Dr.WEB

Enterprise Security Suite

Installation Manual

Dr.Web Enterprise Security Suite
Version 13.0
Installation Manual
5/14/2025

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 that provide effective protection against malicious software and spam.

Doctor Web customers include home users around the world, government agencies, small businesses, and nationwide corporations.

Since 1992, Dr.Web anti-virus solutions have been known for their continuous excellence in malware detection and compliance with international information security standards.

The state certificates and awards received by Dr.Web solutions, as well as the worldwide use of our products, are the best evidence of exceptional trust in the company products.

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

Table of Contents

Chapter 1: Introduction 6

1.1. About the Manual 6

1.2. Conventions and Abbreviations 8

Chapter 2: Dr.Web Enterprise Security Suite 10

2.1. About the Product 10

2.2. System Requirements 20

2.3. Distribution Package 31

Chapter 3: Licensing 34

Chapter 4: Getting Started 36

4.1. Creating the Anti-virus Network 36

4.2. Configuring Network Connections 40

4.2.1. Direct Connections 41

4.2.2. Dr.Web Server Detection Service 42

4.2.3. SRV Protocol 42

4.3. Providing a Secure Connection 43

4.3.1. Traffic Encryption and Compression 43

4.3.2. Tools to Ensure Secure Connection 49

4.3.3. Connecting Clients to Dr.Web Server 51

4.4. Integration of Dr.Web Enterprise Security Suite with Active Directory 53

Chapter 5: Installation of Dr.Web Enterprise Security Suite Components 56

5.1. Installing Dr.Web Server 56

5.1.1. Installing Dr.Web Server for Windows OS 56

5.1.2. Installing Dr.Web Server for Unix-like OS 63

5.2. Installing Dr.Web Agent 65

5.2.1. Installation Files 66

5.2.2. Local Installation of Dr.Web Agent 68

5.2.3. Remote Installation of Dr.Web Agent 80

5.3. Installing Dr.Web Scanning Server 96

5.4. Installing NAP Validator 98

5.5. Installing Dr.Web Proxy Server 98

5.5.1. Creating Dr.Web Proxy Server Account 99

5.5.2. Installing Dr.Web Proxy Server as a Part of Dr.Web Agent for Windows Installation 101

5.5.3. Installing Dr.Web Proxy Server Using Installer 102
5.5.4. Connecting Dr.Web Proxy Server to Dr.Web Server 105
5.6. Installation Error Codes 108
Chapter 6: Removal of Dr.Web Enterprise Security Suite Components 110
6.1. Removing Dr.Web Server 110
6.1.1. Removing Dr.Web Server for Windows OS 110
6.1.2. Removing Dr.Web Server for Unix-like OS 110
6.2. Removing Dr.Web Agent 111
6.2.1. Removing Dr.Web Agent for Windows OS 111
6.2.2. Removing Dr.Web Agent through Active Directory 114
6.3. Removing Dr.Web Scanning Server 115
6.4. Removing Dr.Web Proxy Server 115
6.4.1. Local Removing Dr.Web Proxy Server 116
6.4.2. Remote Removing Dr.Web Proxy Server 117
Chapter 7: Upgrading Dr.Web Enterprise Security Suite Software and Its Components 118
7.1. Upgrading Dr.Web Server for Windows OS 119
7.2. Upgrading Dr.Web Server for Unix-like OS 122
7.3. Upgrading Dr.Web Agent 126
7.3.1. Upgrading Dr.Web Agents on Stations under Windows OS 126
7.3.2. Upgrading Dr.Web Agents on Stations under Android OS 128
7.3.3. Upgrading Dr.Web Agents on Stations under Linux and macOS 129
7.4. Upgrading Dr.Web Proxy Server 129
7.4.1. Updating Dr.Web Proxy Server During Operation 129
7.4.2. Updating Dr.Web Proxy Server via the Installer 131

Chapter 1: Introduction

1.1. About the Manual

Documentation for the administrator of Dr.Web Enterprise Security Suite anti-virus network is intended to introduce general features of the software suite and provide detailed information on delivering comprehensive anti-virus protection for company computers using Dr.Web Enterprise Security Suite.

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

1. **Installation Manual**

   The Installation Manual will be useful to a company manager who makes a decision to purchase and install a comprehensive anti-virus protection system.

   Installation Manual explains how to build an anti-virus network and install its main components.

2. **Administrator Manual**

   The Administrator Manual is meant for the *anti-virus network administrator,* i. e., an employee of the company who is responsible for anti-virus protection of computers (workstations and servers) of this network.

   The anti-virus network administrator should either have system administrator privileges or work closely with a local network administrator, be competent in anti-virus protection strategy, and have an in-depth knowledge of Dr.Web anti-virus packages for all operating systems that are used on the network.

3. **Appendices**

   The Appendices provide technical information describing configuration parameters for the anti-virus components and the syntax and values of instructions used to work with these modules.

Above-mentioned documents have cross-references between them. When you download these documents to a local computer, cross-references will work as long as the documents are placed in the same folder, under their initial names.

In addition, the following manuals are provided:

1. **Anti-virus Network Quick Installation Guide**

   It provides brief information on the installation and initial configuration of anti-virus network components. For detailed information refer to the administrator documentation.

2. **Station management manuals**

   They provide information about centralized configuration of anti-virus software on workstations, performed by the anti-virus network administrator using the Dr.Web Security Control Center.

3. **User Manuals**

   They provide information on how to configure Dr.Web anti-virus software directly on protected stations.

4. **Web API Manual**

   It provides technical details on the integration of Dr.Web Enterprise Security Suite with third-party software via Web API.

5. **Dr.Web Server Database Structure Manual**

   It describes the internal structure of the Dr.Web Server database and provides examples of its use.

All the listed manuals are also provided as part of Dr.Web Enterprise Security Suite and can be accessed 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 continuously updated and the latest version can always be found on 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
	An important note or instruction.
	A warning about possible errors or important notes that require special attention.
Anti-virus network	A new term or an emphasis on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Names of keyboard keys.
`C:\Windows\`	Names of files and folders, code examples.
Appendix A	Cross-references to document chapters or internal hyperlinks to webpages.

