Dr.WEB

Enterprise Security Suite

Anti-virus Network Quick Installation Guide

Trademarks

Disclaimer

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

Dr.Web Enterprise Security Suite
Version 11.0.2
Anti-virus Network Quick Installation Guide
7/3/2020

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125040

Website: https://www.drweb.com/

Phone: +7 (495) 789-45-87

Refer to the official website for regional and international office information.

Doctor Web

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

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

Dr.Web antivirus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards.

State certificates and awards received by the Dr.Web solutions, as well as the globally widespread use of our products are the best evidence of exceptional trust to the company products.

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

Table of Contents

Chapter 1: Dr.Web Enterprise Security Suite

1.1. Introduction

1.1.1. About Manual

Anti-virus Network Quick Installation Guide contains brief information on installation and initial configuration of anti-virus network components. For detailed information refer to administrator documentation.

Documentation of the anti-virus network administrator contains the following parts:

1. **Installation Manual**
2. **Administrator Manual**
3. **Appendices**

Also, the following Manuals are provided:

1. **Manuals on managing stations**
2. **User Manuals**

All the listed Manuals are provided also within Dr.Web Enterprise Security Suite product and can be opened via Dr.Web Security Control Center.

Before reading these documents, make sure you have the latest version of the corresponding Manuals for your product version. The Manuals are constantly updated and the current version can always be found at the official web site of Doctor Web at https://download.drweb.com/doc/.

1.1.2. Conventions and Abbreviations

Conventions

The following symbols and text conventions are used in this guide:

Convention	Comment
(!)	Important note or instruction.
⚠	Warning about possible errors or important notes to which you should pay special attention.
Anti-virus network	A new term or an accent on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
`C:\Windows\`	Names of files and folders, code examples.
Appendix A	Cross-references on the document chapters or internal hyperlinks to web pages.

Abbreviations

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

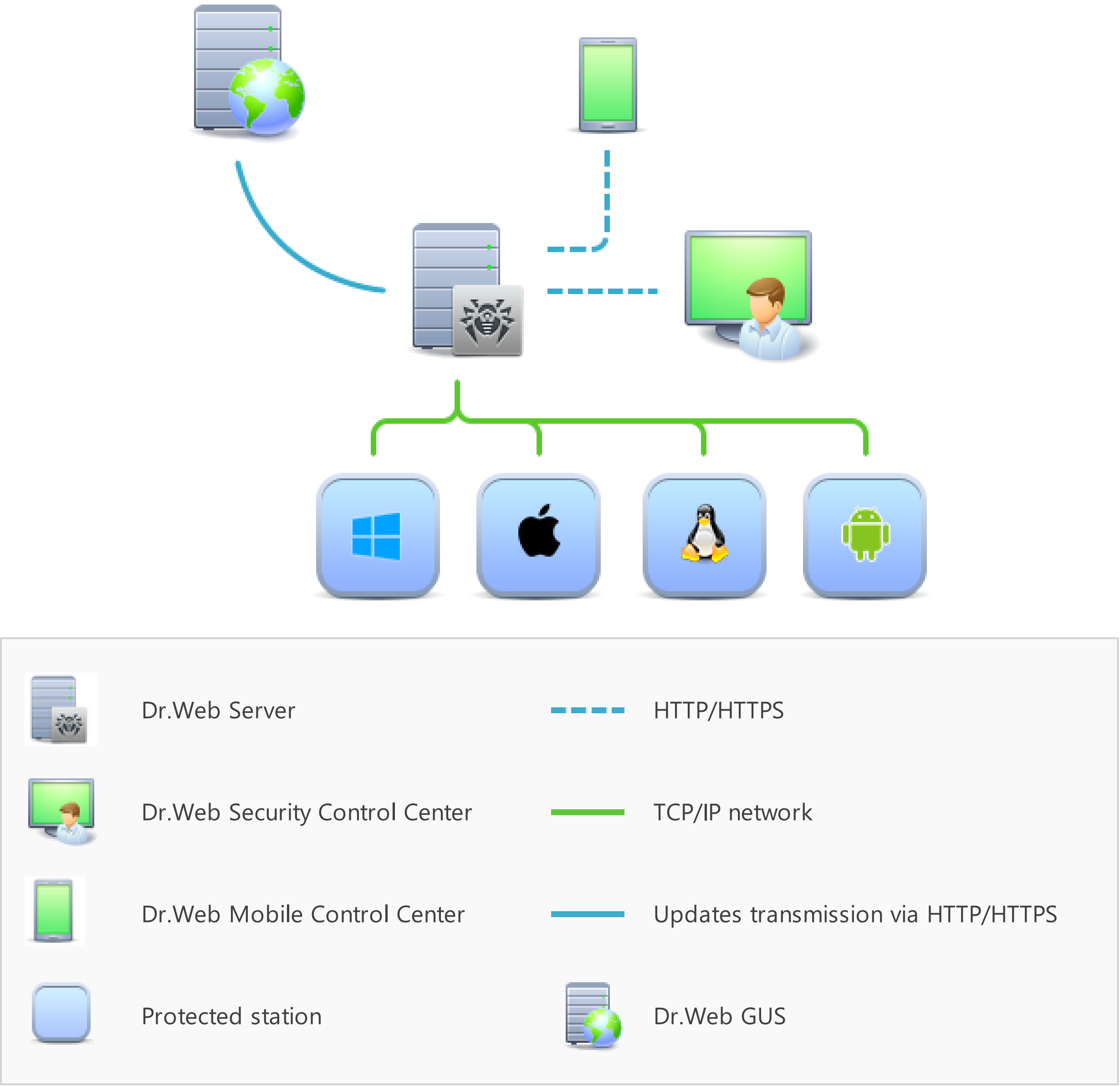
- ACL—Access Control List,
- CDN—Content Delivery Anti-virus network,
- DB, DBMS—Database, Database Management System,
- DFS—Distributed File System,
- DNS—Domain Name System,
- Dr.Web GUS—Dr.Web Global Update System,
- FQDN—Fully Qualified Domain Name,
- GUI—Graphical User Interface, a GUI version of a program—a version using a GUI,
- LAN—Local Area Network,
- MTU—Maximum Transmission Unit,
- NAP—Network Access Protection,
- OS—Operating System,
- TTL—Time To Live,

