Variables

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"` – 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**.

◆ `spidergate.install=no` — similarly; do not install **SpIDer Gate**.

◆ `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.

Servers

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.

Commands described in p. <u>H5.1</u> – <u>H5.5</u> are crossplatform and enable using in both Windows OS and UNIX system-based OS, unless it is specified otherwise.

H5.1. Managing the Dr.Web Enterprise Server

`drwcsd` [*<switches>*] — set the parameters for the **Server** operation (the switches are described in more detail below).

H5.2. Basic Commands

- ◆ `drwcsd start` — run the **Server**.
- ◆ `drwcsd restart` — restart the **Server** (it is executed as the `stop` and then `start` pair).
- ◆ `drwcsd stop` — stop the **Server**.
- ◆ `drwcsd reconfigure` — reread and reboot the configuration file (it is performed quicker and without starting a new process).
- ◆ `drwcsd retemplate` – reread notification templates from the drive.
- ◆ `drwcsd verifyakey` *<key_file_path>* – verify the **Agent** key file (`agent.key`).
- ◆ `drwcsd verifyekey` *<key_file_path>* – verify the **Server** key file (`enterprise.key`).
- ◆ `drwcsd verifyconfig` *<config_file_path>* – verify the syntax of the **Server** configuration file (`drwcsd.conf`).

◆ `drwcsd stat` – log statistics to a file: CPU time, memory usage, etc. (for UNIX system-based OS - similar to `send_signal WINCH` or `kill SIGWINCH` commands).

H5.3. Database Commands

Database Initialization

`drwcsd` [*<keys>*] `initdb` *<Agent_key>* [*<DB_script>* [*<ini_file>* [*<password>*]]] — database initialization.

◆ *<Agent_key>* — path to **Agent** license key file `agent.key` (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 set the initial configuration of **Dr.Web** software 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**.

> ℹ️ A minus can be omitted, if the next parameters are missing.

Adjusting parameters of database initialization

If embedded database is used, initialization parameters can be set via an external file. The following command is used for this:

`drwcsd.exe initdbex` *<response-file>*

<response-file> - file with initialization parameters written line-by-line in the same order as the initdb parameters.

File format:

> *<path_to_key_file>*
>
> *<path_to_initdb.sql>*
>
> *<path_to_drweb32.ini>*
>
> *<administrator_password>*

> **i** If using a response file under Windows OS, any symbols are allowed in the administrator password.

Any strings following the necessary parameter in a particular case are optional. If a string consists of only the minus symbol "-", the default value is used (as in initdb).

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.

Database Upgrading

drwcsd upgradedb *<folder>* – run the **Server** to update the structure of the database at a version upgrade (see the update-db folder).

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).

Database Import

drwcsd importdb *<file>* – import the database from the specified file (the previous content of the database is deleted).

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).

H5.4. Repository Commands

◆ drwcsd syncrepository – synchronize the repository with the **GUS.** Stop the **Server** before initiating this instruction!

◆ drwcsd rerepository – reread the repository from the drive.

H5.5. Backup of Dr.Web Enterprise Server Critical Data

The following command creates backup copies of critical **Server** data (database contents, **Server** license key, private encryption key, **Server** configuration key, and **Dr.Web Control Center** 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 OS:
```
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.).

Starting from the **4.33** version, **ESS** 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**.

H5.6. Commands for Windows® OS Only

- ◆ drwcsd [*<switches>*] install — install the **Server** service in the system.
- ◆ drwcsd uninstall — uninstall the **Server** service from a system.
- ◆ drwcsd kill — perform emergency shutdown of the **Server** service (if normal termination failed). This instruction should not be used without extreme necessity.
- ◆ drwcsd silent — disable messages from the **Server**. Used in command files to disable **Server** interactivity.

H5.7. Commands for UNIX® System-Based OS Only

◆ `drwcsd config` – similar to `reconfigure` or `kill SIGHUP` commands – restart the **Server**.

◆ `drwcsd dumpimportdb` – log imported data to a database.

◆ `drwcsd interactive` – run the **Server**, but do not direct the control to the process.

◆ `drwcsd newkey` – generate a new encryption keys (`drwcsd.pri` and `drwcsd.pub`).

◆ `drwcsd readtempl` – reread notification templates from the drive.

◆ `drwcsd readrepo` – reread repository from the drive.

◆ `drwcsd selfcert` – generate a new SSL certificate (`certificate.pem`) and RSA private key (`private-key.pem`).

◆ `drwcsd shell` *<file_name>* – run the binary file.

◆ `drwcsd showpath` – show all program paths, registered in the system.

◆ `drwcsd status` – show the current status of the **Server** (running, stopped).

H5.8. The Description of Switches

Crossplatform Switches

◆ `-activation-key=`*<license_key>* — **Server** license key. By default, it is the `enterprise.key` file located in the etc subfolder of the root folder.

◆ `-bin-root=`*<folder_for_executables>* — the path to executable files. By default, it is the `bin` 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.

◆ `-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).

◆ `-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.

◆ `-hooks` — to permit the **Server** to perform user extension scripts located in the:

- for Windows OS: `var\extensions`

- for FreeBSD OS and Solaris OS: `/var/drwcs/extensions`

- for Linux OS: `/var/opt/drwcs/extensions`

subcatalog of the **Server** installation catalog. The scripts are meant for automation of the administrator work enabling quicker performance of certain tasks. All scripts are disabled by default.

◆ `-home=<root>` — **Server** installation folder (root folder). The structure of this folder is described in p. <u>Installing the Dr.Web Enterprise Server for Windows OS</u>. By default, it is the current folder at start.

◆ `-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).

◆ `-private-key=<private_key>` — private **Server** key. By default, it is `drwcsd.pri` in the etc subfolder of the root folder.

◆ `-rotate=<N><f>,<M><u>` - **Server** log rotation mode, where:

- *<N>* - total number of log files (including current log file);
- *<f>* - log files storage format, possible values: `z` (gzip) - compress file, uses by default, or `p` (plain) - do not compress files.
- *<M>* - file size;
- *<u>* - unit measure, possible values: `k` (kilo), `m` (mega), `g` (giga).

By default, it is `10,10m`, which means storing of 10 files 10 megabytes each, use compression. Alternatively you can use the `none` format (`-rotate=none`), which means "do not use rotation, always write to the same file of unlimited size".

In the rotation mode, log file names are generated as follows: `file.`*<N>*`.log` or `file.`*<N>*`.log.dz`, where *<N>* - sequence number: 1, 2, etc.

For example, the log file name is set to `file.log` (see the `-log` switch above), then

- `file.log` — current log file,
- `file.1.log` — previous log file,
- `file.2.log` and so on — the greater the number, the older the version of the log.

◆ `-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.

◆ `-verbosity=`*<details_level>* — log level of detail. `WARNING` is by default. Allowed values are: `ALL`, `DEBUG3`, `DEBUG2`, `DEBUG1`, `DEBUG`, `TRACE3`, `TRACE2`, `TRACE1`, `TRACE`, `INFO`, `NOTICE`, `WARNING`, `ERROR`, `CRIT`. The `ALL` and `DEBUG3` values are synonyms (see also Appendix L. Log Files Format).

> **i** 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.

The `-verbosity` and `-log` switches are position-relative.

In case of using these keys simultaneously, the `-verbosity` switch must be set before the `-log` switch: the `-verbosity` switch redefines detail level of logs, that reside in folder, specified in the following switch.

Switches for Windows OS Only

◆ `-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.

◆ `-trace` — to log in detail the location of error origin.

Switches for UNIX system-based OS Only

◆ `-etc=<path>` – path to the `etc` (`<var>/etc`) directory.

◆ `-pid=<file>` – a file to which the **Server** writes the identifier of its process.

◆ `-syslog=<mode>` – 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`.

> The `-syslog` and `-log` keys work together. I.e., if you start the **Server** with the `-syslog` key (e.g., `service drwcsd start -syslog=user`), the **Server** run with specified value for the `-syslog` key and with default value for the `-log` key.

◆ `-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).

H5.9. Variables for UNIX® System-Based OS Only

To make the administration of the **Server** under UNIX system-based OS easier, administrator is provided with variables resided in the `/etc/init.d/drwcsd` script file.

Correspondence between variables and command switches for the `drwcsd` is described in the Table H-1.

Table H-1.

Switch	Variable	Default parameters
-home	DRWCS_HOME	• `/usr/local/drwcs` - for the FreeBSD OS, • `/usr/drwcs` - for all other OS.
-var-root	DRWCS_VAR	
-etc	DRWCS_ETC	$DRWCS_VAR/etc
-rotate	DRWCS_ROT	10,10m
-verbosity	DRWCS_LEV	trace3
-log	DRWCS_LOG	$DRWCS_VAR/log/drwcsd.log
-conf	DRWCS_CFG	$DRWCS_ETC/drwcsd.conf
-pid	DRWCS_PID	
-user	DRWCS_USER	
-group	DRWCS_GROUP	
-hooks	DRWCS_HOOKS	
-trace	DRWCS_TRACE	

> `DRWCS_HOOKS` and `DRWCS_TRACE` variables do not have any parameters. If variables have been defined, corresponding switches will be added during the script execution. If variables have not been defined, switches will not be added.

Other variables are described in the Table H-2.

Table H-2.

Variables	Default parameters	Description
DRWCS_ADDOPT		
DRWCS_CORE	unlimited	The core file maximal size.
DRWCS_FILES	8192	The maximal number of file descriptors, that the **Server** is able to open.
DRWCS_BIN	$DRWCS_HOME/bin	The directory to start the drwcsd from.
DRWCS_LIB	$DRWCS_HOME/lib	The directory with **Server** libraries.

Default values of parameters will be used, if these variables have not been defined in the /etc/init.d/drwcsd script.

> DRWCS_HOME, DRWCS_VAR, DRWCS_ETC, DRWCS_USER, DRWCS_GROUP, DRWCS_HOOKS variables are already defined in the /etc/init.d/ drwcsd script file.
>
> If the ${TGT_ES_ETC}/common.conf file exists, this file will be included to the /etc/init.d/drwcsd, that could redefine some variables, but if they are not exported (using the export command), they will not take any effect.

To set variables, do the following:

1. Add variable definition to the /etc/init.d/drwcsd script file.
2. Export this variable using the export command (at the same place).
3. When one more process will be run from this script, this process will read values that have been set.

For Example:

To change log details level to maximum for the **Server**:

1. Add the following lines to the /etc/init.d/drwcsd:

```
DRWCS_LEV=ALL
export DRWCS_LEV
```

2. Start the **Server**, if it has been stopped:

/etc/init.d/drwcsd start (or service drwcsd start)

Or restart the **Server**, if it has been run:

/etc/init.d/drwcsd restart (or service drwcsd restart)

3. The log details level will possess the ALL value.

H5.10. Configuring the Dr.Web Enterprise Server Under UNIX System-Based OS

During **Server** installation under UNIX system-based OS, you will be prompt to configure some **Server** settings. You can initiate the configuration of **Server** settings manually (the perl environment must be installed). To do this, run the configure.pl script, that can be found in following directories:

◆ /usr/local/drwcs/bin/ for FreeBSD OS;

◆ /opt/drwcs/bin/ for Linux and Solaris OS.

The start instruction format:

configure.pl *<options>*

Possible switches:

◆ --proxy server=*<proxy_server>* – set the proxy server.

- user=*<proxy_user>* – set the proxy server user.
- password=*<proxy_password>* – set the proxy user account password.

◆ --stat server=*<stat_server>* – set the statistics server (stat.drweb.com:80 would be appropriate).

- url=*<url_on_server>* – set the url on statistics server (/update by default)
- interval=*<send_interval>* – set the interval between statistics sending.

◆ --initbase – initialize server database.

◆ --upgradebase – upgrade server database.

◆ --interactive – enter the interactive mode.

◆ --skip proxy=1 – skip one of the interactive stages.

- stat=1 |
- initbase=1 |
- upgradebase=1

◆ --verbose – show detailed information.

◆ --help | ? – show help message.

H6. Administrating Utility of the Internal Database

The administrating utility of the internal DB resides in the following folders:

◆ for **Linux** OS and **Solaris** OS: /opt/drwcs/bin

◆ for **FreeBSD** OS: /usr/local/drwcs/bin

◆ for **Windows** OS: *<Server_installation_folder>*\bin (by default, the **Server** installation folder is: C:\Program Files\DrWeb Enterprise Server).

The start instruction format:
drwidbsh *<path_to_DB_file>*

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. 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 check [-public-key=<public>] <file>` — check the file signature using *<public>* as a public key of a person who signed this file.
- `\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 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 help [<instruction>]` — brief help on the program and on the command line format.
- `\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   sign   [-private-key=`*`<private>`*`]` *`<file>`* — sign the *`<file>`* file using this private key.

H8. Administration of the Dr.Web Enterprise 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** processor by the `kill` utility.

> **i** 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 <u>H5.4</u>.

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.

H10. Proxy Server

To configure some of the **Proxy server** parameters, run with corresponding switches the `drwcsd-proxy` executable file, which resides in:

- ◆ For Windows OS: **Proxy server** installation folder.
- ◆ For UNIX system-based OS: `bin` subfolder of the **Proxy server** installation folder.

The start instruction format:

`drwcsd-proxy` *<switches>*

Possible switches:

- ◆ `--help` – show help message on switches for **Proxy server** setting.
- ◆ `--daemon` – for UNIX system-based OS only: run the **Proxy server** as daemon.
- ◆ `--control` *<arg>* – for Windows OS only: specify parameters for service configuration.

  Allowed parameters:

  - • `run` – (by default) run the **Proxy server** in a background mode as a Windows OS service.
  - • `install` – install the **Proxy server**.
  - • `uninstall` – uninstall the **Proxy server**.

- ◆ `--cfg` *<path>* – path to the **Proxy server** configuration file.
- ◆ `--pool-size` *<N>* – pool size for clients connections. Default is 2.
- ◆ `--trace` – enable detailed logging of **Proxy server** calls. Available only if the **Proxy server** supports calls stack tracing.
- ◆ `--use-console-log` – write **Proxy server** log to console.
- ◆ `--use-file-log` *<file>* – write **Proxy server** log to a file, where the *<file>* is a path to log file.

- ◆ `--rotate=<N><f>,<M><u>` – **Proxy server** log rotation mode, where:
  - • *<N>* - total number of log files (including current log file);
  - • *<f>* - log files storage format, possible values: `z` (gzip) - compress file, uses by default, or `p` (plain) - do not compress files.
  - • *<M>* - file size;
  - • *<u>* - unit measure, possible values: `k` (kilo), `m` (mega), `g` (giga).

By default, it is `10,10m`, which means storing of 10 files 10 megabytes each, use compression.

- ◆ `--verbosity=<details_level>` — log level of detail. `TRACE3` is by default. Allowed values are: `ALL, DEBUG3, DEBUG2, DEBUG1, DEBUG, TRACE3, TRACE2, TRACE1, TRACE, INFO, NOTICE, WARNING, ERROR, CRIT.` The `ALL` and `DEBUG3` values are synonyms.

> All switches for setting **Proxy server** parameters can be set simultaneously.
>
> Writing log to the file and to the console simultaneously is not supported. Meanwhile:
>> ◆ If none of switches is specified, log is written to the console.
>> ◆ If both of switches are specified, log is written to the file.

Appendix I. Environment Variables Exported by the Dr.Web Enterprise Server

To simplify the setting of the processes run by **Enterprise Server** on schedule, the data on location of the **Server** 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** 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** 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** launch; otherwise it is the var subfolder of the root folder.

Appendix J. Using the Script of Dr.Web Enterprise 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:

- `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 displaying the messages on the updating error, on the reboot request, etc. to a user. **0** — do not display, **1** — display a pop-up notification.

Now we create a nonstandard installation scenario in which SplDer 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 Security Suite

Some parameters of **Dr.Web ESS** are specified in the form of regular expressions. Processing of regular expressions is performed via the Perl Compatible Regular Expressions (PCRE) library.

Detailed description of the PCRE library syntax is available at http://www.pcre.org/.

This appendix contains only a brief description of the most common examples for using regular expressions.

K1. Options Used in Regular Expressions

Regular expressions are used in the configuration file and in the **Dr.Web Control Center** when objects to be excluded from scanning in the **Scanner** settings are specified.

Regular expressions 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 OS 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:

\qquad \\ \qquad 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

- ◆ `\011` is a tab followed by the character "3"
    `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

