



Dr.WEB

Enterprise Security Suite

Anti-virus Network Quick Installation Guide



© **Doctor Web, 2022. All rights reserved**

This document is for information and reference purposes in relation to the specified software of the Dr.Web family. This document is not a ground for exhaustive conclusions about the presence or absence of any functional and/or technical features in the software of the Dr.Web family and cannot be used to determine whether the software of the Dr.Web family matches any requirements, technical task and/or parameters, and other third-party documents.

This document is the property of Doctor Web. No part of this document may be reproduced, published or transmitted in any form or by any means for any purpose other than the purchaser's personal use without proper attribution.

Trademarks

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

Disclaimer

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

Dr.Web Enterprise Security Suite
Version 13.0
Anti-virus Network Quick Installation Guide
1/12/2022

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125124

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 anti-virus solutions are well known since 1992 for continuing excellence in malware detection and compliance with international information security standards.

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

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



Table of Contents

Chapter 1: Introduction	5
1.1. About Manual	5
1.2. Conventions and Abbreviations	5
Chapter 2: Dr.Web Enterprise Security Suite	7
2.1. About Product	7
2.2. System Requirements	10
2.3. Distribution Kit	13
Chapter 3: Creating Anti-virus Network	16
Appendix A. Licensing	21
Appendix B. Technical Support	23



Chapter 1: Introduction

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**
3. **Web API Manual**
4. **Dr.Web Server Database Manual**



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 website of Doctor Web at <https://download.drweb.com/doc>.

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.
<i>Anti-virus network</i>	A new term or an accent on a term in descriptions.



Convention	Comment
<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 Network,
- DFS—Distributed File System,
- DNS—Domain Name System,
- FQDN—Fully Qualified Domain Name,
- GUI—Graphical User Interface, a GUI version of a program—a version using a GUI,
- MIB—Management Information Base,
- MTU—Maximum Transmission Unit,
- NAP—Network Access Protection,
- TTL—Time To Live,
- UDS—UNIX Domain Socket,
- DB, DBMS—Database, Database Management System,
- Dr.Web GUS—Dr.Web Global Update System,
- LAN—Local Area Network,
- OS—Operating System.

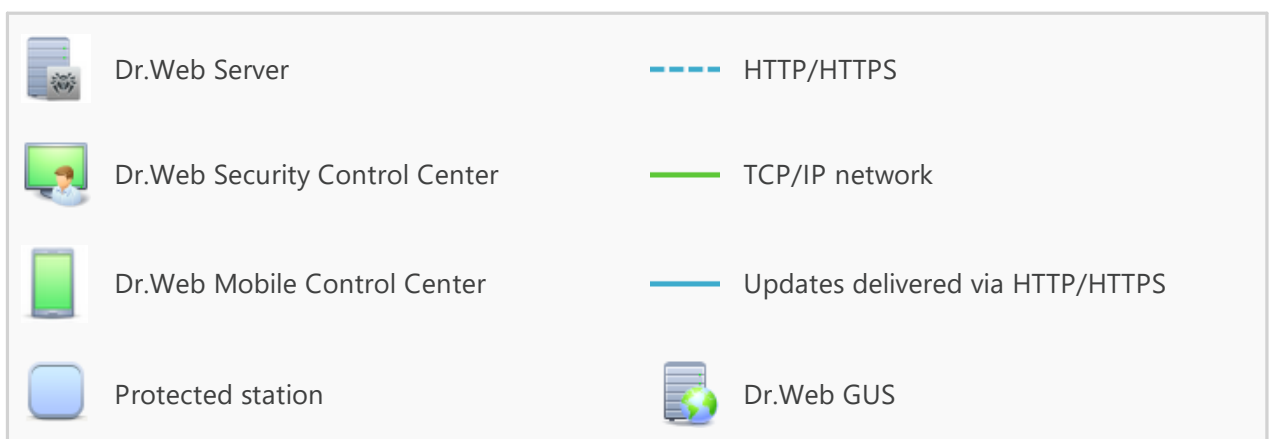
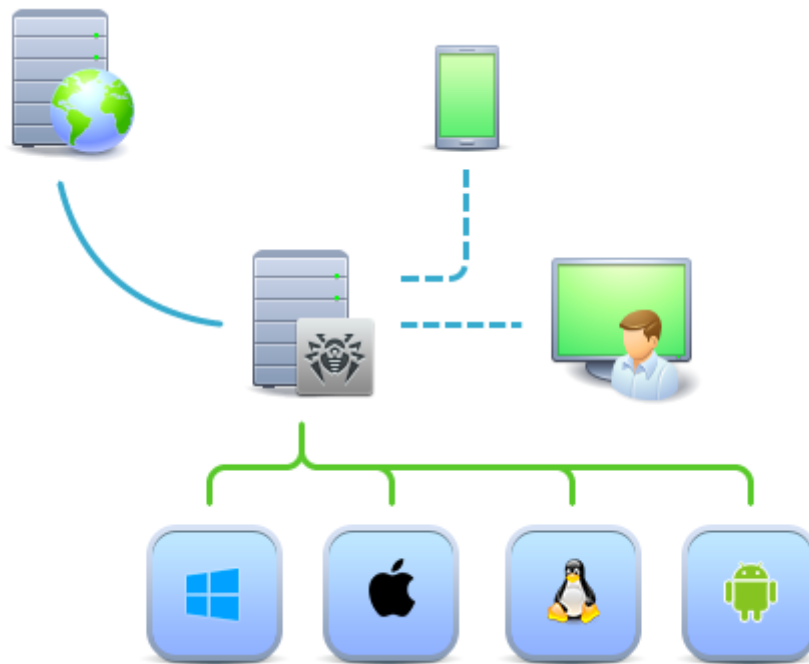