Abbreviations

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

- ACL—Access Control List,
- CDN—Content Delivery Network,
- DB, DBMS—Database, Database Management System,
- DFS—Distributed File System,
- DN—Distinguished Name,
- 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,
- MIB—Management Information Base,
- MTU—Maximum Transmission Unit,

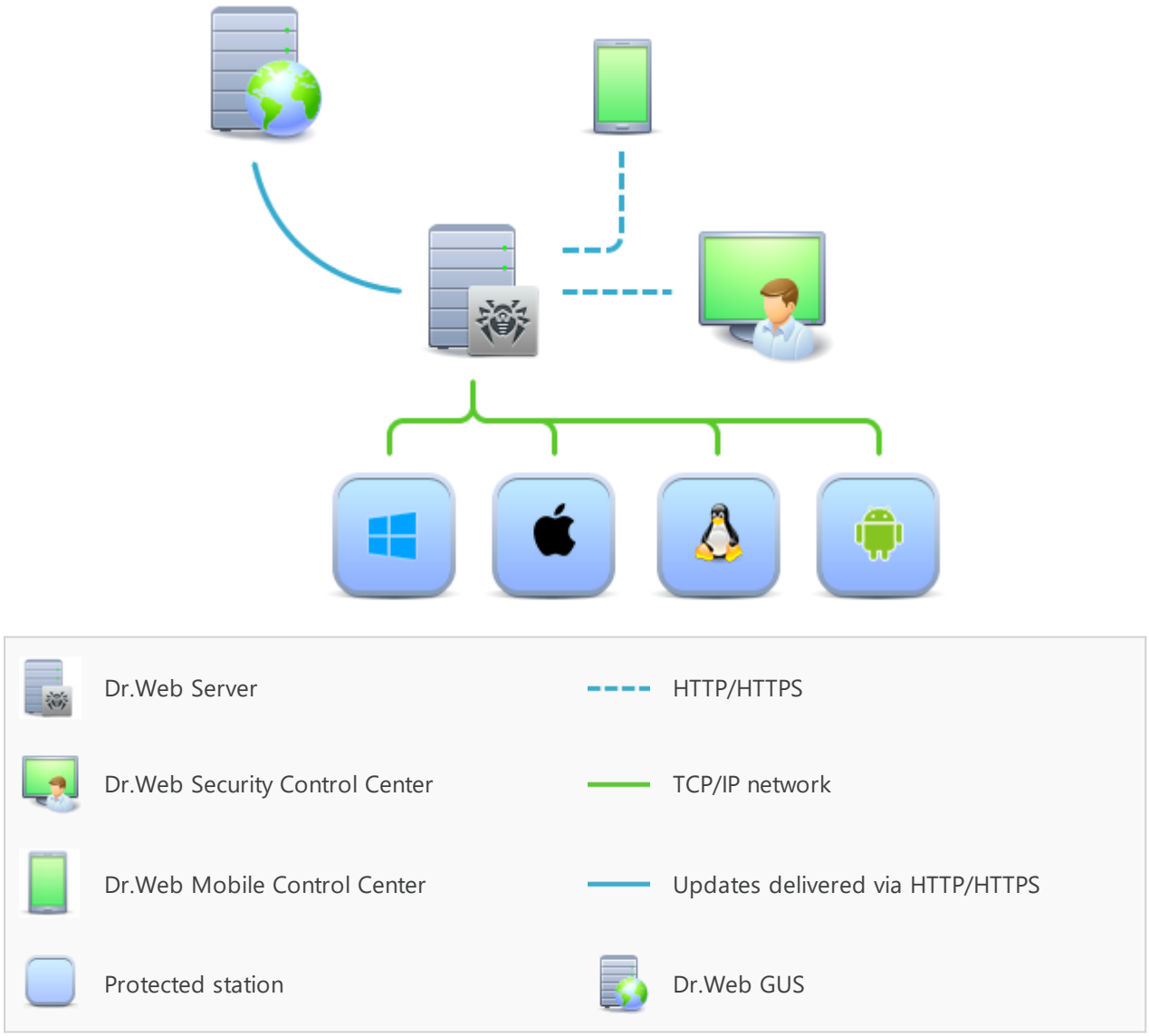
- NAP — Network Access Protection,
- OS—Operating System,
- TTL—Time To Live,
- UDS—UNIX Domain Socket.

Chapter 2: Dr.Web Enterprise Security Suite

2.1. About the Product

Dr.Web Enterprise Security Suite is designed to provide an integrated and complex anti-virus protection either for the local network of a company (including mobile devices) or home computers of its employees.

Once the components of Dr.Web Enterprise Security Suite are installed on corporate computers and mobile devices, they begin communicating with each other and become an integrated anti-virus network.



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 stations. In this context, a "station" means a protected device in

the anti-virus network, with Dr.Web Agent and the anti-virus package installed, acting as a client and interacting with Dr.Web Server. Stations can be computers, virtual and mobile devices of users and administrators, as well as computers functioning as LAN servers.

The anti-virus network components exchange information using TCP/IP network protocols. The anti-virus software can be installed (and subsequently managed) on protected stations either via LAN or the internet.

Centralized protection server

Centralized protection server (Dr.Web Server) is installed on one of the computers in the anti-virus network. The installation can be performed on any computer, not necessarily on a computer acting as a LAN server. General requirements for such a computer are specified in section System Requirements.

The cross-platform nature of Dr.Web Server allows it to be used on a computer with the following operating systems installed:

- Windows OS,
- Unix-like OS (Linux, FreeBSD).

The protection of the computer Dr.Web Server is installed on is identical to the protection of workstations as described in the Protection of network stations subsection, and can be implemented by installing a control module (Dr.Web Agent) and an anti-virus package.

Dr.Web Server stores distribution kits of anti-virus packages for various operating systems on protected computers, updates for virus databases and anti-virus packages, license keys and settings of anti-virus packages 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 distributes them to protected stations.

Several Dr.Web Servers can be combined into a hierarchical structure to serve protected stations in the anti-virus network.

Dr.Web Server backs up critical data (such as databases, configuration files, etc.)

Dr.Web Server keeps a consolidated log of anti-virus network events.

Unified database

Dr.Web Server is connected to a unified database where it stores statistics about anti-virus network events, Dr.Web Server settings, parameters of protected stations and anti-virus components installed on protected stations.

You can use the following types of databases:

An **embedded** SQLite3 database built into Dr.Web software.

An **external** database. Dr.Web software comes with built-in drivers for the following databases:

- MySQL, MariaDB DBMS,

- Oracle,
- PostgreSQL (including PostgreSQL Pro, Jatoba, and others),
- ODBC driver for connecting other databases such as Microsoft SQL Server/Microsoft SQL Server Express.

You can use any database that meets your requirements, such as: scalability, database software maintenance, administrative capabilities provided by the database itself and also the standards adopted in your company.

Centralized Protection Control Center

Dr.Web Security Control Center (also referred to as the Control Center) is automatically installed with Dr.Web Server and provides a web interface for remote administration of Dr.Web Server and the anti-virus network by configuring the settings of Dr.Web Server and the settings of protected computers which are stored on Dr.Web Server and protected computers.