```
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
```

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 pattern. 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 subpatterns. 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.

Appendix L. Log Files Format

Events on the **Server** (see p.) and the **Agent** are logged into a text file, where every line is a separate message.

The format of a message line is as follows:

<year><month><day>.*<hour><minute><second>*.*<centisecond>*
<message_type>   [*<process_id>*]   *<thread_name>*
[*<message_source>*] *<message>*

where:

- ◆ *<year><month><date>*
  .*<hour><minute><second>*.*<hundredth_of_second>* – exact date of message entry to the log file.
- ◆ *<message_type>* – log level:
  - **ftl** (**Fatal error**) — instructs to inform only of the most severe errors;
  - **err** (**Error**) — notify of operation errors;
  - **wrn** (**Warning**) — warn about errors;
  - **ntc** (**Notice**) — display important information messages;
  - **inf** (**Info**) — display information messages;
  - **tr0..3** (**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;
  - **db0..3** (**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.

> The **tr0..3** (**trace**) and **db0..3** (**debug**) levels of detail are applicable for messsages for **Dr. Web ESS** developers only.

◆ [*<process_id>*] – unique numerical identifier of the process within which the thread that wrote the message to the log file was executed. Under certain OS [*<process_id>*] may be represented as [*<process_id> <thread_id>*].

◆ *<thread_name>* – character representation of the thread within which the message was logged.

◆ [*<message_source>*] – name of the system that initiated logging the message. The source is not always present.

◆ *<message>* – text description according to the log level. It may include both a formal description of the event and the values of certain event-relevant variables.

For example,

1) `20081023.171700.74 inf [001316] mth:12 [Sch] Job "Purge unsent IS events" said OK`

where:

◆ `20081023` – *<year><month><date>*,

◆ `171700` – *<hour><minute><second>*,

◆ `74` – *<hundredth_of_second>*,

◆ `inf` – *<message_type>*,

◆ `[001316]` – [*<process_id>*],

◆ `mth:12` – *<thread_name>*,

◆ `[Sch]` – [*<message_source>*],

◆ `Job "Purge unsent IS events" said OK` – *<message>* about the correct performance of the **Purge unsent IS** events job.

2) `20081028.135755.61 inf [001556] srv:0 tcp/10.3.0.55:3575/025D4F80:2: new connection at tcp/10.3.0.75:2193`

where:

◆ `20081028` – *<year><month><date>*,

◆ `135755` – *<hour><minute><second>*,

◆ `61` – *<hundredth_of_second>*,

◆ `inf` – *<message_type>*,

◆ `[001556]` – [*<process_id>*],

◆ `srv:0` – *<thread_name>*,

◆ `tcp/10.3.0.55:3575/025D4F80:2:        new connection at tcp/10.3.0.75:2193` – *<message>* about having established a new connection through the specified socket.

Appendix M. Custom Extensions

The extensions, implemented as a lua-scripts, are meant for automation of the administrator work enabling quicker performance of certain tasks of the **Enterprise Server**. These scripts are located in the folder:

- ◆ for Windows OS: `var\extensions`
- ◆ for FreeBSD OS and Solaris OS: `/var/drwcs/extensions`
- ◆ for Linux OS: `/var/opt/drwcs/extensions`

of **Server** installation folder. After the **Server** installation, preinstalled extension procedure are located in this folder. To permit the **Server** to perform user extension scripts, the **Server** must be launched with the `-hooks` switch.

All scripts are disabled by default. To enable scripts, you must remove the word `disabled` or remove entire comment (keep empty line).

The `extensions` folder contains following scripts:

- ◆ `access_check.ds` – called before check access against appropriate ACL (Access Control List);
- ◆ `access_denied.ds` – called when access denied according ACL settings or result of `access_check` procedure;
- ◆ `admin_logged.ds` – called when administrator successfully authenticate in the **Dr.Web Control Center**;
- ◆ `admin_noauth.ds` – called when administrator failed to authenticate in the **Dr.Web Control Center**;
- ◆ `agent_status.ds` – called when **Agent** report its local policy;
- ◆ `backup.ds` – called when backup completed but before deleting previous backup files;
- ◆ `bad_connection.ds` – called when new client connection cannot be established;
- ◆ `connection_denied.ds` – called when connection denied according license limitation;

- `database_load.ds` – called when database driver load process completed;
- `database_verify.ds` – called when database verification completed;
- `deinstallation.ds` – called when deinstallation of **Agent** completed;
- `disconnected.ds` – called when client disconnected;
- `group_changed.ds` – called when group properties changed;
- `group_created.ds` – called when new group created;
- `group_deleted.ds` – called when group deleted;
- `install.ds` – called when `installation` event occurred;
- `installed_components.ds` – called when **Agent** reported installed components;
- `jobexecuted.ds` – called when `job executed` event received from **Agent**;
- `license_error.ds` – called when new client connection cannot be established due license limitation;
- `load_plugin.ds` – called when plugin module loaded;
- `load_protocol.ds` – called when protocol module loaded;
- `neighbor_connected.ds` – called when server connected;
- `neighbor_install.ds` – called when `installation` event received from neighbor **Server**;
- `neighbor_noauth.ds` – called just after server connection rejected due (authorization) error;
- `neighbor_run_begin.ds` – called when `component started` event received from neighbor **Server**;
- `neighbor_run_end.ds` – called when `component completed` event received from neighbor **Server**;
- `neighbor_scan_error.ds` – called when `scan error` event received from neighbor **Server**;
- `neighbor_scan_statistics.ds` – called when `scan statistics` event received from neighbor **Server**;
- `neighbor_station_status.ds` – called when station

local policies/settings received from neighbor **Server**;

◆ `neighbor_virus.ds` – called when `virus detected` event received from neighbor **Server**;

◆ `newbie_accepted.ds` – called when newbie access granted, authorization is successful and station created in database;

◆ `newbie_came.ds` – called when newbie connected;

◆ `newbie_registered.ds` – called when newbie access granted but before information stored in database;

◆ `pong.ds` – called when `PONG` received from client;

◆ `run_begin.ds` – called when `component started` event received from **Agent**;

◆ `run_end.ds` – called when `component completed` event received from **Agent**;

◆ `scan_error.ds` – called when `scan error` event received from **Agent**;

◆ `scan_statistics.ds` – called when `scan statistics` event received from **Agent**;

◆ `server_jobexecuted.ds` – called when job executed on the server;

◆ `server_load.ds` – called when **Server** binary file loaded for execute some service function (the **Server** will not serve clients);

◆ `server_start.ds` – called when **Server** started and going to serve clients;

◆ `server_terminate.ds` – called when **Server** completed serve clients;

◆ `server_unload.ds` – called when **Server** completed execute some service function (the **Server** did not serve clients);

◆ `station_connected.ds` – called when **Agent** connected successfully;

◆ `station_create.ds` – called when station create completed;

◆ `station_date.ds` – called when invalid station time/date

detected;

◆ `station_deleted.ds` – called when station deleted;

◆ `station_noauth.ds` – called just after **Agent** connection rejected due authorization error;

◆ `station_update_failed.ds` - called after receiving a message from the **Agent** on update error at the station;

◆ `station_update_reboot.ds` - called after receiving a message from the **Agent** on requirement to restart the station after update;

◆ `unload_plugin.ds` – called when plugin module unloaded;

◆ `unload_protocol.ds` – called when protocol module unloaded;

◆ `virus.ds` – called when `virus detected` event received from **Agent**;

◆ `virusbases.ds` – called when **Agent** sent virus bases information.

Appendix N. Integration of XML Web API and Dr.Web Enterprise Security Suite

> The **XML Web API** is described in the **XML API for Dr.Web® Enterprise Security Suite** manual (see also Help section).

Application

XML Web API, when integrated to the **Dr.Web Enterprise Security Suite**, provides functions for operation of transactions with accounts and automatisation of service users management. You can use it, for example, to create dynamic pages to receive requests from users and send them installation files.

Authentication

The HTTP(S) protocol is used to interact with the **Enterprise Server**. XML API accepts RESET requests and replies with the XML. To get access to the XML API, the Basic HTTP authentication is used (in compliance with RFC 2617 standard). Contrary to RFC 2617 and related standards, the HTTP(S) server does not request credentials (i.e., **Dr.Web ESS** administrator account name and its password) from the client.

Appendix O. Procedures for Authentication of Administrators

> General information on authentication of administrators at the **Enterprise Server** is described in p. Authentication of Administrators.

Active Directory Authentication

Only enabling of using authentication method and the order in authenticators list are configured: in the <**enabled**/> and <**order**/> tags of the `auth-ads.xml` configuration file.

Operation principle:

1. Administrator specifies username and password in one of the following formats:
   - `username`,
   - `domain\username`,
   - `username@domain`,
   - user's LDAP DN.
2. Server registers with these name and password at the default domain controller (or at the domain controller which specified in the username).
3. If registration failed, transition to the next authentication mechanizm is performed.
4. LDAP DN of registered user is determined.
5. For the object with determined DN, the `DrWeb_Admin` attribute is read. If it has `FALSE` value, authentication is admitted failed and transition to the next authentication mechanizm is performed.
6. The `DrWeb_AdminReadOnly` attribute is read. If it has `TRUE` value, administrator has read-only rights.
7. The `DrWeb_AdminGroupOnly` attribute is read. If it has

TRUE value, administrator has rights to manage certain groups only.

8. The DrWeb_AdminGroup attribute is read. It must contain the list of groups for managing by this administrator.

9. If any of attributes are not defined at this stage, they are searched in groups to which the user is included to. For each group, its parental groups are checked (search strategy - inward).

> **i** If any error occurs, transition to the next authentication mechanizm is performed.

The drwschema-modify.exe utility (is included to the **Server** distribution kit) creates in Active Directory a new object class and defines new attributes for this class.

Attributes have the following OID in the **Enterprise** space:

```
#define DrWeb_enterprise_OID      "1.3.6.1.4.1"
                // iso.org.dod.internet.private.enterprise
#define DrWeb_DrWeb_OID           DrWeb_enterprise_OID
  ".29690"      // DrWeb
#define DrWeb_EnterpriseSuite_OID DrWeb_DrWeb_OID
  ".1"          // EnterpriseSuite
#define DrWeb_Alerts_OID
DrWeb_EnterpriseSuite_OID ".1"          // Alerts
#define DrWeb_Vars_OID
DrWeb_EnterpriseSuite_OID ".2"          // Vars
#define DrWeb_AdminAttrs_OID
DrWeb_EnterpriseSuite_OID ".3"          // AdminAttrs

// 1.3.6.1.4.1.29690.1.3.1 (AKA
iso.org.dod.internet.private.enterprise.DrWeb.EnterpriseSu
ite.AdminAttrs.Admin)

#define DrWeb_Admin_OID           DrWeb_AdminAttrs_OID
  ".1"          // R/W admin
#define DrWeb_AdminReadOnly_OID   DrWeb_AdminAttrs_OID
  ".2"          // R/O admin
#define DrWeb_AdminGroupOnly_OID  DrWeb_AdminAttrs_OID
  ".3"          // Group admin
#define DrWeb_AdminGroup_OID      DrWeb_AdminAttrs_OID
  ".4"          // Admin's group
```