- UDS—UNIX domain socket.

1.2. About Product

Dr.Web Enterprise Security Suite is designed for organization and management of integrated and secure complex anti-virus protection either local company network including mobile devices, or home computers of employers.

An aggregate of computers and mobile devices on which Dr.Web Enterprise Security Suite cooperating components are installed, represents a single *anti-virus network*.


Dr.Web Server
HTTP/HTTPS
Dr.Web Security Control Center
TCP/IP network
Dr.Web Mobile Control Center
Updates transmission via HTTP/HTTPS
Protected station
Dr.Web GUS

Picture 1-1. The logical structure of the anti-virus network

Dr.Web Enterprise Security Suite anti-virus network has a *client-server* architecture. Its components are installed on a computers and mobile devices of users and administrators as well as on a computers that function as LAN servers. Anti-virus network components exchange information via TCP/IP network protocols. Anti-virus software can be installed (and manage them afterwards) on protected stations either via the LAN, or via the Internet.

Central Protection Server

Central protection Server is installed on a computer of anti-virus network, and installation can be performed on any computer, not only on that functioning as a LAN server. General requirements to this computer are given in the System Requirements section.

Cross-platform Server software allows to use a computer under the following operating systems as a Server:

- Windows® OS,
- UNIX® system-based OS (Linux®, FreeBSD®).

Central protection Server stores distribution kits of anti-virus packages for different OS of protected computers, updates of virus databases and anti-virus packages, license keys and package settings of protected computers. Server receives updates of anti-virus protection components and virus databases via the Internet from the Global Update System and propagate updates on protected stations.

Single Database

The single database is connected to the central protection Server and stores statistic data on anti-virus network events, settings of the Server itself, parameters of protected stations and anti-virus components, installed on protected stations.

Central Protection Control Center

Central protection Control Center is automatically installed with the Server and provides the web interface for remote managing of the Server and the anti-virus network by means of editing the settings of the Server and protected computers settings stored on the Server and protected computers.

The Control Center can be opened on any computer that have the network access to the Server. The Control Center can be used almost under any operating system with full use on the following web browsers:

- Windows® Internet Explorer®,
- Microsoft Edge®,
- Mozilla® Firefox®,
- Google Chrome®.