The Control Center can be accessed on any computer with a network access to Dr.Web Server. The Control Center is compatible with the following web browsers:

- Windows Internet Explorer,
- Microsoft Edge,
- Mozilla Firefox,
- Google Chrome,
- Opera,
- Safari,
- Yandex Browser.

A complete list of supported web browsers is provided in section System Requirements.

The Control Center offers the following features:

- Easy installation of anti-virus protection on protected stations, including remote installation on workstations with a preliminary network scan to search for computers; creation of distribution files with unique identifiers and Dr.Web Server connection parameters, which facilitates the anti-virus installation process by an administrator or allows station users to install the anti-virus themselves (see detailed information in the Installing Dr.Web Agent section).
- Streamlined administration based on grouping of anti-virus network workstations.
- Centralized control of anti-virus packages on stations, including uninstallation of either individual components or the entire anti-virus package on stations running Windows OS; configuration of parameters of anti-virus package components; assignment of permissions to set up and manage the anti-virus packages for the users of protected computers .
- Centralized control of anti-virus scanning at workstations, including remote anti-virus scanning either on a scheduled basis or at the administrator's direct request via the

Control Center; centralized configuration of anti-virus scanning parameters and their delivery to workstations for local scanning using these parameters.

- Statistics on the status of protected stations, threat statistics, status of installed anti-virus software, status of running anti-virus components, and a list of hardware and software on protected stations.
- Flexible Dr.Web Server and anti-virus network administration system based on the differentiation of access rights for different administrators, as well as the ability to connect administrators via external authorization systems such as Active Directory, LDAP, RADIUS, PAM.
- Management of licenses for anti-virus protection of workstations, with a branched system of licenses for stations and groups of stations, as well as the ability to transfer licenses between several Dr.Web Servers in a multi-server configuration of the anti-virus network.
- Wide range of settings for configuring Dr.Web Server and its individual components, including the Dr.Web Server maintenance schedule; adding user hooks; flexible configuration of the update system for all anti-virus network components using the GUS and further propagation of updates on stations; configuration of the administrator notification system about anti-virus network events with various methods of notification delivery; setting up inter-server connections for configuring a multi-server anti-virus network.

Detailed information on described functions is given in the **Administrator Manual**.

The Web server is one of the Control Center components that are 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.

Mobile Control Center for centralized protection

Dr.Web Mobile Control Center is available as a separate component for mobile devices running iOS and Android. The basic device requirements for running the application are given in section System Requirements.

Mobile Control Center connects to Dr.Web Server via an encrypted protocol using the credentials of the anti-virus network administrator. Mobile Control Center supports the basic set of the Control Center features:

1. Managing anti-virus components installed on anti-virus network stations:
   - launching a fast or a full scan either on selected stations or on all stations in selected groups;
   - configuring Dr.Web Scanner's reaction to detected malware;
   - viewing and managing files in the Quarantine either on selected stations or on all stations in the selected group.
2. Displaying statistics on anti-virus network status:

- number of stations registered at Dr.Web Server and their current status (online/offline);
- statistics related to threats on protected stations.

3. Managing stations and groups:
   - reviewing settings;
   - reviewing and managing components of the anti-virus package;
   - deleting stations and groups;
   - send custom messages to the stations;
   - rebooting stations running Windows OS;
   - adding stations and groups to favorites for quick access.
4. Viewing and managing messages about major events in the anti-virus network through interactive push notifications:
   - displaying all notifications on Dr.Web Server;
   - configuring reactions to notification events;
   - searching for a notification by filter parameters;
   - deleting notifications;
   - preventing notifications from being lost due to automatic deletion.
5. Managing new stations, which await connection to Dr.Web Server:
   - approving access;
   - rejecting stations.
6. Managing the stations, where anti-virus software failed to update:
   - displaying failed stations;
   - updating components on failed stations.
7. Managing Dr.Web Server repository:
   - viewing product status in the repository;
   - updating repository from Dr.Web Global Update System.
8. Searching for specific anti-virus network stations and groups by their names, addresses, or IDs.

You can download Dr.Web Mobile Control Center from the Control Center or directly from the App Store or Google Play.

Protection of network stations

A control module (Dr.Web Agent) and an anti-virus package are installed on protected computers and mobile devices in the network.

The cross-platform nature of the software ensures that anti-virus protection is provided for computers and mobile devices running the following operating systems:

- Windows OS,
- Unix-like OS,

- macOS,
- Android OS.

Protected stations can include both workstations and LAN servers. Anti-virus protection of Microsoft Outlook mail system is also supported.

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

If Dr.Web Server is unavailable, virus databases on protected stations can be updated from the Global Update System via the internet.

Depending on the operating system installed on the station, the following protection functions are provided:

Stations running Windows OS

Anti-virus scanning

Scans a computer on demand or according to a schedule. Anti-virus scanning of stations can also be initiated remotely from the Control Center, including scanning for rootkits.

File monitor

Continuous file system protection in real time. Checks all launched processes, as well as all files created on hard drives and files opened on removable media.

Mail monitor

Checks all incoming and outgoing email messages when using email clients.

The spam filter is also available (if your license allows you to use it).

Web monitor

Checks all data exchange with the websites via HTTP protocol. It neutralizes malicious software in HTTP traffic (for example, in sent and received files) and restricts access to suspicious or incorrect resources.

Office Control

Controls access to local and global network resources, specifically restricting access to websites. Controls the integrity of important files by preventing accidental modification or infection It also restricts access to unwanted information for employees.

Firewall

Monitors connection attempts and filters connections both on network and application levels.

Quarantine

Isolates malware and suspicious objects into a specified folder.

Self-protection

Protects Dr.Web Enterprise Security Suite files and folders from unauthorized or accidental removal and modification by users or malicious software. If self-protection is enabled, access to Dr.Web Enterprise Security Suite files and folders is granted to Dr.Web processes only.

Preventive protection

Prevents potential security threats. Controls access to critical operating system objects, controls driver loading, program autorun and system service operation. It also monitors running processes and blocks them if malicious activity is detected.

Application control

Monitors the activity of all processes on stations. Allows the anti-virus network administrator to control which applications are allowed to run and on protected stations and which are not.

Stations running Unix-like OS

Anti-virus scanning

A scanning engine. Performs anti-virus scanning (scans files, disk boot records and other data received from other components of Dr.Web for UNIX). It queues files that are waiting to be scanned. Cures the files that can be cured.