```
#define DrWeb_Admin_AttrName            "DrWebAdmin"
#define DrWeb_AdminReadOnly_AttrName
"DrWebAdminReadOnly"
#define DrWeb_AdminGroupOnly_AttrName
"DrWebAdminGroupOnly"
#define DrWeb_AdminGroup_AttrName       "DrWebAdminGroup"
```

Editing settings of Active Directory users is implemented manually at the Active Directory server (see p.).

Algorithm of attributes handling during authorization is the following:

1. User attributes are read.
2. If the `DrWebAdmin` attribute is set to `TRUE`, when:

    2.1. If some attributes are missing and the `DrWebInheritPermissions` attribute is set to `TRUE`, missing attributes are read from groups. As soon as all attributes are set, procedure of groups bypass stops. Thus, the sooner attributes are read, the bigger priority they have. Administrator access is confirmed.

    2.2. If some attributes are missing and the `DrWebInheritPermissions` attribute is set to `FALSE` (or undefined), administrator access is forbidden.

    2.3. If all attributes are set, administrator access is confirmed

3. If the `DrWebAdmin` attribute is set to `FALSE`, administrator access is forbidden.
4. If the `DrWebAdmin` attribute is undefined, when:

    4.1. If the `DrWebInheritPermissions` attribute is set to `TRUE`, attributes from groups are read. Further, similar to step 2.

    4.2. If the `DrWebInheritPermissions` attribute is set to `FALSE` (or undefined) similar to step 3.

LDAP Authentication

Settings are stored in the `auth-ldap.xml` configuration file.

General tags of the configuration file:

◆ `<enabled/>` and `<order/>` - similar to the Active Directory.

◆ `<server/>` specifies the LDAP server address.

◆ `<user-dn/>` defines rules for translation of name to the DN (Distinguished Name) using DOS-like masks.

In the `<user-dn/>` tag, the following wildcard characters are allowed:

- * replaces sequence of any characters, except . , = @ \ and spaces;
- # replaces sequence of any characters.

◆ `<user-dn-expr/>` defines rules for translation of name to the DN using regular expressions.

For example, the same rule in different variants:
```
<user-dn        user="*@example.com"        dn="CN=
\1,DC=example,DC=com"/>
<user-dn-expr   user="(.*)@example.com"     dn="CN=
\1,DC=example,DC=com"/>
```

`\1` .. `\9` defined the substitution place for values of the * symbol or expression in brackets at the template.

According to this principle, if the user name is specified as `login@example.com`, after translation you will get DN: `"CN=login,DC=example,DC=com"`.

◆ `<user-dn-extension-enabled/>` allows the `ldap-user-dn-translate.ds` (from the `extensions` folder) Lua-script execution for translation usernames to DN. This script runs after attempts of using the `user-dn`, `user-dn-expr` rules, if appropriate rule is not found. Script has one parameter - specified username. Script returns the string that contains DN or nothing. If appropriate rule is not found and script is disabled or returns nothing, specified username is used as it is.

◆ Attributes of LDAP object for DN determined as a result of translation and their possible values can be defined by tags (default values are presented):

```
<!-- DrWebAdmin attribute equivalent (OID
1.3.6.1.4.1.29690.1.3.1) -->
  <admin-attribute-name value="DrWebAdmin" true-
value="^TRUE$" false-value="^FALSE$"/>

  <!-- DrWebAdminGroupOnly attribute equivalent (OID
1.3.6.1.4.1.29690.1.3.2) -->
  <readonly-admin-attribute-name
value="DrWebAdminReadOnly"  true-value="^TRUE$" false-
value="^FALSE$"/>

  <!-- DrWebAdminGroupOnly attribute equivalent (OID
1.3.6.1.4.1.29690.1.3.3) -->
  <grouponly-admin-attribute-name
value="DrWebAdminGroupOnly" true-value="^TRUE$" false-
value="^FALSE$"/>

  <!-- DrWebAdminGroup attribute equivalent (OID
1.3.6.1.4.1.29690.1.3.4) -->
  <groups-admin-attribute-name
value="DrWebAdminGroup"/>
```

As a values of `true-value`/`false-value` parameters, regular expressions are specified.

◆ If undefined values of administrators attributes are present, and the `<group-reference-attribute-name value="memberOf"/>` tag is set in the configuration file, the value of the `memberOf` attribute is considered as the list of DN groups, to which this administrator is included, and the search of needed attributes is performed in this groups as for the Active Directory.

Appendix P. Licences

This section contains the list of third-party software libraries which are used by **Dr.Web ESS** software, information on their licensing and development projects addresses.

Third-party library	Licence	Project URL
boost	http://www.boost.org/users/license.html*	http://www.boost.org/
c-ares	MIT License*	http://c-ares.haxx.se/
Gecko SDK	Mozilla Public License* GNU Lesser General Public License* GNU General Public License*	https://developer.mozilla.org/ru/docs/Gecko_SDK
jQuery	MIT License* GNU General Public License*	http://jquery.com/
libcurl	http://curl.haxx.se/docs/copyright.html*	http://curl.haxx.se/libcurl/
libradius	© Juniper Networks, Inc.*	http://www.freebsd.org
libxml2	MIT License*	http://www.xmlsoft.org/
lua	MIT License*	http://www.lua.org/
lua-xmlreader	MIT License*	http://asbradbury.org/projects/lua-xmlreader/
md5 implementation	© WIDE Project*	–
Net-snmp	http://www.net-snmp.org/about/license.html*	http://www.net-snmp.org/
OpenLDAP	http://www.openldap.org/software/release/license.html*	http://www.openldap.org
OpenSSL	http://www.openssl.org/source/license.html*	http://www.openssl.org/

Third-party library	Licence	Project URL
Oracle Instant Client	http://www.oracle.com/technetwork/licenses/instant-client-lic-152016.html*	http://www.oracle.com
pcre	http://www.pcre.org/licence.txt*	http://www.pcre.org/
Prototype JavaScript framework	MIT License*	http://prototypejs.org/assets/2009/8/31/prototype.js
Regina Rexx Interpreter	GNU Lesser General Public License*	http://regina-rexx.sourceforge.net/
sha2 implementation	© Dr. Brian Gladman, Worcester, UK*	–
SQLite	Public Domain (http://www.sqlite.org/copyright.html)	http://www.sqlite.org/
wtl	Common Public License (http://opensource.org/licenses/cpl1.0.php)*	http://sourceforge.net/projects/wtl/
XML/SWF Charts	Bulk License (http://maani.us/xml_charts/index.php?menu=Buy)	http://www.maani.us/xml_charts/index.php?menu=Introduction
zlib	http://www.zlib.net/zlib_license.html*	http://www.zlib.net/

* - licence texts are listed below.

P1. Boost

```
Boost Software License - Version 1.0 - August 17th, 2003


Permission is hereby granted, free of charge, to any
person or organization obtaining a copy of the software
and accompanying documentation covered by this license
```

P2. Curl

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

P3. Libradius

Copyright 1998 Juniper Networks, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR

```
CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN
IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.


$FreeBSD: src/lib/libradius/radlib_private.h,v 1.6.30.3
2012/04/21 18:30:48 melifaro Exp $
```

P4. MD5 implementation

```
Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project.

All rights reserved.


Redistribution and use in source and binary forms, with
or without modification, are permitted provided that the
following conditions are met:

1. Redistributions of source code must retain the above
   copyright notice, this list of conditions and the
   following disclaimer.

2. Redistributions in binary form must reproduce the
   above copyright notice, this list of conditions and
   the following disclaimer in the documentation and/or
   other materials provided with the distribution.

3. Neither the name of the project nor the names of its
   contributors may be used to endorse or promote
   products derived from this software without specific
   prior written permission.


THIS SOFTWARE IS PROVIDED BY THE PROJECT AND
CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL
THE PROJECT OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
```

INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF SUCH DAMAGE.

P5. Net-snmp

Various copyrights apply to this package, listed in
various separate parts below. Please make sure that you
read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

        Copyright 1989, 1991, 1992 by Carnegie Mellon
University

      Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University
of California

      All Rights Reserved

Permission to use, copy, modify and distribute this
software and its documentation for any purpose and
without fee is hereby granted, provided that the above
copyright notice appears in all copies and that both
that copyright notice and this permission notice appear
in supporting documentation, and that the name of CMU
and The Regents of the University of California not be
used in advertising or publicity pertaining to
distribution of the software without specific written
permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND

CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL
THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice
(BSD) -----

Portions of this code are copyright (c) 2001-2003,
Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with
or without modification, are permitted provided that the
following conditions are met:

* Redistributions of source code must retain the above
copyright notice, this list of conditions and the
following disclaimer.

* Redistributions in binary form must reproduce the
above copyright notice, this list of conditions and the
following disclaimer in the documentation and/or other
materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used
to endorse or promote products derived from this
software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

*   Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2009, Sparta, Inc

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 8: Apple Inc. copyright notice (BSD) -----

Copyright (c) 2007 Apple Inc. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Apple Inc. ("Apple") nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY APPLE AND ITS CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL APPLE OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 9: ScienceLogic, LLC copyright notice (BSD) -----

Copyright (c) 2009, ScienceLogic, LLC

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of ScienceLogic, LLC nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

P6. OpenLDAP

The OpenLDAP Public License

  Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following

  disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time.

Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ''AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR (S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

```
OpenLDAP  is  a  registered  trademark  of  the  OpenLDAP
Foundation.


Copyright  1999-2003  The  OpenLDAP  Foundation,  Redwood
City,

California,  USA.   All  Rights  Reserved.   Permission  to
copy and

distribute verbatim copies of this document is granted.
```

P7. OpenSSL

```
LICENSE ISSUES

  ==============


  The OpenSSL toolkit stays under a dual license, i.e.
both  the  conditions  of  the  OpenSSL  License  and  the
original SSLeay license apply to the toolkit.

  See below for the actual license texts. Actually both
licenses are BSD-style Open Source licenses. In case of
any  license  issues  related  to  OpenSSL  please  contact
openssl-core@openssl.org.


  OpenSSL License

  ---------------



 ================================================
  Copyright (c) 1998-2011 The OpenSSL Project.   All
rights reserved.


  Redistribution  and  use  in  source  and  binary  forms,
with  or  without  modification,  are  permitted  provided
that the following conditions are met:
```

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ''AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ''AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING

```
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF SUCH DAMAGE.


   The licence and distribution terms for any publically
available version or derivative of this code cannot be
changed.  i.e. this code cannot simply be copied and put
under another distribution licence

   [including the GNU Public Licence.]
```

P8. Oracle Instant Client

```
Export Controls on the Programs

Selecting the "Accept License Agreement" button is a
confirmation of your agreement that you comply, now and
during the trial term, with each of the following
statements:


-You are not a citizen, national, or resident of, and
are not under control of, the government of Cuba, Iran,
Sudan, Libya, North Korea, Syria, nor any country to
which the United States has prohibited export.

-You will not download or otherwise export or re-export
the Programs, directly or indirectly, to the above
mentioned countries nor to citizens, nationals or
residents of those countries.

-You are not listed on the United States Department of
Treasury lists of Specially Designated Nationals,
Specially Designated Terrorists, and Specially
Designated Narcotic Traffickers, nor are you listed on
the United States Department of Commerce Table of Denial
Orders.


You will not download or otherwise export or re-export
the Programs, directly or indirectly, to persons on the
above mentioned lists.