The list of possible variants of use is given in the System Requirements section.

The par of the Control Center is the Web server that is automatically installed with the Server. The general task of the Web server is performing operation with web pages of the Control Center and clients network connections.

Central Protection Mobile Control Center

As a separate component, the Mobile Control Center is provided. It is designed for installation and operation on mobile devices under iOS® and Android™ OS. General requirements to the application are given in the System Requirements section.

You can download Mobile Control Center from the Control Center or directly in App Store and Google Play.

Network Stations Protection

On protected computers and mobile devices of the network, the control module (Agent) and the anti-virus package for corresponding operating system are installed.

Cross-platform software allows to provide anti-virus protection of computers and mobile devices under the following operating systems:

- Windows® OS,
- UNIX® system-based OS,
- macOS®,
- Android OS.

Either user computers or LAN servers can be protected stations. Particularly, anti-virus protection of the Microsoft® Outlook® mail system is supported.

Control module performs regular updates of anti-virus components and virus databases from the Server and also, sends information on virus evens on protected computer to the Server.

If the central protection Server is not accessible, it is possible to update virus databases on protected stations via the Internet from the Global Update System.

Providing a Connection between Anti-virus Network Components

To provide stable and secure connection between anti-virus network components, the following features are presented:

Dr.Web Proxy server

Proxy server can be optionally included in an anti-virus network. The main function of the Proxy server is to provide connection between the Server and protected stations in case if direct connection is impossible.

Traffic compression

Special compression algorithms are applicable for transferring data between the anti-virus network components to reduced network traffic to minimum.

Traffic encryption

Data transferred between the anti-virus network components can be encrypted to provide additional secure level.

Additional Features

NAP Validator

NAP Validator is provided as a separate component and allows to use Microsoft Network Access Protection (NAP) technology to check health of protected stations software.

Repository loader

Dr.Web Repository loader is provided as a separate utility and allows to download products of Dr.Web Enterprise Security Suite from the Global Update System. It can be used for downloading of Dr.Web Enterprise Security Suite products updates to place them on the Server not connected to the Internet.

1.3. System Requirements

Dr.Web Server requires:

Component	Requirement
CPU	CPU that supports SSE2 instructions and has 1,3 GHz or faster clock frequency.
RAM	• Minimal requirements: 1 GB. • Recommended requirements: 2 GB and more.
Free disk space	Up to 12 GB: up to 8 GB for a embedded database (installation catalog) and up to 4GB for the system temporary catalog (for work files).
Operating system	• Windows; • Linux; • FreeBSD. Complete list of supported OS see in the **Appendices** document, in Appendix A.
Supported virtual and cloud environments	Can be used under operating systems meeting the above-mentioned requirements, in virtual and cloud environments, including: • VMware; • Hyper-V; • Xen; • KVM.

Additional utilities supplied with Dr.Web Server (are available for downloading via the Control Center, in the **Administration** → **Utilities** section) must be launched on a computer that meets the system requirements for Dr.Web Server.

Dr.Web Security Control Center requires:

a) Web browser:

Web browser	Support
Windows Internet Explorer 11	Supported.
Microsoft Edge 0.10 and later	
Mozilla Firefox 25 and later	
Google Chrome 30 and later	
Opera® 10 and later	Allowed to be used, but operating is not guaranteed.
Safari® 4 and later	

b) Recommended screen resolution to use Dr.Web Security Control Center is 1280x1024 pt.

Dr.Web Mobile Control Center requires:

Requirements are differ depending on the operating system on which the application is installed:

Operating system	Requirement	
	Operating system version	Device
iOS	iOS 8 and later	Apple® iPhone® Apple® iPad®
Android	Android 4.0 and later	–

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

Requirements are differ depending on the operating system on which anti-virus solution is installed (the full list of supported OS see in the **Appendices** document, in Appendix A. The Complete List of Supported OS Versions):

- Windows OS:

Component	**Requirement**
CPU	1 GHz CPU or faster.
Free RAM	Not less than 512 MB.
Free disk space	1 GB for executable files + extra disk space for logs and temporary files.

- Linux system-based OS:

Component	**Requirement**
CPU	CPU with the following Intel/AMD architecture and command system are supported: 32-bit (IA-32, x86); 64-bit (x86-64, x64, amd64).
Free RAM	Not less than 512 MB.
Free disk space	Not less than 400 MB of free disk space on a volume on which Anti-virus folders are placed.