Anti-virus scanning, Quarantine management

Scans file system objects and manages quarantined files. It receives scanning tasks from other Dr.Web for UNIX components. It also scans file system directories according to a received task, submits files for scanning to the scanning engine. It also removes malicious files, moves them to quarantine, restores them from quarantine, and manages quarantine directories. The component creates and updates a cache that stores information on scanned files to reduce the frequency of repeated file scanning.

Used by components that scan file system objects, such as SpIDer Guard (for Linux, SMB, NSS).

Web traffic scanning

ICAP server analyzing requests and traffic, which goes via HTTP proxy servers. It also prevents transmitting malicious files and access to network hosts belonging to the internet resource categories and to domain lists, blocked by the system administrator.

File monitor for GNU/Linux-based OS

The Linux file system monitor. It operates in the background and monitors file operations (creating, opening, closing, and running a file) in the GNU/Linux file systems. It sends tasks to the file check component to scan new, modified or executable files upon a program startup.

File monitor for Samba directories

Monitor of Samba shared file system directories. It operates in the background and monitors file operations (creating, opening, closing, reading or writing operations) in directories used by Samba SMB file server. It sends the contents of new and modified files to the file check component for checking.

NSS file monitor

NSS volume monitor (Novell Storage Services). It operates in the background and monitors file operations (creating, opening, closing and writing operations) on NSS volumes mounted to a specified file system point. It sends the contents of new and modified files to the file check component for checking.

Internet connection scanner

Network traffic and URL monitoring component. It is designed to scan for threats any data downloaded from the global network to a local host and then transmitted from that host to an external network. The component also prevents connections to any network hosts included either into unwanted categories of web resources or to blocked domain lists created by the system administrator.

Mail monitor

Email scanning component. Analyzes messages transferred over email protocols, sorts out emails and prepares them for scanning for threats. It can operate in one of two modes:

1. As a filter for mail servers (Sendmail, Postfix, etc.) connected via the Milter, Spamd or Rspamd interface.
2. As a transparent mail protocol proxy (SMTP, POP3, IMAP). In this mode, it uses SpIDer Gate.

Stations running macOS

Anti-virus scanning

Scans a computer on user demand and according to a schedule. Anti-virus scanning of stations can also be initiated remotely from the Control Center, including scanning for rootkits.

File monitor

Continuous file system protection in real time. Checks all launched processes, as well as all files created on hard drives and files opened on removable media.

Web monitor

Checks all data exchange with the websites via HTTP protocol. It neutralizes malicious software in HTTP traffic (for example, in sent and received files) and restricts access to suspicious or incorrect resources. It neutralizes malicious software in HTTP traffic (for

example, in sent and received files) and restricts access to suspicious or incorrect resources.

Quarantine

Isolates malware and suspicious objects into a specified folder.

Mobile devices running Android OS

Anti-virus scanning

Scans a mobile device on user demand and according to a schedule. Anti-virus scanning of stations can also be initiated remotely from the Control Center, including scanning for rootkits.

File monitor

Continuous file system protection in real time. Checks all files as they are saved in the device memory.

Call and SMS filter

Filters incoming phone calls and SMS messages, while allowing you to block any unwanted messages and calls, such as advertisements or messages and calls from unknown numbers.

Anti-theft

Detects device location or locks its functions in case it has been lost or stolen.

Restricting internet access

URL filter that protects a mobile device user from inappropriate websites.

Firewall

Monitors connection attempts and filters connections both on network and application levels.

Security troubleshooting

Diagnosis and analysis of mobile device security and remediation of any detected problems and vulnerabilities.

Application launch control

Blocks applications from launching on a mobile device, unless they are included in the list of allowed applications by the administrator.

Ensuring connection between anti-virus network components

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

Dr.Web Proxy Server

Dr.Web Proxy Server can be optionally included in the anti-virus network. The main function of the Dr.Web Proxy Server is to provide connection between Dr.Web Server and protected stations in cases when direct connection is impossible.

Dr.Web Proxy Server allows you to use any computer included in the anti-virus network for the following purposes:

- As an update relay center to reduce the network load on Dr.Web Server and on the connection between Dr.Web Server and Dr.Web Proxy Server, as well as to reduce the time required for protected stations to receive updates using the caching function.
- As a forwarder of events related to threats on protected stations to Dr.Web Server, which also reduces the network load and ensures trouble-free operation in cases when, for example, a group of stations is located in a network segment, that is isolated from the segment where Dr.Web Server is located.

Traffic compression

To reduce network traffic to a minimum, special compression algorithms are used when the anti-virus network components exchange data.

Traffic encryption

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

Additional features

NAP Validator

NAP Validator is a separate component that uses Microsoft Network Access Protection (NAP) technology to check the software health of protected stations. Enhanced security is achieved by implementing network station performance requirements.

Repository loader

Dr.Web Repository loader is a separate utility that downloads Dr.Web Enterprise Security Suite products from Dr.Web Global Update System. It can be used for downloading Dr.Web Enterprise Security Suite updates and storing them on Dr.Web Server which is not connected to the internet.

Dr.Web Scanning Server

Dr.Web Scanning Server is provided as a separate component 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

To install and use Dr.Web Enterprise Security Suite the following is required:

- Anti-virus network computers should have access to Dr.Web Server or to the Dr.Web Proxy Server.
- Please open the following ports on the applicable computers to enable interaction of the anti-virus components:

<table>
<tr><th>Port numbers</th><th>Protocols</th><th>Connections</th><th>Purpose</th></tr>
<tr><td rowspan="3">2193</td><td>TCP</td><td>• incoming, outgoing for Dr.Web Server and the Proxy Server
• outgoing for the Dr.Web Agent</td><td rowspan="2">For connection between Dr.Web Server and the anti-virus components and for interserver communications.

Also used by the Proxy Server to establish a connection with clients.</td></tr>
<tr><td>UDP</td><td>incoming, outgoing</td></tr>
<tr><td></td><td></td><td>For the Network Scanner.</td></tr>
<tr><td rowspan="2">139, 445</td><td>TCP</td><td>• outgoing for Dr.Web Server
• incoming for the Dr.Web Agent</td><td rowspan="2">For remote installation of Dr.Web Agent.</td></tr>
<tr><td>UDP</td><td>incoming, outgoing</td></tr>
<tr><td>9080</td><td>HTTP</td><td rowspan="3">• incoming for Dr.Web Server
• outgoing for the computer on which the Control Center is opened</td><td rowspan="2">For Dr.Web Security Control Center.</td></tr>
<tr><td>9081</td><td>HTTPS</td></tr>
<tr><td>10101</td><td>TCP</td><td>For the Dr.Web Server remote diagnostic utility.</td></tr>
<tr><td>80</td><td>HTTP</td><td rowspan="2">outgoing</td><td rowspan="2">For receiving updates from GUS.</td></tr>
<tr><td>443</td><td>HTTPS</td></tr>
<tr><td>18008</td><td>UDP</td><td>• incoming, outgoing for the Scanning Server
• incoming, outgoing for Dr.Web Virtual Agent</td><td>For finding any available Scanning Server by Dr.Web Virtual Agents using the Discovery service.</td></tr>
</table>

Port numbers	Protocols	Connections	Purpose
7090	TCP	• incoming for the Scanning Server • outgoing for Dr.Web Virtual Agent	For communication of Dr.Web Virtual Agents with a specific Scanning Server.