You will not use the Programs for, and will not allow
```

the Programs to be used for, any purposes prohibited by United States law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical or biological weapons of mass destruction.

EXPORT RESTRICTIONS

You agree that U.S. export control laws and other applicable export and import laws govern your use of the programs, including technical data; additional information can be found on Oracle®'s Global Trade Compliance web site (http://www.oracle.com/products/export).

You agree that neither the programs nor any direct product thereof will be exported, directly, or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation.

Oracle Employees: Under no circumstances are Oracle Employees authorized to download software for the purpose of distributing it to customers. Oracle products are available to employees for internal use or demonstration purposes only. In keeping with Oracle's trade compliance obligations under U.S. and applicable multilateral law, failure to comply with this policy could result in disciplinary action up to and including termination.

Note: You are bound by the Oracle Technology Network ("OTN") License Agreement terms. The OTN License Agreement terms also apply to all updates you receive under your Technology Track subscription.

The OTN License Agreement terms below supercede any shrinkwrap license on the OTN Technology Track software CDs and previous OTN License terms (including the Oracle Program License as modified by the OTN Program Use Certificate).

Oracle Technology Network Development and Distribution
License Agreement for Instant Client

"We," "us," and "our" refers to Oracle America, Inc.
"You" and "your" refers to the individual or entity that
wishes to use the Programs from Oracle under this
Agreement. "Programs" refers to the Software Products
referenced below that you wish to download and use and
Program documentation. "License" refers to your right to
use the Programs and Program documentation under the
terms of this Agreement. The substantive and procedural
laws of California govern this Agreement. You and Oracle
agree to submit to the exclusive jurisdiction of, and
venue in, the courts of San Francisco, San Mateo, or
Santa Clara counties in California in any dispute
arising out of or relating to this Agreement.

We are willing to license the Programs to you only upon
the condition that you accept all of the terms contained
in this Agreement. Read the terms carefully and select
the "Accept" button at the bottom of the page to confirm
your acceptance. If you are not willing to be bound by
these terms, select the "Do Not Accept" button and the
registration process will not continue.

Software Product

- Instant Client

License Rights

License.

We grant you a non-exclusive right and license to use
the Programs solely for your business purposes and
development and testing purposes, subject to the terms
of this Agreement. You may allow third parties to use
the Programs, subject to the terms of this Agreement,
provided such third party use is for your business
operations only.

Distribution License

We grant you a non-exclusive right and license to distribute the Programs, provided that you do not charge your end users for use of the Programs. Your distribution of such Programs shall at a minimum include the following terms in an executed license agreement between you and the end user that: (1) restrict the use of the Programs to the business operations of the end user; (2) prohibit (a) the end user from assigning, giving, or transferring the Programs or an interest in them to another individual or entity (and if your end user grants a security interest in the Programs, the secured party has no right to use or transfer the Programs); (b) make the Programs available in any manner to any third party for use in the third party's business operations (unless such access is expressly permitted for the specific program license or materials from the services you have acquired); and (c) title to the Programs from passing to the end user or any other party; (3) prohibit the reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Programs and prohibit duplication of the Programs except for a sufficient number of copies of each Program for the end user's licensed use and one copy of each Program media; (4) disclaim, to the extent permitted by applicable law, our liability for any damages, whether direct, indirect, incidental, or consequential, arising from the use of the Programs; (5) require the end user at the termination of the Agreement, to discontinue use and destroy or return to you all copies of the Programs and documentation; (6) prohibit publication of any results of benchmark tests run on the Programs; (7) require the end user to comply fully with all relevant export laws and regulations of the United States and other applicable export and import laws to assure that neither the Programs, nor any direct product thereof, are exported, directly or indirectly, in violation of applicable laws; (8) do not require us to perform any obligations or incur any liability not previously agreed to between you and us; (9) permit you to audit your end user's use of the Programs or to assign your right to audit the end user's use of the Programs to us; (10) designate us as a third party beneficiary of the end user license agreement; (11) include terms consistent with those contained in the sections of this Agreement entitled "Disclaimer of Warranties" and Exclusive Remedies," "No Technical Support," "End of Agreement," "Relationship Between the

Parties," and "Open Source"; and (11) exclude the application of the Uniform Computer Information Transactions Act.

You may allow your end users to permit third parties to use the Programs on such end user's behalf for the purposes set forth in the end user license agreement, subject to the terms of such agreement. You shall be financially responsible for all claims and damages to us caused by your failure to include the required contractual terms set forth above in each end user license agreement between you and an end user. We are a third party beneficiary of any end user license agreement between you and the end user, but do not assume any of your obligations thereunder, and you agree that you will not enter into any end user license agreement that excludes us as a third party beneficiary and will inform your end users of our rights.

If you want to use the Programs for any purpose other than as expressly permitted under this Agreement you must contact us to obtain the appropriate license. We may audit your use of the Programs. Program documentation is either shipped with the Programs, or documentation may be accessed online at http://www.oracle.com/technetwork/indexes/documentation/index.html.

You agree to: (a) defend and indemnify us against all claims and damages caused by your distribution of the Programs in breach of this Agreement and/or failure to include the required contractual provisions in your end user agreement as stated above; (b) keep executed end user agreements and records of end user information including name, address, date of distribution and identity of Programs distributed; (c) allow us to inspect your end user agreements and records upon request; and, (d) enforce the terms of your end user agreements so as to effect a timely cure of any end user breach, and to notify us of any breach of the terms.

Ownership and Restrictions

We retain all ownership and intellectual property rights

in the Programs. You may make a sufficient number of
copies of the Programs for the licensed use and one copy
of the Programs for backup purposes.

You may not:

-use the Programs for any purpose other than as provided
above;

-charge your end users for use of the Programs;

-remove or modify any Program markings or any notice of
our proprietary rights;

-assign this agreement or give the Programs, Program
access or an interest in the Programs to any individual
or entity except as provided under this agreement;

-cause or permit reverse engineering (unless required by
law for interoperability), disassembly or decompilation
of the Programs;

-disclose results of any Program benchmark tests without
our prior consent.

Export

You agree that U.S. export control laws and other
applicable export and import laws govern your use of the
Programs, including technical data; additional
information can be found on Oracle's Global Trade
Compliance web site located at http://www.oracle.com/
products/export/index.html. You agree that neither the
Programs nor any direct product thereof will be
exported, directly, or indirectly, in violation of these
laws, or will be used for any purpose prohibited by
these laws including, without limitation, nuclear,
chemical, or biological weapons proliferation.

Disclaimer of Warranty and Exclusive Remedies

THE PROGRAMS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF
ANY KIND. WE FURTHER DISCLAIM ALL WARRANTIES, EXPRESS
AND IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED
WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR
PURPOSE OR NONINFRINGEMENT.

IN NO EVENT SHALL WE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR ENTIRE LIABILITY FOR DAMAGES HEREUNDER SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000).

No Technical Support

Our technical support organization will not provide technical support, phone support, or updates to you or end users for the Programs licensed under this agreement.

Restricted Rights

If you distribute a license to the United States government, the Programs, including documentation, shall be considered commercial computer software and you will place a legend, in addition to applicable copyright notices, on the documentation, and on the media label, substantially similar to the following:

NOTICE OF RESTRICTED RIGHTS

"Programs delivered subject to the DOD FAR Supplement are 'commercial computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement. Otherwise, programs delivered subject to the Federal Acquisition Regulations are 'restricted computer software' and use, duplication, and disclosure of the programs, including documentation, shall be subject to the restrictions in FAR 52.227-19, Commercial Computer Software-Restricted Rights (June 1987). Oracle Corporation, 500 Oracle Parkway, Redwood City, CA 94065."

End of Agreement

You may terminate this Agreement by destroying all copies of the Programs. We have the right to terminate your right to use the Programs if you fail to comply

with any of the terms of this Agreement, in which case you shall destroy all copies of the Programs.

Relationship Between the Parties

The relationship between you and us is that of licensee/licensor. Neither party will represent that it has any authority to assume or create any obligation, express or implied, on behalf of the other party, nor to represent the other party as agent, employee, franchisee, or in any other capacity. Nothing in this Agreement shall be construed to limit either party's right to independently develop or distribute software that is functionally similar to the other party's products, so long as proprietary information of the other party is not included in such software.

Open Source

"Open Source" software - software available without charge for use, modification and distribution - is often licensed under terms that require the user to make the user's modifications to the Open Source software or any software that the user 'combines' with the Open Source software freely available in source code form. If you use Open Source software in conjunction with the Programs, you must ensure that your use does not: (i) create, or purport to create, obligations of us with respect to the Oracle Programs; or (ii) grant, or purport to grant, to any third party any rights to or immunities under our intellectual property or proprietary rights in the Oracle Programs. For example, you may not develop a software program using an Oracle Program and an Open Source program where such use results in a program file(s) that contains code from both the Oracle Program and the Open Source program (including without limitation libraries) if the Open Source program is licensed under a license that requires any "modifications" be made freely available. You also may not combine the Oracle Program with programs licensed under the GNU General Public License ("GPL") in any manner that could cause, or could be interpreted or asserted to cause, the Oracle Program or any modifications thereto to become subject to the terms of the GPL.

Entire Agreement

You agree that this Agreement is the complete agreement
for the Programs and licenses, and this Agreement
supersedes all prior or contemporaneous Agreements or
representations. If any term of this Agreement is found
to be invalid or unenforceable, the remaining provisions
will remain effective.

Last updated: 01/24/08

Should you have any questions concerning this License
Agreement, or if you desire to contact Oracle for any
reason, please write:

Oracle America, Inc.

500 Oracle Parkway,

Redwood City, CA 94065

Oracle may contact you to ask if you had a satisfactory
experience installing and using this OTN software
download.

P9. PCRE

PCRE is a library of functions to support regular
expressions whose syntax and semantics are as close as
possible to those of the Perl 5 language.

Release 8 of PCRE is distributed under the terms of the
"BSD" licence, as specified below. The documentation for
PCRE, supplied in the "doc" directory, is distributed
under the same terms as the software itself.

The basic library functions are written in C and are
freestanding. Also included in the distribution is a set
of C++ wrapper functions, and a just-in-time compiler
that can be used to optimize pattern matching. These are

```
both optional features that can be omitted when the
library is built.


THE BASIC LIBRARY FUNCTIONS
---------------------------


Written by:      Philip Hazel

Email local part: ph10

Email domain:    cam.ac.uk


University of Cambridge Computing Service,

Cambridge, England.


Copyright (c) 1997-2013 University of Cambridge

All rights reserved.


PCRE JUST-IN-TIME COMPILATION SUPPORT
-------------------------------------


Written by:      Zoltan Herczeg

Email local part: hzmester

Emain domain:    freemail.hu


Copyright(c) 2010-2013 Zoltan Herczeg

All rights reserved.


STACK-LESS JUST-IN-TIME COMPILER
--------------------------------
```

```
Written by:       Zoltan Herczeg

Email local part: hzmester

Emain domain:     freemail.hu


Copyright(c) 2009-2013 Zoltan Herczeg

All rights reserved.


THE C++ WRAPPER FUNCTIONS

------------------------


Contributed by:   Google Inc.


Copyright (c) 2007-2012, Google Inc.

All rights reserved.


THE "BSD" LICENCE

-----------------


Redistribution and use in source and binary forms, with
or without modification, are permitted provided that the
following conditions are met:


     * Redistributions of source code must retain the
above copyright notice, this list of conditions and the
following disclaimer.


     * Redistributions in binary form must reproduce the
above copyright notice, this list of conditions and the
following disclaimer in the documentation and/or other
materials provided with the distribution.
```

      * Neither the name of the University of Cambridge
nor the name of Google Inc. nor the names of their
contributors may be used to endorse or promote products
derived from this software without specific prior
written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND
CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED
WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE
COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY
DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER
CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY
OF SUCH DAMAGE.

P10. Sha2 implementation

      Copyright (c) 2001, Dr Brian Gladman
<brg@gladman.me.uk>, Worcester, UK.

   All rights reserved.

   TERMS

   Redistribution and use in source and binary forms,
with or without modification, are permitted subject to
the following conditions:

   1. Redistributions of source code must retain the
above copyright notice, this list of conditions and the
following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The copyright holder's name must not be used to endorse or promote any products derived from this software without his specific prior written permission.

This software is provided 'as is' with no express or implied warranties of correctness or fitness for purpose.

This is a byte oriented version of SHA256 that operates on arrays of bytes stored in memory. The operation uses a type 'sha256_ctx' to hold details of the current hash state and uses the following three calls:

```
void sha256_begin(sha256_ctx ctx[])

void sha256_hash(const unsigned char data[], unsigned
long len, sha256_ctx ctx[])

void sha256_end(unsigned char hval[], sha256_ctx ctx
[])
```

The first subroutine initialises a hash computation by setting up the context in the sha256_ctx context.

The second subroutine hashes 8-bit bytes from array data[] into the hash state withinh sha256_ctx context, the number of bytes to be hashed being given by the the unsigned long integer len.

The third subroutine completes the hash calculation and places the resulting digest value in the array of 8-bit bytes hval[]

```
    This implementation of SHA256 also supports SHA384
and SHA512 but these hash functions depend on the use of
64-bit long integers and are not very efficient on 32-
bit machines. This code is NOT recommended for these
hash functions.


    My thanks to Erik Andersen <andersen@codepoet-
consulting.com> for testing this code on big-endian
systems and for his assistance with corrections
```

P11. Wtl

```
Common Public License Version 1.0


THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF
THIS COMMON PUBLIC LICENSE ("AGREEMENT"). ANY USE,
REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES
RECIPIENT'S ACCEPTANCE OF THIS AGREEMENT.


1. DEFINITIONS


"Contribution" means:


a) in the case of the initial Contributor, the initial
code and documentation distributed under this Agreement,
and


b) in the case of each subsequent Contributor:


i) changes to the Program, and


ii) additions to the Program;
```

where such changes and/or additions to the Program
originate from and are distributed by that particular
Contributor. A Contribution 'originates' from a
Contributor if it was added to the Program by such
Contributor itself or anyone acting on such
Contributor's behalf. Contributions do not include
additions to the Program which: (i) are separate modules
of software distributed in conjunction with the Program
under their own license agreement, and (ii) are not
derivative works of the Program.

"Contributor" means any person or entity that
distributes the Program.

"Licensed Patents " mean patent claims licensable by a
Contributor which are necessarily infringed by the use
or sale of its Contribution alone or when combined with
the Program.

"Program" means the Contributions distributed in
accordance with this Agreement.

"Recipient" means anyone who receives the Program under
this Agreement, including all Contributors.

2. GRANT OF RIGHTS

a) Subject to the terms of this Agreement, each
Contributor hereby grants Recipient a non-exclusive,
worldwide, royalty-free copyright license to reproduce,
prepare derivative works of, publicly display, publicly
perform, distribute and sublicense the Contribution of
such Contributor, if any, and such derivative works, in
source code and object code form.

b) Subject to the terms of this Agreement, each
Contributor hereby grants Recipient a non-exclusive,

worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form.

This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3. REQUIREMENTS

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

a) it complies with the terms and conditions of this Agreement; and

b) its license agreement:

i) effectively disclaims on behalf of all Contributors all warranties and conditions, express and implied, including warranties or conditions of title and non-infringement, and implied warranties or conditions of merchantability and fitness for a particular purpose;

ii) effectively excludes on behalf of all Contributors all liability for damages, including direct, indirect, special, incidental and consequential damages, such as lost profits;

iii) states that any provisions which differ from this Agreement are offered by that Contributor alone and not by any other party; and

iv) states that source code for the Program is available from such Contributor, and informs licensees how to obtain it in a reasonable manner on or through a medium customarily used for software exchange.

When the Program is made available in source code form:

a) it must be made available under this Agreement; and

b) a copy of this Agreement must be included with each copy of the Program.

Contributors may not remove or alter any copyright notices contained within the Program.

Each Contributor must identify itself as the originator of its Contribution, if any, in a manner that reasonably

allows subsequent Recipients to identify the originator
of the Contribution.

4. COMMERCIAL DISTRIBUTION

Commercial distributors of software may accept certain
responsibilities with respect to end users, business
partners and the like. While this license is intended to
facilitate the commercial use of the Program, the
Contributor who includes the Program in a commercial
product offering should do so in a manner which does not
create potential liability for other Contributors.
Therefore, if a Contributor includes the Program in a
commercial product offering, such Contributor
("Commercial Contributor") hereby agrees to defend and
indemnify every other Contributor ("Indemnified
Contributor") against any losses, damages and costs
(collectively "Losses") arising from claims, lawsuits
and other legal actions brought by a third party against
the Indemnified Contributor to the extent caused by the
acts or omissions of such Commercial Contributor in
connection with its distribution of the Program in a
commercial product offering. The obligations in this
section do not apply to any claims or Losses relating to
any actual or alleged intellectual property
infringement. In order to qualify, an Indemnified
Contributor must: a) promptly notify the Commercial
Contributor in writing of such claim, and b) allow the
Commercial Contributor to control, and cooperate with
the Commercial Contributor in, the defense and any
related settlement negotiations. The Indemnified
Contributor may participate in any such claim at its own
expense.

For example, a Contributor might include the Program in
a commercial product offering, Product X. That
Contributor is then a Commercial Contributor. If that
Commercial Contributor then makes performance claims, or
offers warranties related to Product X, those
performance claims and warranties are such Commercial
Contributor's responsibility alone. Under this section,
the Commercial Contributor would have to defend claims
against the other Contributors related to those
performance claims and warranties, and if a court
requires any other Contributor to pay any damages as a
result, the Commercial Contributor must pay those

damages.

5. NO WARRANTY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE
PROGRAM IS PROVIDED ON AN "AS IS" BASIS, WITHOUT
WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR
IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR
CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY
OR FITNESS FOR A PARTICULAR PURPOSE. Each Recipient is
solely responsible for determining the appropriateness
of using and distributing the Program and assumes all
risks associated with its exercise of rights under this
Agreement, including but not limited to the risks and
costs of program errors, compliance with applicable
laws, damage to or loss of data, programs or equipment,
and unavailability or interruption of operations.

6. DISCLAIMER OF LIABILITY

EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER
RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT
LIMITATION LOST PROFITS), HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
ARISING IN ANY WAY OUT OF THE USE OR DISTRIBUTION OF THE
PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER,
EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7. GENERAL

If any provision of this Agreement is invalid or
unenforceable under applicable law, it shall not affect
the validity or enforceability of the remainder of the
terms of this Agreement, and without further action by
the parties hereto, such provision shall be reformed to
the minimum extent necessary to make such provision
valid and enforceable.

If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient's patent(s), then such Recipient's rights granted under Section 2(b) shall terminate as of the date such litigation is filed.

All Recipient's rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient's rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient's obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive.

Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the

intellectual property of any Contributor under this
Agreement, whether expressly, by implication, estoppel
or otherwise. All rights in the Program not expressly
granted under this Agreement are reserved.

This Agreement is governed by the laws of the State of
New York and the intellectual property laws of the
United States of America. No party to this Agreement
will bring a legal action under this Agreement more than
one year after the cause of action arose. Each party
waives its rights to a jury trial in any resulting
litigation.

P12. Zlib

zlib.h -- interface of the 'zlib' general purpose
compression library

  version 1.2.8, April 28th, 2013

   Copyright (C) 1995-2013 Jean-loup Gailly and Mark
Adler

This software is provided 'as-is', without any express
or implied warranty. In no event will the authors be
held liable for any damages arising from the use of this
software.

Permission is granted to anyone to use this software for
any purpose, including commercial applications, and to
alter it and redistribute it freely, subject to the
following restrictions:

1. The origin of this software must not be
   misrepresented; you must not claim that you wrote the
   original software. If you use this software in a
   product, an acknowledgment in the product
   documentation would be appreciated but is not
   required.

2. Altered source versions must be plainly marked as
   such, and must not be misrepresented as being the
   original software.

3. This notice may not be removed or altered from any
   source distribution.

   Jean-loup Gailly   Mark Adler

   jloup@gzip.org   madler@alumni.caltech.edu

P13. MIT License

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any
person obtaining a copy of this software and associated
documentation files (the "Software"), to deal in the
Software without restriction, including without
limitation the rights to use, copy, modify, merge,
publish, distribute, sublicense, and/or sell copies of
the Software, and to permit persons to whom the Software
is furnished to do so, subject to the following
conditions:

The above copyright notice and this permission notice
shall be included in all copies or substantial portions
of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF
ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED
TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT
SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY
CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR
IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER
DEALINGS IN THE SOFTWARE.

P14. GNU General Public License

Version 3, 29 June 2007

Copyright © 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The GNU General Public License is a free, copyleft license for software and other kinds of works.

The licenses for most software and other practical works are designed to take away your freedom to share and change the works. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change all versions of a program--to make sure it remains free software for all its users. We, the Free Software Foundation, use the GNU General Public License for most of our software; it applies also to any other work released this way by its authors. You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for them if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs, and that you know you can do these things.

To protect your rights, we need to prevent others from denying you these rights or asking you to surrender the rights. Therefore, you have certain responsibilities if

you distribute copies of the software, or if you modify it: responsibilities to respect the freedom of others.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must pass on to the recipients the same freedoms that you received. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

Developers that use the GNU GPL protect your rights with two steps: (1) assert copyright on the software, and (2) offer you this License giving you legal permission to copy, distribute and/or modify it.

For the developers' and authors' protection, the GPL clearly explains that there is no warranty for this free software. For both users' and authors' sake, the GPL requires that modified versions be marked as changed, so that their problems will not be attributed erroneously to authors of previous versions.

Some devices are designed to deny users access to install or run modified versions of the software inside them, although the manufacturer can do so. This is fundamentally incompatible with the aim of protecting users' freedom to change the software. The systematic pattern of such abuse occurs in the area of products for individuals to use, which is precisely where it is most unacceptable. Therefore, we have designed this version of the GPL to prohibit the practice for those products. If such problems arise substantially in other domains, we stand ready to extend this provision to those domains in future versions of the GPL, as needed to protect the freedom of users.

Finally, every program is threatened constantly by software patents. States should not allow patents to restrict development and use of software on general-purpose computers, but in those that do, we wish to avoid the special danger that patents applied to a free program could make it effectively proprietary. To

prevent this, the GPL assures that patents cannot be used to render the program non-free.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS

0. Definitions.

"This License" refers to version 3 of the GNU General Public License.

"Copyright" also means copyright-like laws that apply to other kinds of works, such as semiconductor masks.

"The Program" refers to any copyrightable work licensed under this License. Each licensee is addressed as "you". "Licensees" and "recipients" may be individuals or organizations.

To "modify" a work means to copy from or adapt all or part of the work in a fashion requiring copyright permission, other than the making of an exact copy. The resulting work is called a "modified version" of the earlier work or a work "based on" the earlier work.

A "covered work" means either the unmodified Program or a work based on the Program.

To "propagate" a work means to do anything with it that, without permission, would make you directly or secondarily liable for infringement under applicable copyright law, except executing it on a computer or modifying a private copy. Propagation includes copying, distribution (with or without modification), making available to the public, and in some countries other activities as well.

To "convey" a work means any kind of propagation that enables other parties to make or receive copies. Mere interaction with a user through a computer network, with no transfer of a copy, is not conveying.

An interactive user interface displays "Appropriate Legal Notices" to the extent that it includes a convenient and prominently visible feature that (1) displays an appropriate copyright notice, and (2) tells the user that there is no warranty for the work (except to the extent that warranties are provided), that licensees may convey the work under this License, and how to view a copy of this License. If the interface presents a list of user commands or options, such as a menu, a prominent item in the list meets this criterion.

1. Source Code.

The "source code" for a work means the preferred form of the work for making modifications to it. "Object code" means any non-source form of a work.

A "Standard Interface" means an interface that either is an official standard defined by a recognized standards body, or, in the case of interfaces specified for a particular programming language, one that is widely used among developers working in that language.

The "System Libraries" of an executable work include anything, other than the work as a whole, that (a) is included in the normal form of packaging a Major Component, but which is not part of that Major Component, and (b) serves only to enable use of the work with that Major Component, or to implement a Standard Interface for which an implementation is available to the public in source code form. A "Major Component", in this context, means a major essential component (kernel, window system, and so on) of the specific operating system (if any) on which the executable work runs, or a compiler used to produce the work, or an object code interpreter used to run it.

The "Corresponding Source" for a work in object code

form means all the source code needed to generate, install, and (for an executable work) run the object code and to modify the work, including scripts to control those activities. However, it does not include the work's System Libraries, or general-purpose tools or generally available free programs which are used unmodified in performing those activities but which are not part of the work. For example, Corresponding Source includes interface definition files associated with source files for the work, and the source code for shared libraries and dynamically linked subprograms that the work is specifically designed to require, such as by intimate data communication or control flow between those subprograms and other parts of the work.

The Corresponding Source need not include anything that users can regenerate automatically from other parts of the Corresponding Source.

The Corresponding Source for a work in source code form is that same work.

2. Basic Permissions.

All rights granted under this License are granted for the term of copyright on the Program, and are irrevocable provided the stated conditions are met. This License explicitly affirms your unlimited permission to run the unmodified Program. The output from running a covered work is covered by this License only if the output, given its content, constitutes a covered work. This License acknowledges your rights of fair use or other equivalent, as provided by copyright law.

You may make, run and propagate covered works that you do not convey, without conditions so long as your license otherwise remains in force. You may convey covered works to others for the sole purpose of having them make modifications exclusively for you, or provide you with facilities for running those works, provided that you comply with the terms of this License in conveying all material for which you do not control copyright. Those thus making or running the covered works for you must do so exclusively on your behalf,

under your direction and control, on terms that prohibit them from making any copies of your copyrighted material outside their relationship with you.

Conveying under any other circumstances is permitted solely under the conditions stated below. Sublicensing is not allowed; section 10 makes it unnecessary.

3. Protecting Users' Legal Rights From Anti-Circumvention Law.

No covered work shall be deemed part of an effective technological measure under any applicable law fulfilling obligations under article 11 of the WIPO copyright treaty adopted on 20 December 1996, or similar laws prohibiting or restricting circumvention of such measures.

When you convey a covered work, you waive any legal power to forbid circumvention of technological measures to the extent such circumvention is effected by exercising rights under this License with respect to the covered work, and you disclaim any intention to limit operation or modification of the work as a means of enforcing, against the work's users, your or third parties' legal rights to forbid circumvention of technological measures.

4. Conveying Verbatim Copies.

You may convey verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice; keep intact all notices stating that this License and any non-permissive terms added in accord with section 7 apply to the code; keep intact all notices of the absence of any warranty; and give all recipients a copy of this License along with the Program.

You may charge any price or no price for each copy that you convey, and you may offer support or warranty protection for a fee.

5. Conveying Modified Source Versions.

You may convey a work based on the Program, or the modifications to produce it from the Program, in the form of source code under the terms of section 4, provided that you also meet all of these conditions:

a) The work must carry prominent notices stating that you modified it, and giving a relevant date.

b) The work must carry prominent notices stating that it is released under this License and any conditions added under section 7. This requirement modifies the requirement in section 4 to "keep intact all notices".

c) You must license the entire work, as a whole, under this License to anyone who comes into possession of a copy. This License will therefore apply, along with any applicable section 7 additional terms, to the whole of the work, and all its parts, regardless of how they are packaged. This License gives no permission to license the work in any other way, but it does not invalidate such permission if you have separately received it.

d) If the work has interactive user interfaces, each must display Appropriate Legal Notices; however, if the Program has interactive interfaces that do not display Appropriate Legal Notices, your work need not make them do so.

A compilation of a covered work with other separate and independent works, which are not by their nature extensions of the covered work, and which are not combined with it such as to form a larger program, in or on a volume of a storage or distribution medium, is called an "aggregate" if the compilation and its resulting copyright are not used to limit the access or legal rights of the compilation's users beyond what the individual works permit. Inclusion of a covered work in an aggregate does not cause this License to apply to the other parts of the aggregate.

6. Conveying Non-Source Forms.

You may convey a covered work in object code form under the terms of sections 4 and 5, provided that you also convey the machine-readable Corresponding Source under the terms of this License, in one of these ways:

a) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by the Corresponding Source fixed on a durable physical medium customarily used for software interchange.

b) Convey the object code in, or embodied in, a physical product (including a physical distribution medium), accompanied by a written offer, valid for at least three years and valid for as long as you offer spare parts or customer support for that product model, to give anyone who possesses the object code either (1) a copy of the Corresponding Source for all the software in the product that is covered by this License, on a durable physical medium customarily used for software interchange, for a price no more than your reasonable cost of physically performing this conveying of source, or (2) access to copy the Corresponding Source from a network server at no charge.

c) Convey individual copies of the object code with a copy of the written offer to provide the Corresponding Source. This alternative is allowed only occasionally and noncommercially, and only if you received the object code with such an offer, in accord with subsection 6b.

d) Convey the object code by offering access from a designated place (gratis or for a charge), and offer equivalent access to the Corresponding Source in the same way through the same place at no further charge. You need not require recipients to copy the Corresponding Source along with the object code. If the place to copy the object code is a network server, the Corresponding Source may be on a different server (operated by you or a third party) that supports equivalent copying facilities, provided you maintain clear directions next to the object code saying where to find the Corresponding Source. Regardless of what server hosts the Corresponding Source, you remain obligated to ensure that it is available for as long as needed to satisfy these requirements.

e) Convey the object code using peer-to-peer transmission, provided you inform other peers where the object code and Corresponding Source of the work are

being offered to the general public at no charge under subsection 6d.

A separable portion of the object code, whose source code is excluded from the Corresponding Source as a System Library, need not be included in conveying the object code work.

A "User Product" is either (1) a "consumer product", which means any tangible personal property which is normally used for personal, family, or household purposes, or (2) anything designed or sold for incorporation into a dwelling. In determining whether a product is a consumer product, doubtful cases shall be resolved in favor of coverage. For a particular product received by a particular user, "normally used" refers to a typical or common use of that class of product, regardless of the status of the particular user or of the way in which the particular user actually uses, or expects or is expected to use, the product. A product is a consumer product regardless of whether the product has substantial commercial, industrial or non-consumer uses, unless such uses represent the only significant mode of use of the product.

"Installation Information" for a User Product means any methods, procedures, authorization keys, or other information required to install and execute modified versions of a covered work in that User Product from a modified version of its Corresponding Source. The information must suffice to ensure that the continued functioning of the modified object code is in no case prevented or interfered with solely because modification has been made.

If you convey an object code work under this section in, or with, or specifically for use in, a User Product, and the conveying occurs as part of a transaction in which the right of possession and use of the User Product is transferred to the recipient in perpetuity or for a fixed term (regardless of how the transaction is characterized), the Corresponding Source conveyed under this section must be accompanied by the Installation Information. But this requirement does not apply if

neither you nor any third party retains the ability to install modified object code on the User Product (for example, the work has been installed in ROM).

The requirement to provide Installation Information does not include a requirement to continue to provide support service, warranty, or updates for a work that has been modified or installed by the recipient, or for the User Product in which it has been modified or installed. Access to a network may be denied when the modification itself materially and adversely affects the operation of the network or violates the rules and protocols for communication across the network.

Corresponding Source conveyed, and Installation Information provided, in accord with this section must be in a format that is publicly documented (and with an implementation available to the public in source code form), and must require no special password or key for unpacking, reading or copying.

7. Additional Terms.

"Additional permissions" are terms that supplement the terms of this License by making exceptions from one or more of its conditions. Additional permissions that are applicable to the entire Program shall be treated as though they were included in this License, to the extent that they are valid under applicable law. If additional permissions apply only to part of the Program, that part may be used separately under those permissions, but the entire Program remains governed by this License without regard to the additional permissions.

When you convey a copy of a covered work, you may at your option remove any additional permissions from that copy, or from any part of it. (Additional permissions may be written to require their own removal in certain cases when you modify the work.) You may place additional permissions on material, added by you to a covered work, for which you have or can give appropriate copyright permission.

Notwithstanding any other provision of this License, for material you add to a covered work, you may (if authorized by the copyright holders of that material) supplement the terms of this License with terms:

a) Disclaiming warranty or limiting liability differently from the terms of sections 15 and 16 of this License; or

b) Requiring preservation of specified reasonable legal notices or author attributions in that material or in the Appropriate Legal Notices displayed by works containing it; or

c) Prohibiting misrepresentation of the origin of that material, or requiring that modified versions of such material be marked in reasonable ways as different from the original version; or

d) Limiting the use for publicity purposes of names of licensors or authors of the material; or

e) Declining to grant rights under trademark law for use of some trade names, trademarks, or service marks; or

f) Requiring indemnification of licensors and authors of that material by anyone who conveys the material (or modified versions of it) with contractual assumptions of liability to the recipient, for any liability that these contractual assumptions directly impose on those licensors and authors.

All other non-permissive additional terms are considered "further restrictions" within the meaning of section 10. If the Program as you received it, or any part of it, contains a notice stating that it is governed by this License along with a term that is a further restriction, you may remove that term. If a license document contains a further restriction but permits relicensing or conveying under this License, you may add to a covered work material governed by the terms of that license document, provided that the further restriction does not survive such relicensing or conveying.

If you add terms to a covered work in accord with this section, you must place, in the relevant source files, a

statement of the additional terms that apply to those files, or a notice indicating where to find the applicable terms.

Additional terms, permissive or non-permissive, may be stated in the form of a separately written license, or stated as exceptions; the above requirements apply either way.

8. Termination.

You may not propagate or modify a covered work except as expressly provided under this License. Any attempt otherwise to propagate or modify it is void, and will automatically terminate your rights under this License (including any patent licenses granted under the third paragraph of section 11).

However, if you cease all violation of this License, then your license from a particular copyright holder is reinstated (a) provisionally, unless and until the copyright holder explicitly and finally terminates your license, and (b) permanently, if the copyright holder fails to notify you of the violation by some reasonable means prior to 60 days after the cessation.

Moreover, your license from a particular copyright holder is reinstated permanently if the copyright holder notifies you of the violation by some reasonable means, this is the first time you have received notice of violation of this License (for any work) from that copyright holder, and you cure the violation prior to 30 days after your receipt of the notice.

Termination of your rights under this section does not terminate the licenses of parties who have received copies or rights from you under this License. If your rights have been terminated and not permanently reinstated, you do not qualify to receive new licenses for the same material under section 10.

9. Acceptance Not Required for Having Copies.

You are not required to accept this License in order to receive or run a copy of the Program. Ancillary propagation of a covered work occurring solely as a consequence of using peer-to-peer transmission to receive a copy likewise does not require acceptance. However, nothing other than this License grants you permission to propagate or modify any covered work. These actions infringe copyright if you do not accept this License. Therefore, by modifying or propagating a covered work, you indicate your acceptance of this License to do so.

10. Automatic Licensing of Downstream Recipients.

Each time you convey a covered work, the recipient automatically receives a license from the original licensors, to run, modify and propagate that work, subject to this License. You are not responsible for enforcing compliance by third parties with this License.

An "entity transaction" is a transaction transferring control of an organization, or substantially all assets of one, or subdividing an organization, or merging organizations. If propagation of a covered work results from an entity transaction, each party to that transaction who receives a copy of the work also receives whatever licenses to the work the party's predecessor in interest had or could give under the previous paragraph, plus a right to possession of the Corresponding Source of the work from the predecessor in interest, if the predecessor has it or can get it with reasonable efforts.

You may not impose any further restrictions on the exercise of the rights granted or affirmed under this License. For example, you may not impose a license fee, royalty, or other charge for exercise of rights granted under this License, and you may not initiate litigation (including a cross-claim or counterclaim in a lawsuit) alleging that any patent claim is infringed by making, using, selling, offering for sale, or importing the Program or any portion of it.

11. Patents.

A "contributor" is a copyright holder who authorizes use under this License of the Program or a work on which the Program is based. The work thus licensed is called the contributor's "contributor version".

A contributor's "essential patent claims" are all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using, or selling its contributor version, but do not include claims that would be infringed only as a consequence of further modification of the contributor version. For purposes of this definition, "control" includes the right to grant patent sublicenses in a manner consistent with the requirements of this License.

Each contributor grants you a non-exclusive, worldwide, royalty-free patent license under the contributor's essential patent claims, to make, use, sell, offer for sale, import and otherwise run, modify and propagate the contents of its contributor version.

In the following three paragraphs, a "patent license" is any express agreement or commitment, however denominated, not to enforce a patent (such as an express permission to practice a patent or covenant not to sue for patent infringement). To "grant" such a patent license to a party means to make such an agreement or commitment not to enforce a patent against the party.

If you convey a covered work, knowingly relying on a patent license, and the Corresponding Source of the work is not available for anyone to copy, free of charge and under the terms of this License, through a publicly available network server or other readily accessible means, then you must either (1) cause the Corresponding Source to be so available, or (2) arrange to deprive yourself of the benefit of the patent license for this particular work, or (3) arrange, in a manner consistent with the requirements of this License, to extend the patent license to downstream recipients. "Knowingly relying" means you have actual knowledge that, but for

the patent license, your conveying the covered work in a country, or your recipient's use of the covered work in a country, would infringe one or more identifiable patents in that country that you have reason to believe are valid.

If, pursuant to or in connection with a single transaction or arrangement, you convey, or propagate by procuring conveyance of, a covered work, and grant a patent license to some of the parties receiving the covered work authorizing them to use, propagate, modify or convey a specific copy of the covered work, then the patent license you grant is automatically extended to all recipients of the covered work and works based on it.

A patent license is "discriminatory" if it does not include within the scope of its coverage, prohibits the exercise of, or is conditioned on the non-exercise of one or more of the rights that are specifically granted under this License. You may not convey a covered work if you are a party to an arrangement with a third party that is in the business of distributing software, under which you make payment to the third party based on the extent of your activity of conveying the work, and under which the third party grants, to any of the parties who would receive the covered work from you, a discriminatory patent license (a) in connection with copies of the covered work conveyed by you (or copies made from those copies), or (b) primarily for and in connection with specific products or compilations that contain the covered work, unless you entered into that arrangement, or that patent license was granted, prior to 28 March 2007.

Nothing in this License shall be construed as excluding or limiting any implied license or other defenses to infringement that may otherwise be available to you under applicable patent law.

12. No Surrender of Others' Freedom.

If conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the

conditions of this License, they do not excuse you from the conditions of this License. If you cannot convey a covered work so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not convey it at all. For example, if you agree to terms that obligate you to collect a royalty for further conveying from those to whom you convey the Program, the only way you could satisfy both those terms and this License would be to refrain entirely from conveying the Program.

13. Use with the GNU Affero General Public License.

Notwithstanding any other provision of this License, you have permission to link or combine any covered work with a work licensed under version 3 of the GNU Affero General Public License into a single combined work, and to convey the resulting work. The terms of this License will continue to apply to the part which is the covered work, but the special requirements of the GNU Affero General Public License, section 13, concerning interaction through a network will apply to the combination as such.

14. Revised Versions of this License.

The Free Software Foundation may publish revised and/or new versions of the GNU General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies that a certain numbered version of the GNU General Public License "or any later version" applies to it, you have the option of following the terms and conditions either of that numbered version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of the GNU General Public License, you may choose any version ever published by the Free Software Foundation.

If the Program specifies that a proxy can decide which future versions of the GNU General Public License can be

used, that proxy's public statement of acceptance of a version permanently authorizes you to choose that version for the Program.

Later license versions may give you additional or different permissions. However, no additional obligations are imposed on any author or copyright holder as a result of your choosing to follow a later version.

15. Disclaimer of Warranty.

THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. Limitation of Liability.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MODIFIES AND/OR CONVEYS THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

17. Interpretation of Sections 15 and 16.

If the disclaimer of warranty and limitation of liability provided above cannot be given local legal effect according to their terms, reviewing courts shall apply local law that most closely approximates an