- macOS, Android OS: configuration requirements coincide with the requirements for operating system.

Dr.Web Agent can be used under operating systems meeting the above-mentioned requirements, in virtual and cloud environments, including:

- VMware;
- Hyper-V;
- Xen;
- KVM.

1.4. Distribution Kit

The program software is distributed depending on the OS of the selected Dr.Web Server:

1. For UNIX system-base OS:
   - `drweb-11.00.2-`<*build*>`-esuite-server-`<*OS_version*>`.tar.gz.run`

     Dr.Web Server general distribution kit*
   - `drweb-11.00.2-`<*build*>`-esuite-extra-`<*OS_version*>`.tar.gz.run`

Dr.Web Server extra distribution kit

- `drweb-11.00.2-`*<build>*`-esuite-proxy-`*<OS_version>*`.tar.gz.run`

  Dr.Web Proxy Server

- `drweb-reploader-`*<OS>*`-`*<bitness>*

  Console version of Dr.Web Repository Loader

2. For Windows OS:

- `drweb-11.00.2-`*<build>*`-esuite-server-`*<OS_version>*`.exe`

  Dr.Web Server general distribution kit*

- `drweb-11.00.2-`*<build>*`-esuite-extra-`*<OS_version>*`.exe`

  Dr.Web Server extra distribution kit

- `drweb-11.00.2-`*<build>*`-esuite-proxy-`*<OS_version>*`.exe`

  Dr.Web Proxy Server

- `drweb-11.05.4-`*<build>*`-esuite-agent-activedirectory.msi`

  Dr.Web Agent for Active Directory

- `drweb-11.00.1-`*<build>*`-esuite-modify-ad-schema-`*<OS_version>*`.exe`

  Utility for Active Directory scheme modification

- `drweb-11.00.1-`*<build>*`-esuite-aduac-`*<OS_version>*`.msi`

  Utility to change attributes for Active Directory objects

- `drweb-11.00.1-`*<build>*`-esuite-napshv-`*<OS_version>*`.msi`

  NAP Validator

- `drweb-11.05.2-`*<build>*`-esuite-agent-full-windows.exe`

  Dr.Web Agent full installer. Also included into the extra distribution kit of Dr.Web Server.

- `drweb-reploader-windows-`*<bitness>*`.exe`

  Console version of Dr.Web Repository Loader

- `drweb-reploader-gui-windows-`*<bitness>*`.exe`

  GUI version of Dr.Web Repository Loader

***Dr.Web Server general distribution kit contains the following components:**

- Dr.Web Server software for the respective OS,
- Dr.Web Agents software and anti-virus packages software for staions under Windows OS,
- Dr.Web Security Control Center software,
- Virus databases,
- Dr.Web Security Control Center extension,
- Dr.Web Server FrontDoor extension,
- 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.

Chapter 2: Creating Anti-virus Network

Quick start to an anti-virus network deployment:

1. Make a plan of the anti-virus network structure, include all protected computers and mobile devices.

   Select a computer to perform the functions of Dr.Web Server. The anti-virus network can incorporate several Dr.Web Servers. The features of such configuration are described in **Administrator Manual**, p. Peculiarities of a Network with Several Dr.Web Servers.

   > Dr.Web Server can be installed on any computer, not only on a computer functioning as a LAN server. General system requirements to this computer are described in p. System Requirements.
   >
   > On all protected stations including LAN servers, the same Dr.Web Agent version is installed. Difference is in the installing anti-virus components list which is defined be the settings on the Server.

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

   When planning the anti-virus network, it is also recommended that a list of persons is made up, who are to be granted access to the Control Center as required by their job duties, as well as a list of roles with respective responsibilities assigned to each role. An administrative group shall be created for every role. Specific administrators can be linked with the roles by having their accounts placed into administrative groups. If necessary, administrative groups (roles) can be grouped hierarchically as a multilevel system allowing for individual editing of administrative permissions for each level.

   For detailed guidelines of how to manage administrative groups and permissions see **Administrator Manual**, Chapter 5: Anti-Virus Network Administrators

2. According to the constructed plan, define what products for what operating systems should be installed on corresponding network nodes. Detailed information on the supported products is given in the Distribution Kit section.