Dr.Web Server

Parameter	Requirements
CPU	An SSE2-capable CPU, 1.3 GHz or faster
RAM	• Minimum: 1 GB • Recommended: 2 GB or more
Free disk space	• At least 50 GB for the Dr.Web Server software, plus additional space for storing temporary files, for example. Agent personal installation packages (about 17 MB each) in the `var\installers-cache` subfolder of the Dr.Web Server installation folder • Up to 5 GB for the database • Regardless of where Dr.Web Server is installed, the following amount of free space is required on the Windows OS system disk or in /var/tmp for UNIX-like OS (or in any other temporary files folder, if it is redefined): ▫ Dr.Web Server installation requires at least 4.3 GB for launching the installer and unpacking temporary files ▫ Dr.Web Server requires free disk space on the system disk for storing temporary and working files depending on the size of the database and repository configuration
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 • ECP Veil • Rosa Virtualization 2.1, 3.0
Other	To use Oracle DB, the `Linux kernel AIO access library libaio`) is required Administrative utilities which can be downloaded from the **Administration** → **Utilities** section of the Control Center must be run on a computer that meets the Dr.Web Server system requirements

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.

Dr.Web Server cannot be installed on the same station with Dr.Web Proxy Server.

To install on Alt Linux, disable SELinux.

Dr.Web Server and Dr.Web Proxy Server installation on a Unix-like OS requires operating system support for the SysVinit initialization system. If it is not installed, install the appropriate package.

The list of supported operating systems:

Windows	**UNIX**
32 bit • Windows 7 • Windows 8 • Windows 8.1 • Windows 10 *64 bit* • Windows 7 • Windows 8 • Windows 8.1 • Windows 10 • Windows 11 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Server 2025	• Linux using the glibc library 2.13 or later • FreeBSD 11.3 or later As well as special versions of Linux distributions: ▪ Astra Linux Common Edition 2.12 Orel ▪ Astra Linux Special Edition 1.5 (with cumulative patch 20201201SE15) ▪ Astra Linux Special Edition 1.6 (with cumulative patch 20220829SE16) ▪ Astra Linux Special Edition 1.7 (with cumulative patch 20221110SE17) ▪ Astra Linux Special Edition 1.8 ▪ ALT 8 SP ▪ ALT Workstation 8 ▪ ALT Workstation 9 ▪ ALT Server 8 ▪ ALT Server 9 ▪ ALT Server 10 ▪ GosLinux IC6 ▪ RED OS 7.3 MUROM ▪ RED OS 8.0 In Alt 8 SP and Goslinux IC6 OS, mandatory access control is not supported. For Astra Linux OS, installation should be performed at startup with the "High" integrity level.

Dr.Web Proxy Server

Parameter	Requirements
CPU	An SSE2-capable CPU, 1.3 GHz or faster
RAM	At least 1 GB
Free disk space	At least 1 GB
Operating system	The list of operating systems is the same as for Dr.Web Server

Dr.Web Proxy Server cannot be installed on the same station as Dr.Web Server.

Dr.Web Security Control Center

Parameter	Requirements
Web browser	• Internet Explorer 11 • Microsoft Edge 0.10 or later • Mozilla Firefox 44 or later • Google Chrome 49 or later • Latest version of Opera • Latest version of Safari • Latest version of Yandex Browser
Screen resolution	Recommended screen resolution is 1280×1024
Other	If you are using Internet Explorer, be aware of the following limitations: • Full functionality of the Control Center in **Internet Explorer** with the **Enhanced Security Configuration** mode enabled is not guaranteed • If you install Dr.Web Server on a computer with an underscore (_) character in its name, you will not be able to use the Control Center to configure Dr.Web Server in Internet Explorer. In this case, use a different web browser • For proper operation of the Control Center, the IP address and/or DNS name of the computer where Dr.Web Server is installed must be added to the trusted sites of the web browser, in which you open the Control Center • To correctly open the Control Center from the **Start** menu on Windows 8 and Windows Server 2012 with a tiled interface, configure the following web browser parameters: go to **Internet Options** → **Programs** → **Opening Internet Explorer** and set the **Always in Internet Explorer** flag

	• To use the Control Center in Internet Explorer over the secure `https` protocol, install all the latest updates for the web browser • Using Internet Explorer in compatibility mode to access the Control Center is not supported

If your organization uses a reverse proxy server to access Dr.Web Security Control Center, certain settings are required to work with it. Examples of the settings are available at the following links:

For Nginx:

https://nginx.org/docs/http/websocket.html

For Apache:

https://httpd.apache.org/docs/2.4/mod/mod_proxy_wstunnel.html

https://www.serverlab.ca/tutorials/linux/web-servers-linux/how-to-reverse-proxy-websockets-with-apache-2-4/

Dr.Web Mobile Control Center

Operating system	Requirements
iOS	• Apple iPhone: iOS 9 and later • Apple iPad: iOS 9–12
Android	Android 5.0–14

NAP Validator

Parameter	Requirements
Operating system	Operating systems with Network Access Protection (NAP) technology support. Minimum requirements: • For a computer with a configured NAP server: Windows Server 2008. • For a computer with Dr.Web Agent installed: Windows Server 2008 with SP2
Other	Other system requirements for the NAP Validator are the same as those for Dr.Web Agent (see below). The requirements may vary depending on the operating system on which the anti-virus solution is installed

Dr.Web Scanning Server

Parameter	Requirements
CPU	CPU with the following architecture and command system: Intel/AMD: 32-bit (IA-32, x86) and 64-bit (x86_64, x64, AMD64)
RAM	At least 500 MB of free RAM (1 GB or more is recommended)
Free disk space	At least 1 GB of free disk space
Hypervisor	• VMware • Hyper-V • Xen • KVM
Operating system	Linux, FreeBSD. The list of operating systems is the same as the list for the UNIX OS anti-virus package
Network connections	Availability of network connections: • Connection to Dr.Web Server to enable updates for virus databases and filter databases • Connection for processing requests from Virtual agents

Dr.Web Agent and anti-virus package

The requirements differ depending on the operating system for which the anti-virus solution is installed.