```
absolute waiver of all civil liability in connection
with the Program, unless a warranty or assumption of
liability accompanies a copy of the Program in return
for a fee.


END OF TERMS AND CONDITIONS
```

P15. GNU Lesser General Public License

```
Version 3, 29 June 2007


Copyright © 2007 Free Software Foundation, Inc. <http://
fsf.org/>


Everyone is permitted to copy and distribute verbatim
copies of this license document, but changing it is not
allowed.


This version of the GNU Lesser General Public License
incorporates the terms and conditions of version 3 of
the GNU General Public License, supplemented by the
additional permissions listed below.

0. Additional Definitions.


As used herein, "this License" refers to version 3 of
the GNU Lesser General Public License, and the "GNU GPL"
refers to version 3 of the GNU General Public License.


"The Library" refers to a covered work governed by this
License, other than an Application or a Combined Work as
defined below.


An "Application" is any work that makes use of an
interface provided by the Library, but which is not
otherwise based on the Library. Defining a subclass of a
```

class defined by the Library is deemed a mode of using an interface provided by the Library.

A "Combined Work" is a work produced by combining or linking an Application with the Library. The particular version of the Library with which the Combined Work was made is also called the "Linked Version".

The "Minimal Corresponding Source" for a Combined Work means the Corresponding Source for the Combined Work, excluding any source code for portions of the Combined Work that, considered in isolation, are based on the Application, and not on the Linked Version.

The "Corresponding Application Code" for a Combined Work means the object code and/or source code for the Application, including any data and utility programs needed for reproducing the Combined Work from the Application, but excluding the System Libraries of the Combined Work.

1. Exception to Section 3 of the GNU GPL.

You may convey a covered work under sections 3 and 4 of this License without being bound by section 3 of the GNU GPL.

2. Conveying Modified Versions.

If you modify a copy of the Library, and, in your modifications, a facility refers to a function or data to be supplied by an Application that uses the facility (other than as an argument passed when the facility is invoked), then you may convey a copy of the modified version:

    a) under this License, provided that you make a good faith effort to ensure that, in the event an Application does not supply the function or data, the facility still operates, and performs whatever part of its purpose remains meaningful, or

b) under the GNU GPL, with none of the additional permissions of this License applicable to that copy.

3. Object Code Incorporating Material from Library Header Files.

The object code form of an Application may incorporate material from a header file that is part of the Library. You may convey such object code under terms of your choice, provided that, if the incorporated material is not limited to numerical parameters, data structure layouts and accessors, or small macros, inline functions and templates (ten or fewer lines in length), you do both of the following:

a) Give prominent notice with each copy of the object code that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the object code with a copy of the GNU GPL and this license document.

4. Combined Works.

You may convey a Combined Work under terms of your choice that, taken together, effectively do not restrict modification of the portions of the Library contained in the Combined Work and reverse engineering for debugging such modifications, if you also do each of the following:

a) Give prominent notice with each copy of the Combined Work that the Library is used in it and that the Library and its use are covered by this License.

b) Accompany the Combined Work with a copy of the GNU GPL and this license document.

c) For a Combined Work that displays copyright notices during execution, include the copyright notice for the Library among these notices, as well as a

reference directing the user to the copies of the GNU GPL and this license document.

d) Do one of the following:

0) Convey the Minimal Corresponding Source under the terms of this License, and the Corresponding Application Code in a form suitable for, and under terms that permit, the user to recombine or relink the Application with a modified version of the Linked Version to produce a modified Combined Work, in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.

1) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (a) uses at run time a copy of the Library already present on the user's computer system, and (b) will operate properly with a modified version of the Library that is interface-compatible with the Linked Version.

e) Provide Installation Information, but only if you would otherwise be required to provide such information under section 6 of the GNU GPL, and only to the extent that such information is necessary to install and execute a modified version of the Combined Work produced by recombining or relinking the Application with a modified version of the Linked Version. (If you use option 4d0, the Installation Information must accompany the Minimal Corresponding Source and Corresponding Application Code. If you use option 4d1, you must provide the Installation Information in the manner specified by section 6 of the GNU GPL for conveying Corresponding Source.)

5. Combined Libraries.

You may place library facilities that are a work based on the Library side by side in a single library together with other library facilities that are not Applications and are not covered by this License, and convey such a combined library under terms of your choice, if you do both of the following:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities, conveyed under the terms of

```
this License.

     b) Give prominent notice with the combined library
that part of it is a work based on the Library, and
explaining where to find the accompanying uncombined
form of the same work.


6. Revised Versions of the GNU Lesser General Public
License.


The Free Software Foundation may publish revised and/or
new versions of the GNU Lesser General Public License
from time to time. Such new versions will be similar in
spirit to the present version, but may differ in detail
to address new problems or concerns.


Each version is given a distinguishing version number.
If the Library as you received it specifies that a
certain numbered version of the GNU Lesser General
Public License "or any later version" applies to it, you
have the option of following the terms and conditions
either of that published version or of any later version
published by the Free Software Foundation. If the
Library as you received it does not specify a version
number of the GNU Lesser General Public License, you may
choose any version of the GNU Lesser General Public
License ever published by the Free Software Foundation.


If the Library as you received it specifies that a proxy
can decide whether future versions of the GNU Lesser
General Public License shall apply, that proxy's public
statement of acceptance of any version is permanent
authorization for you to choose that version for the
Library.
```

P16. Mozilla Public License