Chapter 2: Dr.Web Enterprise Security Suite

2.1. About Product

Dr.Web Enterprise Security Suite is designed for implementation and management of integrated and secure complex anti-virus protection for either local company network (mobile devices included) or home computers of employees.

A sum of computers and mobile devices with Dr.Web Enterprise Security Suite cooperating components installed represents a single *anti-virus network*.



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 computers and mobile devices of users and administrators, as well as computers functioning as LAN servers. Anti-virus network components exchange information via TCP/IP



network protocols. Anti-virus software can be installed (and managed afterwards) onto protected stations either via LAN, or the internet.

Central Protection Server

Central protection Server (Dr.Web Server) is installed on a computer in anti-virus network. The installation can be performed on any computer, not necessarily the one functioning as a LAN server. General requirements to such computer are given in the [System Requirements](#) section.

Cross-platform nature of the Dr.Web Server software allows using a computer under any of the following operating systems as a Dr.Web Server:

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

Central protection Server stores distribution kits of anti-virus packages for different operating systems on protected computers, updates for virus databases and anti-virus packages, license keys and anti-virus package settings for protected computers. Dr.Web Server receives updates of anti-virus protection components and virus databases via the internet from Dr.Web Global Update System and propagates the updates to protected stations.

Single Database

The single database is connected to the central protection Server and stores statistics about anti-virus network events, Dr.Web Server settings, parameters of protected stations and anti-virus components installed on protected stations.

Central Protection Control Center

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

The Control Center can be opened on any computer with a network access to Dr.Web Server. The Control Center can be used almost under any operating system with full use in 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 Web server is one of the Control Center parts that is automatically installed with Dr.Web Server. The main purpose of the Web server is to ensure operation of the Control Center web pages and client network connections.



Central Protection Mobile Control Center

Dr.Web Mobile Control Center is available as a separate component for mobile devices under iOS and Android. Basic requirements for devices to run the application are given in the [System Requirements](#) section.

The Mobile Control Center connects to Dr.Web Server over encrypted protocol using the anti-virus network administrator credentials.

You can download Dr.Web Mobile Control Center from the Control Center or from [App Store](#) and [Google Play](#) directly.

Protection of Network Stations

Protected computers and mobile devices in the network have control module (Agent) and anti-virus package installed for corresponding operating system.

Cross-platform nature of the software ensures that anti-virus protection of computers and mobile devices is provided under the following operating systems:

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

Protected stations can include both user computers and LAN servers. Anti-virus protection of the Microsoft Outlook mail system is supported as well.

The control module updates anti-virus components and virus databases regularly by downloading them from Dr.Web Server. It also sends information about virus events on protected computer to Dr.Web Server.

If the central protection Server is not accessible, virus databases on protected stations can be updated from the Global Update System via the internet.

Providing 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 Dr.Web Server and protected stations in cases when direct connection is impossible.

Traffic compression

To reduce network traffic to minimum, special compression algorithms come into effect when anti-virus network components exchange the data.



Traffic encryption

Data transferred between anti-virus network components can be encrypted to provide additional security 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 Dr.Web Global Update System. It can be used for downloading of Dr.Web Enterprise Security Suite products updates and placing them on a Dr.Web Server, which is not connected to the internet.

Dr.Web Scanning Server

Dr.Web Scanning Server is provided as a separate component. It is designed for operating in virtual environments, The Scanning Server is installed on a separate virtual machine and processes anti-virus scanning requests from other virtual machines.