No other anti-virus software (including other versions of Dr.Web anti-virus programs, firewalls or content filters) should be installed on the workstations of an anti-virus network managed by Dr.Web Enterprise Security Suite.

Windows

Parameter	Requirements
CPU	An i686-compatible processor
Operating system	For 32-bit platforms: • Windows XP with Service Pack 2 or later • Windows Vista with Service Pack 2 or later • Windows 7 with Service Pack 1 or later

Parameter	Requirements
	• Windows 8 • Windows 8.1 • Windows 10 22H2 or earlier • Windows Server 2003 with Service Pack 1 • Windows Server 2008 with Service Pack 2 or later For 64-bit platforms: • Windows Vista with Service Pack 2 or later • Windows 7 with Service Pack 1 or later • Windows 8 • Windows 8.1 • Windows 10 22H2 or earlier • Windows 11 24H2 or earlier • Windows Server 2008 with Service Pack 2 or later • Windows Server 2008 R2 with Service Pack 1 or later • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Server 2025
RAM	Minimum 512 MB
Screen resolution	Recommended 1024 × 768 or higher
Cloud and virtualization environment support	Operation of the program is guaranteed in the following environments: • VMware • Hyper-V • Xen • KVM
Other	To update Dr.Web virus databases and Dr.Web components, it is required to connect to the centralized protection server or to the internet in the Mobile mode. Dr.Web plug-in for Microsoft Outlook requires one of the following Microsoft Outlook clients from the Microsoft Office suite: • Outlook 2000 • Outlook 2002 • Outlook 2003 • Outlook 2007

Parameter	Requirements
	• Outlook 2010 with Service Pack 2 • Outlook 2013 • Outlook 2016 • Outlook 2019 • Outlook 2021

File system protection on stations running Windows Enterprise multi-session (Windows Enterprise for Virtual Desktops) requires the **SpIDer Guard for Windows servers** component to be licensed.

As Microsoft has stopped supporting the SHA-1 hashing algorithm, please ensure that your operating system supports the SHA-256 hashing algorithm before installing the software on Windows Vista, Windows 7, Windows Server 2008, or Windows Server 2008 R2. To do this, install all the recommended updates listed in the Windows Update section. For detailed information, please visit the Doctor Web official website.

UNIX

Parameter	Requirements
Platform	Processors of the following architectures and command systems are supported: • Intel/AMD: 32-bit (*IA-32*, *x86*); 64-bit (*x86-64*, *x64*, *amd64*) • ARM64 • E2K (*Elbrus*) • IBM POWER9, Power10 (*ppc64el*)
RAM	At least 500 MB of free RAM (1 GB or more is recommended)
Free disk space	At least 2 GB of free disk space on a volume where the product directories are located
Operating system	GNU/Linux (based on kernel version 2.6.37 or later, using `glibc` library 2.13 or later, `systemd` initialization system ver. 209 or later), FreeBSD. The supported operating system versions are listed below. The operating system must support the PAM authentication mechanism
Other	The following valid network connections: • valid Internet connection to enable updates for virus databases and Dr.Web components; • when operating in the centralized protection mode, connection to the server on the local network is enough; connection to the Internet is not required

Platform	Supported GNU/Linux versions
x86_64	• ALT 8 SP • ALT Server 9, 10 • ALT Workstation 9, 10 • Astra Linux Common Edition (Orel) 2.12 • Astra Linux Special Edition 1.6 (with cumulative patch 20200722SE16), 1.7, 1.8 • CentOS 7, 8 • Debian 9, 10, 11, 12 • Fedora 37, 38 • GosLinux IC6 • Red Hat Enterprise Linux 7, 8 • RED OS 7.2 MUROM, RED OS 7.3 MUROM, RED OS 8 • SUSE Linux Enterprise Server 12 SP3 • Ubuntu 18.04, 20.04, 22.04, 24.04
x86	• ALT 8 SP • ALT Workstation 9, 10 • CentOS 7 • Debian 10
ARM64	• ALT 8 SP • ALT Server 9, 10 • ALT Workstation 9, 10 • Astra Linux Special Edition (Novorossiysk) 4.7 • CentOS 7, 8 • Debian 11, 12 • Ubuntu 18.04
E2K	• ALT 8 SP • ALT Server 10 • ALT Workstation 10 • Astra Linux Special Edition (Leningrad) 8.1 (with cumulative patch 8.120200429SE81) • Elbrus-D MCST 1.4 • GS CS Elbrus 8.32 TVGI.00311-28
ppc64el	• CentOS 8 • Ubuntu 20.04

In ALT 8 SP, Elbrus-D MCST 1.4 and GosLinux IC6 mandatory access control is not supported.

For other GNU/Linux distributions that meet the above mentioned requirements, full compatibility with the application is not guaranteed. If a compatibility issue occurs, contact technical support.

Platform	Supported FreeBSD versions
x86	11, 12, 13, 14
x86_64	11, 12, 13, 14

For FreeBSD OS, application can be installed only from the universal package.

macOS

Parameter	Requirements
Device	Mac running macOS operating system. We cannot guarantee that Dr.Web will function correctly on non-Apple-branded computers
Free disk space	2 GB
Operating system	• OS X 10.11 El Capitan • macOS 10.12 Sierra • macOS 10.13 High Sierra • macOS 10.14 Mojave • macOS 10.15 Catalina • macOS 11 Big Sur • macOS 12 Monterey • macOS 13 Ventura • macOS 14 Sonoma • macOS 15 Sequoia We cannot guarantee that Dr.Web will function correctly on modified macOS systems or Hackintoshes

Android OS

Parameter	Requirements
Operating system	Android version 4.4–15
CPU	x86/x86-64/ARMv7/ARMv8/ARMv9

Parameter	Requirements
Free RAM	At least 512 MB
Free space on device	At least 45 MB (for data storage)
Screen resolution	At least 800×480
Other	Internet connection (for virus database updates)

Dr.Web Mail Security Suite (Microsoft Exchange Server)

Parameter	Requirements
RAM	512 MB or more
Free disk space	1 GB or more
Operating system	• Windows Server 2008 x64 with SP2 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 • Windows Server 2025
Microsoft Exchange Server version	• Microsoft Exchange Server 2007 x64 with SP1 • Microsoft Exchange Server 2010 x64 with SP1 • Microsoft Exchange Server 2013 with SP1 (Cumulative Update 5 or running Exchange2013-KB2938053-Fixit script is required) • Microsoft Exchange Server 2016 with Cumulative Update 3 (or later) • Microsoft Exchange Server 2019