```
Version 2.0
1. Definitions
```

1.1. "Contributor"

    means each individual or legal entity that creates, contributes to the creation of, or owns Covered Software.

1.2. "Contributor Version"

    means the combination of the Contributions of others (if any) used by a Contributor and that particular Contributor's Contribution.

1.3. "Contribution"

   means Covered Software of a particular Contributor.

1.4. "Covered Software"

    means Source Code Form to which the initial Contributor has attached the notice in Exhibit A, the Executable Form of such Source Code Form, and Modifications of such Source Code Form, in each case including portions thereof.

1.5. "Incompatible With Secondary Licenses"

    means

       that the initial Contributor has attached the notice described in Exhibit B to the Covered Software; or

       that the Covered Software was made available under the terms of version 1.1 or earlier of the License, but not also under the terms of a Secondary License.

1.6. "Executable Form"

means any form of the work other than Source Code Form.

1.7. "Larger Work"

means a work that combines Covered Software with other material, in a separate file or files, that is not Covered Software.

1.8. "License"

means this document.

1.9. "Licensable"

means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently, any and all of the rights conveyed by this License.

1.10. "Modifications"

means any of the following:

any file in Source Code Form that results from an addition to, deletion from, or modification of the contents of Covered Software; or

any new file in Source Code Form that contains any Covered Software.

1.11. "Patent Claims" of a Contributor

means any patent claim(s), including without limitation, method, process, and apparatus claims, in any patent Licensable by such Contributor that would be infringed, but for the grant of the License, by the making, using, selling, offering for sale, having made,

import, or transfer of either its Contributions or its Contributor Version.

1.12. "Secondary License"

means either the GNU General Public License, Version 2.0, the GNU Lesser General Public License, Version 2.1, the GNU Affero General Public License, Version 3.0, or any later versions of those licenses.

1.13. "Source Code Form"

means the form of the work preferred for making modifications.

1.14. "You" (or "Your")

means an individual or a legal entity exercising rights under this License. For legal entities, "You" includes any entity that controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants and Conditions

2.1. Grants

Each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

under intellectual property rights (other than patent or trademark) Licensable by such Contributor to use, reproduce, make available, modify, display, perform, distribute, and otherwise exploit its Contributions, either on an unmodified basis, with Modifications, or as part of a Larger Work; and

under Patent Claims of such Contributor to make, use, sell, offer for sale, have made, import, and otherwise transfer either its Contributions or its Contributor Version.

2.2. Effective Date

The licenses granted in Section 2.1 with respect to any Contribution become effective for each Contribution on the date the Contributor first distributes such Contribution.

2.3. Limitations on Grant Scope

The licenses granted in this Section 2 are the only rights granted under this License. No additional rights or licenses will be implied from the distribution or licensing of Covered Software under this License. Notwithstanding Section 2.1(b) above, no patent license is granted by a Contributor:

for any code that a Contributor has removed from Covered Software; or

for infringements caused by: (i) Your and any other third party's modifications of Covered Software, or (ii) the combination of its Contributions with other software (except as part of its Contributor Version); or

under Patent Claims infringed by Covered Software in the absence of its Contributions.

This License does not grant any rights in the trademarks, service marks, or logos of any Contributor (except as may be necessary to comply with the notice requirements in Section 3.4).

2.4. Subsequent Licenses

No Contributor makes additional grants as a result of Your choice to distribute the Covered Software under a subsequent version of this License (see Section 10.2) or under the terms of a Secondary License (if permitted under the terms of Section 3.3).

2.5. Representation

Each Contributor represents that the Contributor believes its Contributions are its original creation(s) or it has sufficient rights to grant the rights to its Contributions conveyed by this License.

2.6. Fair Use

This License is not intended to limit any rights You have under applicable copyright doctrines of fair use, fair dealing, or other equivalents.

2.7. Conditions

Sections 3.1, 3.2, 3.3, and 3.4 are conditions of the licenses granted in Section 2.1.

3. Responsibilities

3.1. Distribution of Source Form

All distribution of Covered Software in Source Code Form, including any Modifications that You create or to which You contribute, must be under the terms of this License. You must inform recipients that the Source Code Form of the Covered Software is governed by the terms of this License, and how they can obtain a copy of this License. You may not attempt to alter or restrict the recipients' rights in the Source Code Form.

3.2. Distribution of Executable Form

If You distribute Covered Software in Executable Form then:

such Covered Software must also be made available in Source Code Form, as described in Section 3.1, and You must inform recipients of the Executable Form how they can obtain a copy of such Source Code Form by reasonable means in a timely manner, at a charge no more than the cost of distribution to the recipient; and

You may distribute such Executable Form under the terms of this License, or sublicense it under different terms, provided that the license for the Executable Form does not attempt to limit or alter the recipients' rights in the Source Code Form under this License.

3.3. Distribution of a Larger Work

You may create and distribute a Larger Work under terms of Your choice, provided that You also comply with the requirements of this License for the Covered Software. If the Larger Work is a combination of Covered Software with a work governed by one or more Secondary Licenses, and the Covered Software is not Incompatible With Secondary Licenses, this License permits You to additionally distribute such Covered Software under the terms of such Secondary License(s), so that the recipient of the Larger Work may, at their option, further distribute the Covered Software under the terms of either this License or such Secondary License(s).

3.4. Notices

You may not remove or alter the substance of any license notices (including copyright notices, patent notices, disclaimers of warranty, or limitations of liability) contained within the Source Code Form of the Covered Software, except that You may alter any license notices to the extent required to remedy known factual inaccuracies.

3.5. Application of Additional Terms

You may choose to offer, and to charge a fee for,

warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, You may do so only on Your own behalf, and not on behalf of any Contributor. You must make it absolutely clear that any such warranty, support, indemnity, or liability obligation is offered by You alone, and You hereby agree to indemnify every Contributor for any liability incurred by such Contributor as a result of warranty, support, indemnity or liability terms You offer. You may include additional disclaimers of warranty and limitations of liability specific to any jurisdiction.

4. Inability to Comply Due to Statute or Regulation

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Software due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be placed in a text file included with all distributions of the Covered Software under this License. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Termination

5.1. The rights granted under this License will terminate automatically if You fail to comply with any of its terms. However, if You become compliant, then the rights granted under this License from a particular Contributor are reinstated (a) provisionally, unless and until such Contributor explicitly and finally terminates Your grants, and (b) on an ongoing basis, if such Contributor fails to notify You of the non-compliance by some reasonable means prior to 60 days after You have come back into compliance. Moreover, Your grants from a particular Contributor are reinstated on an ongoing basis if such Contributor notifies You of the non-compliance by some reasonable means, this is the first time You have received notice of non-compliance with this License from such Contributor, and You become compliant prior to 30 days after Your receipt of the notice.

5.2. If You initiate litigation against any entity by asserting a patent infringement claim (excluding declaratory judgment actions, counter-claims, and cross-claims) alleging that a Contributor Version directly or indirectly infringes any patent, then the rights granted to You by any and all Contributors for the Covered Software under Section 2.1 of this License shall terminate.

5.3. In the event of termination under Sections 5.1 or 5.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or Your distributors under this License prior to termination shall survive termination.

6. Disclaimer of Warranty

Covered Software is provided under this License on an "as is" basis, without warranty of any kind, either expressed, implied, or statutory, including, without limitation, warranties that the Covered Software is free of defects, merchantable, fit for a particular purpose or non-infringing. The entire risk as to the quality and performance of the Covered Software is with You. Should any Covered Software prove defective in any respect, You (not any Contributor) assume the cost of any necessary servicing, repair, or correction. This disclaimer of warranty constitutes an essential part of this License. No use of any Covered Software is authorized under this License except under this disclaimer.

7. Limitation of Liability

Under no circumstances and under no legal theory, whether tort (including negligence), contract, or otherwise, shall any Contributor, or anyone who distributes Covered Software as permitted above, be liable to You for any direct, indirect, special, incidental, or consequential damages of any character including, without limitation, damages for lost profits, loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses, even if such party shall have been informed of the possibility of such damages. This limitation of liability shall not apply to liability for death or personal injury resulting from such party's negligence

to the extent applicable law prohibits such limitation. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so this exclusion and limitation may not apply to You.

8. Litigation

Any litigation relating to this License may be brought only in the courts of a jurisdiction where the defendant maintains its principal place of business and such litigation shall be governed by laws of that jurisdiction, without reference to its conflict-of-law provisions. Nothing in this Section shall prevent a party's ability to bring cross-claims or counter-claims.

9. Miscellaneous

This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not be used to construe this License against a Contributor.

10. Versions of the License

10.1. New Versions

Mozilla Foundation is the license steward. Except as provided in Section 10.3, no one other than the license steward has the right to modify or publish new versions of this License. Each version will be given a distinguishing version number.

10.2. Effect of New Versions

You may distribute the Covered Software under the terms of the version of the License under which You originally received the Covered Software, or under the terms of any subsequent version published by the license steward.

10.3. Modified Versions

If you create software not governed by this License, and you want to create a new license for such software, you may create and use a modified version of this License if you rename the license and remove any references to the name of the license steward (except to note that such modified license differs from this License).

10.4. Distributing Source Code Form that is Incompatible With Secondary Licenses

If You choose to distribute Source Code Form that is Incompatible With Secondary Licenses under the terms of this version of the License, the notice described in Exhibit B of this License must be attached.

Exhibit A - Source Code Form License Notice

This Source Code Form is subject to the terms of the Mozilla Public License, v. 2.0. If a copy of the MPL was not distributed with this file, You can obtain one at http://mozilla.org/MPL/2.0/.

If it is not possible or desirable to put the notice in a particular file, then You may include the notice in a location (such as a LICENSE file in a relevant directory) where a recipient would be likely to look for such a notice.

You may add additional accurate notices of copyright ownership.

Exhibit B - "Incompatible With Secondary Licenses" Notice

This Source Code Form is "Incompatible With Secondary Licenses", as defined by the Mozilla Public License, v. 2.0.

Frequently Asked Questions

Moving the Dr.Web Enterprise Server to Another Computer (under Windows® OS)

To transfer the Dr.Web Enterprise Server (for the similar Dr.Web Enterprise Server versions) under Windows OS:

1. Stop the **Server** (see Start and Stop the Dr.Web Enterprise Server).

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" exportdb <file_path>
   ```

3. Backup the `C:\Program Files\DrWeb Enterprise Server\etc` folder and the `drwcsd.pub` key from the `\Program Files\DrWeb Enterprise Server \Installer` folder.

4. Remove **Enterprise Server** software.

5. Install the new **Server** (empty, with the new DB) at the necessary computer. Stop the **Server** via the Windows OS service administrative loots or via the **Dr.Web Control Center**.

6. Copy the automatic saved `etc` folder to the `C:\Program Files\DrWeb Enterprise Server\etc` folder and the `drwcsd.pub` key to the `C:\Program Files \DrWeb Enterprise Server\Installer` folder.

7. Run `drwcsd.exe` using the `importdb` switch to import the content of the database from a file. The full command line (for Windows) looks as follows:

```
"C:\Program Files\DrWeb Enterprise Server\bin
\drwcsd.exe" importdb <file_path>
```

8. Start the **Server** (see Start and Stop the Dr.Web Enterprise Server).

> In case of using internal DB, it is not necessary to export and import DB. Just save the dbinternal.dbs file and replace the new DB file at the installed **Server** by an old DB file from the previous version of the **Server**.

To transfer the Dr.Web Enterprise Server (for the different Dr.Web Enterprise Server versions) under Windows OS:

1. Stop the **Server** (see Start and Stop the Dr.Web Enterprise Server).

2. Save the database via the SQL server tools (in case of using internal DB, just save the dbinternal.dbs file)

3. Backup the C:\Program Files\DrWeb Enterprise Server\etc folder and the drwcsd.pub key from the \Program Files\DrWeb Enterprise Server \Installer folder.

4. Remove **Enterprise Server** software.

5. Install the new **Server** (empty, with the new DB) at the necessary computer. Stop the **Server** via the Windows OS service administrative loots or via the **Dr.Web Control Center**.

6. Copy the automatic saved etc folder to the C:\Program Files\DrWeb Enterprise Server\etc folder and the drwcsd.pub key to the C:\Program Files \DrWeb Enterprise Server\Installer folder.

7. Restore the DB on new **Server** and specify the path to the DB in the configuration file.

8. Run drwcsd.exe using the upgradedb switch to upgrade the database. The full command line (for Windows) looks as follows:

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

9. Start the **Server** (see <u>Start and Stop the Dr.Web Enterprise Server</u>).

If Server IP address is changed during transfer:

1. Perform the **Server** transfer according to the corresponding procedure, described above.

2. For all **Agents**, which are served by transferred **Server**, specify the address of the new **Server** (see <u>Connecting the Dr.Web Enterprise Agent to Other Dr.Web Enterprise Server</u>).

3. For the possibility of transfer of **Agents** for which the new **Server** address is set via the **Control Center**, but not in the **Agent** settings at the station, keep both **Servers** operating (on both **Servers** in the **Agent** settings, the new **Server** IP address must be specified) till all **Agents** connect to the old **Server** to get the new IP address and complete transfer to the new **Server**.

Connecting the Dr.Web Enterprise Agent to Other Dr.Web Enterprise Server

> ⚠ To connect the **Agent** to other **Enterprise Server**, you must perform all actions at the station with the administrative rights.

To connect Dr.Web Enterprise Agent to other Dr.Web Enterprise Server, do the following:

1. If the `drwcsd.pub` public key of the new **Server** does not match with the public key of the old **Server**, you must change this key at the **Agent**:

    1.1. If the **SelfPROtect** component is active on the station with the **Agent**, disable it via the **Agent** context menu (to do this, you must have administrative rights at the station and rights for disabling the component, which are set at the **Server**).

    1.2. Copy the `drwcsd.pub` public key from the new **Server** to the **Agent** installation directory.

2. Change the **Server** address at the **Agent** settings:

    ◆ Via the **Dr.Web Control Center** (for the old **Server**): **Network** option of the main menu → **Dr.Web Enterprise Agent for Windows** option of the control menu → **Network** tab → **Server** field.

    ◆ At the station: **Settings** submenu of the **Agent** context menu → **Connection** option → **Server** field.

3. Set the station to the Newbie (reset parameters of connection with the **Server**):

    ◆ Via the **Dr.Web Control Center** (for the new **Server**): **Administration** option of the main menu → **Dr.Web Enterprise Server Configuration** option of the control menu → **General** tab → set the **Reset unauthorized to newbie** flag.

    ◆ At the station: **Settings** submenu of the **Agent** context menu → **Connection** option → **Newbie** button.

4. Restart the **Agent** service (see the Dr.Web Enterprise Agent section).

If rights for changing the Dr.Web Enterprise Agent settings are not allowed for the station, use the following procedure:

1. If the `drwcsd.pub` public key of the new **Server** does not match with the public key of the old **Server**, you must change this key at the **Agent**:

   ◆ If the **SelfPROtect** component is active on the station with the **Agent**, disable it via the **Agent** context menu (to do this, you must have administrative rights at the station and rights for disabling the component, which are set at the **Server**).

   ◆ Copy the `drwcsd.pub` public key from the new **Server** to the **Agent** installation directory.

2. Run the following command to specify the **Agent** settings:

   ```
   drwagntd -save <new_server_ip>
   ```

   where *<new_server_ip>* is the address of a new **Server**, to which the **Agent** must be connected. The address must be set according to the The Specification of Network Addresses.

3. Restart the **Agent** service (see the The Dr.Web Enterprise Agent section).

Changing the Type of the DBMS for Dr.Web Enterprise Security Suite

For Windows OS

1. Stop the **Enterprise Server** (see Start and Stop the Dr.Web Enterprise Server).

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 **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 clipboard 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 **Enterprise Server**, connect the **Dr.Web Control Center** to the **Server** and configure the **Server** to use a different DBMS. Cancel restarting the **Server**.

4. Stop the **Enterprise Server** (see Start and Stop the Dr.Web Enterprise Server).

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 the **Enterprise Server** (see Start and Stop the Dr.Web Enterprise Server).

For UNIX OS

1. Stop **Enterprise Server** using the script
   - for **Linux** OS and **Solaris** OS:

   ```
   /etc/init.d/drwcsd stop
   ```

   - for **FreeBSD** OS:

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

or via **Dr.Web Control Center** (except the Solaris OS).