2.2. System Requirements

Dr.Web Server

Component	Requirement
CPU	CPU that supports SSE2 instructions and has 1.3 GHz or faster clock frequency.
RAM	<ul style="list-style-type: none">Minimal requirements: 1 GB.Recommended requirements: 2 GB and more.
Free disk space	<ul style="list-style-type: none">At least 50 GB for the Dr.Web Server software, also additional space for storing temporary files, e.g. Agent personal installation packages (app. 17 MB each) in the <code>var\installers-cache</code> subfolder of the Dr.Web Server installation folder.Up to 5 GB for the database.Not depending on the Dr.Web Server installation folder, on Windows OS system disk or in the <code>/var/tmp</code> for UNIX system-based OS (or in the other temporary files folder, if it is redefined):<ul style="list-style-type: none">the Dr.Web Server installation requires at least 4.3 GB to launch the installer and unpack temporary files;



Component	Requirement
	<ul style="list-style-type: none">▫ the Dr.Web Server operation requires free disk space on the system disk for storing temporary and working files depending on the database size and repository configuration.
Operating system	<ul style="list-style-type: none">• Windows.• Linux using the <code>glibc</code> library 2.13 or later.• FreeBSD 11.3 or later. See complete list of supported OS in the Appendices document, Appendix A .
Supported virtual and cloud environments	Can be used under operating systems meeting the above-mentioned requirements, in virtual and cloud environments, including: <ul style="list-style-type: none">• VMware;• Hyper-V;• Xen;• KVM.



Dr.Web Server cannot be installed on logical drives with file systems that do not support symbolic links, in particular, with file systems from the FAT family.



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

a) Web browser:

- Internet Explorer 11
- Microsoft Edge 0.10 or later
- Mozilla Firefox 44 or later
- Google Chrome 49 or later
- Opera of the latest version
- Safari of the latest version.

b) Recommended screen resolution to use Dr.Web Security Control Center is 1280×1024 pt.



Dr.Web Mobile Control Center

The requirements differ depending on the operating system on which the application is installed:

Operating system	Requirement	
	Operating system version	Device
iOS	iOS 9 and later	Apple iPhone Apple iPad
Android	Android 4.1—11.0	–

Dr.Web Agent and the Anti-virus Package

The requirements differ depending on the operating system on which anti-virus solution is installed (the full list of supported OSs can be found 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	At least 512 MB.
Free disk space	1.5 GB for executable files, also extra disk space for logs and temporary files.



As Microsoft has stopped supporting the SHA-1 hashing algorithm, please ensure that your operating system supports the SHA-256 hashing algorithm before installing Dr.Web Agent on Windows Vista, Windows 7, Windows Server 2008 or Windows Server 2008 R2. To do this, install all the recommended updates listed in Windows Update. Please visit [Doctor Web official website](#) for details.

- Linux system-based OS:

Component	Requirement
CPU	CPU with the following architecture and command system <ul style="list-style-type: none">• Intel/AMD: 32-bit (IA-32, x86) and 64-bit (x86_64, x64, AMD64);• ARM64;• E2K (Elbrus).



Component	Requirement
Free RAM	At least 512 MB (1 GB and more is recommended).
Free disk space	At least 2 GB of free disk space on a volume where Dr.Web directories are located.

- 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.

Dr.Web Scanning Server

Component	Requirement
Hypervisor	VMware, Hyper-V, Xen, KVM.
Operating System	Linux, FreeBSD. The list of supported OS is the same as the list for anti-virus package for UNIX OS.
CPU	CPU with the following architecture and command system: <ul style="list-style-type: none">• Intel/AMD: 32-bit (IA-32, x86) and 64-bit (x86_64, x64, AMD64).
Random Access Memory (RAM)	At least 500 Mb of free RAM (1 Gb or more is recommended).
Hard disk space	At least 1 GB of free disk space.
Network connections	Availability of network connections: <ul style="list-style-type: none">• Valid Internet connection to enable updates for virus databases and filter database• Connection for processing requests from Virtual Agents to the service VM.

2.3. Distribution Kit

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

1. For UNIX system-based OS:



- `drweb-13.00.0-<build>-esuite-server-<OS_version>.tar.gz.run`
Dr.Web Server distribution kit
- `drweb-reloader-<OS>-<bitness>`
Console version of Dr.Web Repository Loader

2. For Windows OS:

- `drweb-13.00.0-<build>-esuite-server-<OS_version>.exe`
Dr.Web Server distribution kit
- `drweb-13.00.0-<build>-esuite-agent-full-windows.exe`
Dr.Web Agent full installer
- `drweb-reloader-windows-<bitness>.exe`
Console version of Dr.Web Repository Loader
- `drweb-reloader-gui-windows-<bitness>.exe`
GUI version of Dr.Web Repository Loader

Dr.Web Server distribution kit contains the following components:

- Dr.Web Server software for the respective OS
- Dr.Web Server security data
- Dr.Web Security Control Center software
- Dr.Web Agent and anti-virus package software for stations running Windows OS
- Update module for Dr.Web Agent for Windows
- Dr.Web Anti-spam for Windows
- Virus databases, databases of anti-virus components built-in filters and Dr.Web Anti-spam for Windows
- Documentation
- Doctor Web company news.