   All required products can be obtained as a box solution or downloaded at the official web site of Doctor Web at https://download.drweb.com.

   > Dr.Web Agents for stations under Android OS, Linux OS, macOS can be also installed from the standalone packages and in the sequel get connected to the centralized Dr.Web Server. Description of the Agent settings is given in the corresponding **User manuals**.

3. Install Dr.Web Server general distribution kit on selected computer or computers. Installation description is given in **Installation Manual**, p. Installing Dr.Web Server.

Dr.Web Security Control Center is installed with the Server.

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

4. If anti-virus network will include protected stations under Android OS, Linux OS, macOS, install Dr.Web Server extra distribution kit on all computers with Dr.Web Server general distribution kit installed.
5. Install and configure the Proxy Server, if necessary. Description is given in **Installation Manual**, p. Installing Proxy Server.
6. To configure the Server and anti-virus software on stations, connect to the Server via Dr.Web Security Control Center.

   > Dr.Web Security Control Center can be opened on any computer, not just on the one with Dr.Web Server installed. It is enough to have a network connection with a computer on which the Server is installed.

   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 Dr.Web Server is installed.

   In the authorisation request dialogue window, specify the administrator's credentials. For default administrator:

   - Name—**admin**.
   - Password:
     - for Windows OS—password that was set during the Server installation.
     - for UNIX system-based OS—password that was automatically created during the Server installation (see also **Installation Manual**, p. Installing Dr.Web Server for UNIX® System-Based OS).

   On successful connect to the Server, the main window of the Control Center will be opened (detailed description see in the **Administrator Manual**, in p. Dr.Web Security Control Center).
7. Perform the initial configuration of the Server (detailed description of the Server settings is given in the **Administrator Manual**, in p. Chapter 8: Configuring Dr.Web Server):

   a. In the License Manager section, add one or several license keys and propagate them on corresponding groups, particularly on the **Everyone** group. The step is obligatory if the license key was not set during the Server installation.

   b. In the General repository configuration section, set the components of anti-virus network to update from Dr.Web GUS. In the Repository state section, update products in the

Server repository. Update might take a long time to complete. Wait for the end of the update process before continuing the further configuring.

c. The **Administrating → Dr.Web Server** page contain the information on the Server version. If a new version is available, update the Server as described in the **Administrator manual**, in p. Updating Dr.Web Server and Restoring from the Backup.

d. If necessary, set up the Network connections to change default network settings used for interaction of all anti-virus network components.

e. If necessary, set up the list of the Servers administrators. The external administrators authentication is also available. For more details see the **Administrator Manual**, in Chapter 5: Anti-Virus Network Administrators.

f. Before using the anti-virus software, it is recommended to change the settings of the backup folder for the Server critical data (see **Administrator Manual**, p. Setting Dr.Web Server Schedule). It is recommended to keep the backup folder on another local disk to reduce the risk of losing the Server software files and backup copies at the same time.

8. Specify settings and configuration of anti-virus software for workstations (detailed description of groups and stations setup is given in the **Administrator Manual**, in Chapter 6 and Chapter 7):

   a. If necessary, create user groups of stations.

   b. Configure settings of the **Everyone** group and created user groups. Particularly, configure installing components section.

9. Install Dr.Web Agent software on workstations.

   In the Installation Files section, look through the list of supported files for the Agent installation. Select suitable for you installation option based on stations operating system, remote installation ability, option to specify the Server settings during the Agent installation, etc. For example:

   - If users install the anti-virus independently, use personal installation packages which are created vie the Control Center separately for each station. This type of packages also can be sent to users by email directly from the Control Center. Connection of stations to the Server perform automatically after the installation.
   - If you need to install the anti-virus on several stations within one user group, you can use the group installation package which is created via the Control Center in a single copy for multiple stations of a certain group.
   - For the remote installation via the network on a station or on several stations simultaneously (for stations under Windows OS only), use the network installer. The installation is performed via the Control Center.
   - Also you can perform the remote installation via the network on a station or on several stations simultaneously via the Active Directory service. For this, use Dr.Web Agent installer for networks with Active Directory, which is supported together with Dr.Web Enterprise Security Suite distribution kit but separately from the Server installer.
   - If you need to reduce the load on a communication channel between the Server and stations during the installation, you can use the full installer that perform the installation of the Agent and protection components at a time.