Dr.Web Mail Security Suite (IBM Lotus Domino Windows)

Parameter	Requirements
CPU	Compatible with the i686 command system
RAM	512 MB or more
Free disk space	750 MB or more. Temporary files created during installation require additional disk space

Parameter	Requirements
Screen resolution	Recommended 1280 × 1024 or higher, supporting at least 256 colors
File system	NTFS or FAT32
Operating system	For 32-bit platforms: • Windows Server 2008 • Windows Server 2008 R2 For 64-bit platforms: • Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022
Additional software	Lotus software: • IBM Lotus Domino for Windows version 8.5 - 9.0.1 • IBM Lotus Notes for Windows version 7.0.2 - 9.0.1 • IBM Domino for Windows 10.1 • IBM Notes for Windows 10.0 • HCL Domino for Windows 11.0 • HCL Notes for Windows 11.0 Web browsers suitable for the web interface: • Internet Explorer 8 or later • Mozilla Firefox 3 or later • Opera 9 or later

2.3. Distribution Package

Dr.Web Enterprise Security Suite distribution package is selected based on the operating system running Dr.Web Server:

1. For Unix-like OS:
   - `drweb-esuite-server-<package_version>-<build>-<OS_version>.tar.gz.run`
     Dr.Web Server distribution kit
   - `drweb-reploader-<OS>-<bitness>`

Console version of Dr.Web Repository Loader

2. For Windows OS:
   - `drweb-esuite-server-<package_version>-<build>-<OS_version>.exe`
     Dr.Web Server distribution kit
   - `drweb-<package_version>-<build>-esuite-agent-full-windows.exe`
     Dr.Web Agent full installer
   - `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

The Dr.Web Server distribution package includes 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 built-in filters of anti-virus components and Dr.Web Anti-spam for Windows
- Documentation
- Doctor Web company news.

Serial numbers are bundled with the distribution package. After registering these serial numbers you will get files with license keys.

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

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

You can find detailed information on how to work with the Dr.Web Server repository in the **Administrator Manual**, section Administration of Dr.Web Server Repository.

Chapter 3: Licensing

Dr.Web Enterprise Security Suite anti-virus solution requires a license.

The scope and price of Dr.Web Enterprise Security Suite license depend on the number of protected stations including servers within the Dr.Web Enterprise Security Suite network.

You should provide this information to your local distributor when purchasing a license for Dr.Web Enterprise Security Suite. The number of Dr.Web Servers running on the network does not affect the cost of the license.

License key file

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

A license key file is write-protected with an electronic signature. Editing the file makes it invalid. To avoid accidentally corrupting a license key file, do not modify and/or save it after opening it in a text editor.

License key files are provided as a ZIP archive, which contains one or several key files for protected stations.

The user can receive the key files as follows:

- A license key file is included into the Dr.Web Enterprise Security Suite anti-virus distribution package with the purchase, if this license key file was included when the distribution package was created. 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 the Doctor Web company website at https://products.drweb.com/register/v4/ unless a different address was specified in the registration card attached to the product. Visit the website above, fill in the form with the buyer information and type the registration serial number (it is provided on the registration card) in the corresponding field. An archive with key files will be sent to the specified email address. Also, the key files will be available for download directly from the website.
- A license key file can be provided on a separate storage medium.

It is recommended that you keep a license key file until it expires and use it to reinstall and restore program components. If a license key file is lost, you can repeat the registration process at the above mentioned website and restore the license key file. Please note that you will need to enter the same registration serial number and the same buyer information as during the initial registration, you can only change the email address. In this case, a license key file will be sent to the new address.

Demo key file

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 time of use. Demo key files are sent upon a request made through the web form at https://download.drweb.com/demoreq/biz/. Requests are considered on a case-by-case basis. If your request is approved, an archive with license key files will be sent to the specified email address.

Detailed information on principles and features of Dr.Web Enterprise Security Suite licensing is given in the **Administrator Manual**, Licensing.

The use of key files during the installation is described in section Installing Dr.Web Server.

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

Chapter 4: Getting Started

4.1. Creating the Anti-virus Network

Quick start to anti-virus network deployment:

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

   Select a computer that will perform the functions of Dr.Web Server. The anti-virus network can incorporate several Dr.Web Servers. This configuration is described in the **Administrator Manual**, section Peculiarities of a Network with Several Dr.Web Servers.

   Dr.Web Server can be installed on any computer, not only on a computer acting as a LAN server. General system requirements for this computer are described in section System Requirements.

   The same version of Dr.Web Agent is installed on all protected stations including LAN servers. The difference is in the list of installed anti-virus components which is determined by the Dr.Web Server settings.

   Installation of Dr.Web Server and Dr.Web Agent requires one-time access (physical or using tools for remote control and program launch) to corresponding computers. All further actions are performed remotely from the anti-virus network administrator's workstation (which can also be located outside the local network) and do not require access to Dr.Web Servers or stations.

   When planning the anti-virus network, it is also recommended that you create a list of persons who will have access to the Control Center as required by their job duties, as well as a list of roles and the responsibilities assigned to each role. An administrative group needs to 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 on managing administrative groups and permissions see the **Administrator Manual**, Chapter 6: Anti-Virus Network Administrators.

2. Based on the plan you created earlier, determine which products for which operating systems should be installed on the corresponding network nodes. Detailed information about the supported products is given in the Distribution Package section.

   All required products can be purchased as a Dr.Web Enterprise Security Suite box solution or downloaded from the official website of Doctor Web at https://download.drweb.com.

   Dr.Web Agents for stations running Android OS, Linux OS, macOS can also be installed from standalone packages and then get connected to the central Dr.Web Server. The

settings of Dr.Web Agents are described in the corresponding **User Manuals**.

3. Install the Dr.Web Server general distribution kit on the selected computer or computers. The installation procedure is described in section Installing Dr.Web Server.

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

By default, Dr.Web Server starts automatically after installation and upon every restart of the operating system.

4. Install and configure Dr.Web Proxy Server, if necessary. A detailed description is given in section Installing Dr.Web Proxy Server.
5. If your anti-virus network consists of virtual machines, it is recommended that you use the Scanning Server. The detailed description of the installation and the configuration procedures is given in section Installing Dr.Web Scanning Server.
6. To configure Dr.Web Server and the anti-virus software on stations, connect to Dr.Web Server using Dr.Web Security Control Center.

Dr.Web Security Control Center can be opened on any computer, not only on the computer where Dr.Web Server is installed. It requires only a network connection to the computer where 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, NetBIOS or domain name of the computer on which Dr.Web Server is installed.