In addition to the distribution kit, serial numbers are also supplied. Having registered these serial numbers one can get files with license keys.

After installation of Dr.Web Server you can also download from the GUS servers the following Dr.Web enterprise products to the repository:

- Products for installation on protected stations under UNIX (including LAN servers), Android, macOS
- Dr.Web for IBM Lotus Domino
- Dr.Web for Microsoft Exchange Server
- Dr.Web Proxy Server
- Dr.Web Scanning Server



- Dr.Web Agent for Windows full installer
- Dr.Web Agent for Active Directory
- Utility for Active Directory scheme modification
- Utility to change attributes for Active Directory objects
- NAP Validator.



Detailed information on how to handle the Dr.Web Server repository you can find in the **Administrator Manual**, the [Administration of Dr.Web Server Repository](#) section.



Chapter 3: 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. The difference is in the list of installed anti-virus components defined by the Dr.Web Server settings.

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 6: 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 website 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 Dr.Web Server.
By default, Dr.Web Server automatically starts after installation and every time after restarting the operating system.
4. Install and configure the Proxy Server, if necessary. Description is given in **Installation Manual**, p. [Installing Proxy Server](#).
5. If your anti-virus network consists of virtual machines, it is recommended to use the Scanning Server. The detailed description of the installation and the configuration procedures is given in **Installation Manual**, p. [Installing Dr.Web Scanning Server](#).
6. To configure Dr.Web Server and anti-virus software on stations, connect to Dr.Web 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 Dr.Web Server is installed.

Control Center is available at the following address:

`http://<Dr.Web_Server_Address>:9080`

or

`https://<Dr.Web_Server_Address>:9081`

where `<Dr.Web_Server_Address>` is the IP address or domain name for the computer on which Dr.Web Server is installed.

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

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

On successful connect to Dr.Web 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](#)).

If you installed Dr.Web Scanning Server, specify its address in the settings of the stations. For detailed information refer to the **Administrator Manual**, p. [Connecting Stations to the Scanning Server](#).

7. Perform the initial configuration of Dr.Web Server (detailed description of the Dr.Web Server settings is given in the **Administrator Manual**, in p. [Chapter 9: 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 Dr.Web Server installation.
- b. In the [General repository configuration](#) section, set the components of anti-virus network to update from Dr.Web GUS. If anti-virus network will include protected stations under Android OS, Linux OS, macOS, **Dr.Web enterprise products** must be downloaded.

In the [Repository state](#) section, update products in the Dr.Web Server repository. Update might take a long time to complete. Wait for the end of the update process before continuing the further configuring.



By default, after installing Dr.Web Server version 13, updates of the **Dr.Web for Android databases, Dr.Web Agent for UNIX and Dr.Web Proxy Server** repository products are downloaded from GUS only when these products are requested from stations. For more details, see **Administrator Manual**, p. [Detailed Repository Configuration](#).

If your Dr.Web Server is not connected to the internet, and updates are loaded manually from another Dr.Web Server or using the Repository Loader, before installing or updating products with the **Update on demand only** option, you must first manually load these products to the repository.

- c. The **Adminstrating** → **Dr.Web Server** page contains information about the Dr.Web Server version. If a new version is available, update Dr.Web 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 Dr.Web Server administrators. The external administrators authentication is also available. For more details, see the **Administrator Manual**, in [Chapter 6: Anti-Virus Network Administrators](#).
 - f. Before using the anti-virus software, it is recommended to change the settings of the backup folder for the Dr.Web 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 Dr.Web 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 7](#) and [Chapter 8](#)):
- 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 Dr.Web Server settings during the Agent installation, etc. For example:

- If users install the anti-virus independently, use personal installation packages which are created via the Control Center separately for each station. This type of packages also can be sent to users by email directly from the Control Center. The stations connect to Dr.Web Server automatically, once the installation is complete.
- 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 remote installation via network on a station or several stations simultaneously running Windows OS or Linux OS, use the network installer. The installation is performed from 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 Dr.Web Server installer.
- If you need to reduce the load on a communication channel between Dr.Web 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 running Android OS and macOS can be performed locally by the general rules. Also, already installed standalone product can be connected to Dr.Web Server according to the corresponding configuration.



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. The Agents establish connection with Dr.Web Server immediately after the installation. Anti-virus workstations are authorized at Dr.Web 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 Dr.Web Server, workstations automatically get registration at first connect to Dr.Web 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 Dr.Web Server.

11. At this, new workstations are not connected automatically, but placed by Dr.Web Server into the newbies group. After connecting to Dr.Web 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 8](#)).



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 website at <https://products.drweb.com/register/v4/> unless other address specified in the registration card attached to the product. Visit the website 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 website.
- 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 website 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 **Administrator Manual**, subchapters of [Chapter 3: 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 **Administrator 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.