- Installation on stations under Android OS, Linux OS, macOS can be performed locally by the general rules. Also, already installed standalone product can be connected to the Server according to the corresponding configuration.

> ⚠ To be able to use the full installer for Windows OS as well as installers for operating systems other than Windows OS, it is necessary that additional ("extra") distribution kit of Dr.Web Server is installed first.
>
> To guarantee that Dr.Web Agent works properly on a server Windows OS starting from Windows Server 2016, make sure to manually disable Windows Defender using group policies.

10. Agents establish a connection with the Server immediately after the installation. Anti-virus workstations are authorised at the Server according to the set policy (see **Administrator Manual**, p. New Stations Approval Policy):

    a. For installation from installation packages and also for automatic approval on the Server, workstations automatically get registration at first connect to the Server, and additional approval is not required.

    b. For installation from installer and manual access approval, new workstations should be approved by an administrator manually to be registered at the Server. At this, new workstations are not connected automatically, but placed by the Server into the newbies group.

11. After connecting to the Server and receiving settings, corresponding set of anti-virus components specified in the primary group settings are installed on the station.

> ! To finish the installation of workstation components, computer restart required.

12. Configuring stations and anti-virus software is also available after the installation (detailed description is given in the **Administrator Manual**, in Chapter 7).

Appendix A. Licensing

The license is required for the operation of Dr.Web Enterprise Security Suite anti-virus solution.

Dr.Web Enterprise Security Suite license compound and price depend on the number of protected stations including the servers within Dr.Web Enterprise Security Suite network in a position of protected stations.

> Before purchasing a license for a Dr.Web Enterprise Security Suite solution you should carefully consider this information and discuss all the details with your local distributor. The number of Dr.Web Servers running the network does not affect the license price.

License Key File

Rights to use Dr.Web Enterprise Security Suite are regulated by license key files.

> A license key file is write-protected by the mechanism of electronic signature. Editing a file makes it invalid. To avoid occasionally corrupting of a license key file, you must not modify and/or save it after opening in a text editor.

License key files come in a zip-archive, which contains one or several key files for protected stations.

The user can receive the key files by one of the following ways:

- A license key file is included into Dr.Web Enterprise Security Suite anti-virus distribution kit at a purchasing, if license files were included at kitting. However, generally only serial numbers are provided.
- A license key file is sent to users by email after the product serial number has been registered at Doctor web company web site at https://products.drweb.com/register/ unless other address specified in the registration card attached to the product. Visit the web site above, fill the form with the buyer information 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 email address. Also, you will be allowed to download the key files directly from the web site.
- A license key file can be provided on a separate carrier.

It is recommended to keep a license key file until its expiration and use it during the reinstallation and restoring the program components. In case a license key file is lost, you can repeat the registration on the web site specified above and restore the license key file. Note that you will need to enter the same registration serial number and the same buyer information as during the first registration, you can change the email address only. In this case, a license key file will be sent to the new address.

To familiarize yourself with the anti-virus, you can use demo key files. Such key files provide 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 https://download.drweb.com/demoreq/biz/. Your request will be examined individually. In case of approval, an archive with license key files will be sent to the designated email address.

Detailed information on principles and features of Dr.Web Enterprise Security Suite licensing is given in the **Administration Manual**, subchapters of Chapter 2: Licensing.

The use of key files during the installation is described in **Installation Manual**, p. Installing Dr.Web Server.

The use of key files for already deployed anti-virus network is described in **Administration Manual**, p. License Manager.

Appendix B. Technical Support

If you encounter any issues installing or using company products, before requesting for the assistance of the technical support, take advantage of the following options:

- Download and review the latest manuals and guides at https://download.drweb.com/doc/.
- Read the frequently asked questions at https://support.drweb.com/show_faq/.
- Browse the Dr.Web official forum at https://forum.drweb.com/.

If you have not found solution for the problem, you can request direct assistance from Doctor Web company technical support by one of the following ways:

- Fill in the web form in the corresponding section at https://support.drweb.com/.
- Call by phone in Moscow: +7 (495) 789-45-86.

Refer to the official website at https://company.drweb.com/contacts/offices/ for regional and international office information of Doctor Web company.