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 **Solaris** OS:

```
"/etc/init.d/drwcsd   exportdb   /var/drwcs/
etc/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 **Enterprise Server** using the script

◆ for **Linux** OS and **Solaris** OS:

```
/etc/init.d/drwcsd start
```

◆ for **FreeBSD** OS:

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

connect **Dr.Web Control Center** to the **Server** and configure the **Server** to use another database through the **Dr.Web Control Center** 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 G1. Dr.Web
> Enterprise Server Configuration File).

You will be prompted to restart the **Server**. Reject restarting.

4. Stop **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 and **Solaris** 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 and **Solaris** OS:

   ```
   "/etc/init.d/drwcsd        importdb        /var/
   esbase.es"
   ```

   ◆ for **Solaris** OS:

   ```
   "/etc/init.d/drwcsd    importdb    /var/drwcs/
   etc/esbase.es"
   ```

   ◆ for **FreeBSD** OS:

   ```
   "/usr/local/etc/rc.d/drwcsd.sh    importdb    /
   var/esbase.es"
   ```

7. Start **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 Security Suite

Dr.Web ESS regularly backs up important data (database contents, **Server** license key, private encryption key, **Server** configuration key, and **Dr.Web Control Center** configuration key). The backup files are stored in the following folders (relatively to the **Server** installation folder):

- ◆ for **Windows** OS: `\var\Backup`
- ◆ for **Linux** OS: `/var/opt/drwcs/backup`
- ◆ for **FreeBSD** and **Solaris** OS: `/var/drwcs/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.

Restoring the DB for Different Versions of the Enterprise Server

You can restore the DB from the backup copy only if it had been created via the **Server** of the same major version as the version of the **Server** which you use for restoring.

For example:

- ◆ You can restore DB from the backup created via the **Server** of **5.0** version using the **Server** of **5.0** version only.
- ◆ You can restore DB from the backup created via the **Server** of **6.0** version using the **Server** of **6.0** version only.
- ◆ You cannot restore DB from the backup created via the **Server** of **5.0** or **4.XX** version using the **Server** of **6.0** version.

If DB has been corrupted for some reasons during Server upgrade from previous versions to 6.0 version, do the following:

1. Remove the **Server** software of **6.0** version. Backup copies of files, used by the **Server**, will be stored automatically.

2. Install the **Server** of version, which had been installed before upgrading and had been used to create backup copy.

   According to the general upgrade procedure, you should use all stored **Server** files except the DB file.

   Create a new DB during the **Server** installation.

3. Restore DB from the backup according to general rules (see procedures below).

4. Disable the **Agent**, the **Server** and the **Network Installer** protocols in the **Server** settings. To do this, select the **Administration** item in the main menu and click **Configure Dr.Web Enterprise Server** in the control menu, go to the **Modules** tab and clear corresponding flags.

5. Upgrade the **Server** to the **6.0** version according to general rules (see p.).

6. Enable the **Agent**, the **Server** and the **Network Installer** protocols, disabled at the step 4.

For Windows OS

To restore DB from backup:

1. Stop the **Enterprise Server** (if it is running, see).

2. 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 "<path_to_the_backup_file>
\database.dz"
```

The command must be entered in a single line. It is presumed that **Enterprise Server** is installed to the `C:\Program Files\DrWeb Enterprise Server` folder.

3. Start the **Enterprise Server** (see Start and Stop the Dr.Web Enterprise Server).

To restore DB from backup in case of changing the Dr.Web Enterprise Server version or corruption of the previous DB version:

1. Stop the **Enterprise Server** (if it is running, see Start and Stop the Dr.Web Enterprise Server).

2. Remove the current DB. To do this:

   2.1. For the internal DB:

   a) Remove `dbinternal.dbs` file.

   b) 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 - - <password>
   ```

   The command must be entered in a single line. (See also `drwcsd` command format with the `initdb` switch at the Appendix H5.3.). It is presumed that **Enterprise Server** is installed to the `C:\Program Files\DrWeb Enterprise Server` folder and `agent.key` is located in `D:\Keys`.

   c) Once this command is executed, a new `dbinternal.dbs` of about 200 Kb will be generated in the `var` subfolder of **Enterprise Server** installation folder.

2.2. For the external DB: cleanup the DB via the `clean.sql` script, located in the `etc` subfolder of **Enterprise Server** installation folder.

3. 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 **Enterprise Server** is installed to the `C:\Program Files\DrWeb Enterprise Server` folder.

4. Start the **Enterprise Server** (see Start and Stop the Dr.Web Enterprise Server).

For UNIX OS

1. Stop **Enterprise Server**.
   ◆ for **Linux** 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
   ◆ for **Linux** OS:

   ```
   /var/opt/drwcs/
   ```

   ◆ for **FreeBSD** OS and **Solaris** OS:

   ```
   /var/drwcs/
   ```

subfolder of the **Server** installation folder.

> To clean an external DB, use the `clean.sql` script, located at:
>
> ◆ `/var/opt/drwcs/etc` for **Linux** OS,
> ◆ `/var/drwcs/etc` for **Solaris** OS and **FreeBSD** OS.

3. Initialize the **Server** database. The command will look as follows:

   ◆ for **Linux** OS and **Solaris** OS:

```
/etc/init.d/drwcsd initdb
```

   ◆ for **FreeBSD** OS:

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

   ◆ for **other** supported versions:

```
su drwcs -c "bin/drwcsd -var-root=./var -
verbosity=all -log=./var/server.log initdb
etc/agent.key - - <password>"
```

4. Once this command is executed, a new `dbinternal.dbs` database of about 200 Kb will be generated in the `var` subfolder of **Enterprise Server** installation folder.

5. Import the content of the database from the correspondent backup. The command line will look as follows:

   ◆ for **Linux** OS and **Solaris** OS:

```
/etc/init.d/drwcsd importdb "/
<path_to_the_backup_file>/database.dz"
```

   ◆ for **FreeBSD** OS:

```
/usr/local/etc/rc.d/drwcsd.sh importdb "/
<path_to_the_backup_file>/database.dz"
```

   ◆ for **other** supported versions:

```
bin/drwcsd -var-root=./var -verbosity=all -
log=logfile.log importdb "/
```

<path_to_the_backup_file>/database.dz"

6. Start **Enterprise Server**:

◆ for **Linux** 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 you want to run the script with parameters (e.g., set **Server** installation directory, change log details level and etc.), you must make all changes in the start script:

◆ for **FreeBSD** OS: `/usr/local/etc/rc.d/ drwcsd.sh`

◆ for **Linux** and **Solaris** OS: `/etc/init.d/ drwcsd`

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 **Dr.Web Control Center** **Administration** menu, select **Configure Server**. A **Dr.Web Enterprise Server configuration** window will be opened on the **General** tab. Set the **Reset unauthorized to newbie** flag.

As soon as the database is restored from the backup it is recommended to connect the **Dr.Web Control Center** 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 Dr.Web Enterprise Server from Data Backup

Dr.Web Enterprise Security Suite regularly backs up important data: database contents, **Server** license key, private encryption key, **Server** configuration key, and **Dr.Web Control Center** configuration key. The backup files are stored in the following folders (relatively to the **Server** installation folder):

- ◆ for **Windows** OS: `\var\Backup`
- ◆ for **Linux** OS: `/var/opt/drwcs/backup`
- ◆ for **FreeBSD** and **Solaris** OS: `/var/drwcs/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. <u>Restoring the Database of Dr.Web Enterprise Security Suite</u>).

It is also recommended to store copies of the following files on another PC: `drwcsd.pri` and `drwcsd.pub` encryption keys, `enterprise.key` and `agent.key` license keys, `certificate.pem` SSL certiifcate, `private-key.pem` RSA private key and regularly copy **Server** database contents backup `database.dz,` **Server** and **Dr.Web Control Center** configuration files `drwcsd.conf` and `webmin.conf` to another PC. Thus you will be able to avoid data loss should the PC, on which **Enterprise 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. <u>Key Files</u>.

To Restore a Dr.Web Enterprise Server for Windows OS

Install **Enterprise Server** software of the same version as the lost one on a working PC (see p.). 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.).

To Restore a Dr.Web Enterprise Server for UNIX System-Based OS

1. Install **Enterprise Server** software of the same version as the lost one on a working PC (see p.).

2. Put the saved files to:

◆ for **Linux** 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 **Linux** 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.).

   c) If you have a saved copy of the internal DB, replace the new file with it:

   for **Linux** 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 **Linux** 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
```

5. Launch **Enterprise Server**.

> **i** 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 **Dr.Web Control Center** **Administration** menu, select **Configure Dr.Web Enterprise Server**. A **Dr.Web Enterprise Server configuration** window will be opened. On the **General** tab, set the **Reset unauthorized to newbie** flag.

Upgrading Dr.Web Enterprise Agents on the LAN servers

When upgrading **Agents** installed on the LAN servers, restarting stations or stopping a network software on such stations can be unwanted.

To avoid functionality downtime of stations that implement significant network functions, the following upgrading mode of **Agents** and anti-virus software is recommended:

1. In the **Server** schedule, change standard jobs for upgrading all components to upgrading virus bases only.

2. Create a new job for upgrading all components at the suitable time, when it will not be critical for LAN servers functionality.

   How to create and edit jobs in the **Server** schedule, described in the Setting the Dr.Web Enterprise Server Schedule section.

> ⚠️ It is not recommended to install **SpIDer Gate**, **SpIDer Mail** and **Dr.Web Firewall** components on servers those implement significant network functions (domain controllers, licence distribution servers and etc.) to avoid probable conflicts between network services and internal components of **Dr.Web** antivirus.

Restoring the Password of Dr.Web Enterprise Security Suite Administrator

If the administrative password for access to the **Enterprise Server** is lost, you can view or change it by direct access to the **Server** DB:

a) For an internal DB, to view and change administrative password, use the `drwidbsh` utility, which is included in the **Server** distribution kit.

b) For an external DB, use corresponding sql client.

> **i** Parameters of administrative accounts are stored in the `admins` table.

Example of using the drwidbsh utility

1. Run the `drwidbsh` utility and specify the path to the DB file:

   ◆ For the internal DB under Linux OS:

   ```
   /opt/drwcs/bin/drwidbsh          /var/opt/
   drwcs/dbinternal.dbs
   ```

   ◆ For the internal DB under Windows OS:

   ```
   "C:\Program    Files\DrWeb    Enterprise
   Server\bin\drwidbsh" "C:\Program Files
   \DrWeb      Enterprise      Server\var
   \dbinternal.dbs"
   ```

2. To view all data from the `admins` table, run the following command:

   ```
   select * from admins;
   ```

3. To view logins and passwords of all administrative accounts, run the following command:

   ```
   select login,password from admins;
   ```

4. If only one account with the `admin` name exists and it has

the `root` password, you will get the following result:

```
drwidbsh> select login,password from admins;
admin|root
 0 ms
drwidbsh> _
```

5. To change the password, use the `update` command. In the following example, the command changes the password of the `admin` account to `qwerty`:

```
update admins set password='qwerty' where
login='admin';
```

6. To exit the `drwidbsh` utility, run the following command:

```
.exit
```

Description of the `drwidbsh` utility is given in the appendix H6. The Administrating Utility of the Internal Database.

Using DFS During Installation of the Agent via the Active Directory

During installation of the **Enterprise Agent** via the Active Directory service, you can use Distributed File System (DFS).

It can be useful, for example, for several domain controllers in LAN.

For installation in the LAN with several domain controllers:

1. Create directory with the same name on each domain controller.
2. Via the DFS, unite created directories to one root destination directory.
3. Perform the administrative installation of the `*.msi` package to the created destination directory.
4. Use this destination directory during package assignment in the group policy object editor.

   Use the network address as: *<domain>**<folder>*

   where: *<domain>* - the domain name, *<folder>* - the name of destination directory.

Remote Installation Trouble Shooting

Principle of the installation:

1. The browser (**Dr.Web Browser-Plugin module**) connects to the `ADMIN$` resource at the remote station (`\\<remote_station>\ADMIN$`) and copies installer files (`drwinst.exe`, `drwcsd.pub`), specified in the **Dr.Web Control Center** to the `\\<remote_station>\ADMIN$\Temp` folder.

2. The plug-in runs `drwinst.exe` file at the remote station with the switches according to the **Dr.Web Control Center** settings.

Successful installation requires that at the station from which the installation will be performed:

1. The `ADMIN$` resource must be available at the remote station.

   The availability can be checked in the following way:

   In the address line of the `Windows Explorer` application, enter the following:

   `\\<remote_station>\ADMIN$`

   You will get the prompt for entering login and password for assess to this resource. Enter the account data, which have been specified on the installation page.

   The `ADMIN$` resource can be unavailable for the following reasons:

   a) account does not have administrative rights;
   b) the station is powered off or firewall blocks assess to the 455 port;

      c) limitations of remote assess to the `ADMIN$` resource at the Windows Vista and later OS, if the station is outside a domain.

2. The `drwinst.exe` and `drwcsd.pub` files are available.

At the **Dr.Web Control Center**, the external information (step and error code), which can help to diagnose the error reason, is displayed.

The list of the most frequently errors

Step	Error Code	Reason
Validating user inputs of the remote stations (1)	No such host is known (11001).	DNS name to address conversion failed. No such DNS name or wrong name server settings.
Checking if NetBIOS on the remote station is available (2)	A socket operation failed because the destination host was down (10064).	445 port is not available at the remote station. Possible reasons: ◆ station is shut down; ◆ firewall blocks specified port; ◆ the OS at the remote station is different from the Windows OS.
Connecting to an administrative resource ADMIN$ on the remote station (1001)	At this step, connection with the `ADMIN$` administrative resource at the remote station is performed.	
	The system detected a possible attempt to compromise security. Please ensure that you can contact the server that authenticated you (1265).	◆ Sharing and security model for local accounts is not configured. ◆ Authorization server is not available (domain controller).

Step	Error Code	Reason
	Logon failure: unknown user name or bad password (1326).	Unknown user name or bad password.
	The filename, directory name, or volume label syntax is incorrect (123).	The ADMIN$ resource does not exist at the remote station.
Checking installer exit code (1009)	At this step, result of installation is checked.	
	Unknown error (2).	Ask for the technical support of the **Doctor Web** company.
	Installation is not required on this computer (4).	The **Agent** is already installed or has been incorrectly deleted (in this case, use the **drwebremover** utility) at this station.
	Protocol violation (6).	The drwinst.exe installer is not matched with the **Server** version. Make sure, that the installer is from the **Server** installation package.
	Cannot initialize scripting engine (7).	System error. Ask for the technical support of the **Doctor Web** company.
	Connection to server timed out (8).	The **Enterprise Server** is not available from the remote station.
	System should be rebooted to finish previous deinstallation (9).	Restart the station to complete previously uninstallation.

Index

Index

Index

Index

Index

Index

Index