In the authorization request dialog window, specify the administrator credentials. By default, the administrator credentials are as follows:

- Name: **admin**.
- Password:
  - for Windows OS—the password that was set during the Dr.Web Server installation.
  - for a Unix-like OS—the password that was automatically created during the installation of Dr.Web Server (see also Installing Dr.Web Server for Unix-like OS).

On successful connection to Dr.Web Server, the main window of the Control Center opens (for detailed description refer to the **Administrator Manual**, section Dr.Web Security Control Center).

If you installed Dr.Web Scanning Server, specify its address in the station settings. For detailed information refer to the **Administrator Manual,** section Connecting Stations to the Scanning Server).

7. Perform the initial configuration of Dr.Web Server (a detailed description of the Dr.Web Server settings is given in the **Administrator Manual**, in Chapter 10: Configuring Dr.Web Server):
   a. In the License manager section, add one or several license keys and allocate them to corresponding groups, particularly to the **Everyone** group. This 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 the anti-virus network to be update by Dr.Web GUS. If the anti-virus network includes protected stations running Android OS, Linux OS or macOS, you need to download the corresponding **Dr.Web enterprise products**.

   In the Repository State section, update the products in the Dr.Web Server repository. Updating might take a long time. Wait for the update process to complete before proceeding with the configuration.

By default, after installing Dr.Web Server, the updates for the **Virus databases for Android**, **Content filter databases for UNIX** and **Dr.Web Proxy Server** repository products are downloaded from GUS only when these products are requested by the stations. For more details, see the **Administrator Manual**, section Detailed Repository Configuration.

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

   c. The **Administration** → **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**, section Updating Dr.Web Server and Restoring it from Backup.
   d. If necessary, set up network connections to change the default network settings used for interaction of all anti-virus network components (see the **Administrator Manual**, section Network connections).
   e. If necessary, set up the list of Dr.Web Server administrators. External authentication of administrators is also available. For more details, see the **Administrator Manual**, Chapter 6: Anti-Virus Network Administrators.
   f. Before using the anti-virus software, you may want to change the settings of the backup folder for the Dr.Web Server critical data (see the **Administrator Manual**, section Setting Dr.Web Server Schedule). It is recommended that you keep the backup folder on a different local disk to reduce the risk of losing the Dr.Web Server files and backup copies at the same time.
8. Specify the settings and configuration of the anti-virus software for stations (for a detailed description of how to set up groups and stations see the **Administrator Manual**, Chapter 7 and Chapter 8):
   a. If necessary, create user groups on the protected stations.
   b. Configure the settings of the **Everyone** group and created user groups. In particular, configure the section with the components to be installed.

9. Install Dr.Web Agent software on the stations.

   In the Installation Files section, review the list of files provided for the Dr.Web Agent installation. Select an installation option that is suitable for you based on the station's operating system, remote installation support, Dr.Web Server settings specified during Dr.Web Agent installation, etc. For example:

   - If users install the anti-virus manually, use personal installation packages which are created using the Control Center separately for each station. This type of packages can also be sent to users by email directly from the Control Center. The stations will automatically connect to Dr.Web Server once the installation is complete.
   - If you need to install the anti-virus on several stations within a user group, you can use the group installation package which is created using the Control Center in a single copy for several stations of a particular group.
   - For remote installation over the network on one or more stations running Windows or Linux, use the network installer. The installation is performed from the Control Center.
   - You can also perform the remote installation over the network to one or more stations simultaneously using the Active Directory service. To do this, use the Dr.Web Agent installer for networks with Active Directory, which is included in the Dr.Web Enterprise Security Suite distribution kit; however, it is not included in the Dr.Web Server installer.
   - If you need to reduce the load on the network connection between Dr.Web Server and stations during the installation, you can use the full installer which installs Dr.Web Agent and the protection components simultaneously.
   - Installation on stations running Android OS and macOS can be performed locally according to general practices. It is also possible to connect an already installed standalone product to Dr.Web Server using an appropriate configuration.

   To ensure proper operation of Dr.Web Agent on server editions of Windows OS starting with Windows Server 2016, make sure to manually disable Windows Defender using group policies.

10. Dr.Web Agents connect to Dr.Web Server immediately after installation. Anti-virus stations are authorized by Dr.Web Server according to the policy defined by the administrator (see the **Administrator Manual**, section New Stations Approval Policy):
    a. When installing using installation packages and selecting automatic approval on Dr.Web Server, the stations are automatically registered when they first connect to Dr.Web Server, and no additional approval is required.
    b. When installing using the installer and selecting manual access approval, new stations should be manually approved by the administrator to be registered with Dr.Web Server. In this case, new stations are not connected automatically, instead they are placed by Dr.Web Server into a group of newbies.
11. After connecting to Dr.Web Server and receiving the settings, a corresponding set of anti-virus components specified in the primary group settings is installed on the station.

Restart the computer to finish the installation of station components.

12. The stations and anti-virus software can also be configured after the installation (detailed description is given in the **Administrator Manual**, in Chapter 8).

4.2. Configuring Network Connections

General Information

The following clients are connected to Dr.Web Server:

- Dr.Web Agents
- Dr.Web Agent installers.
- Neighboring Dr.Web Servers.
- Dr.Web Proxy Servers.

Connection is always initiated by a client.

The following types of connection to Dr.Web 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 Dr.Web Server Detection Service.

   Clients use this Service by default (if a different type of connection is not explicitly set).

   You can use this approach, if the system requires an overhaul, in particular, if you need to move Dr.Web Server to another computer or change the IP-address of a computer with Dr.Web Server.
3. Using the SRV protocol.

   This approach allows you to search for Dr.Web Server by the computer name or the Dr.Web Server service using the SRV records on the DNS server.

If you configure the anti-virus network to use direct connections, the Dr.Web Server Detection Service can be disabled. To do this, in the transport settings (**Administration** → **Dr.Web Server configuration** → the **Network** tab → the **Transport** tab) leave the **Cluster address** field empty.

Firewall setup

To enable communication between anti-virus network components, all ports and interfaces, which are used by these components, must be opened on all computers in the anti-virus network.

During Dr.Web Server installation, the installer automatically adds Dr.Web Server ports and interfaces to the exceptions of the Windows operating system firewall.

If your computer has a firewall other than the built-in Windows firewall, the network administrator should set it up manually.

4.2.1. Direct Connections

Configuring Dr.Web Server

An address must be set in the Dr.Web Server settings (see the **Appendices**, section Appendix D. The Specification of Network Addresses) to listen for incoming TCP-connections.

You can specify this parameter in the following Dr.Web Server settings: **Administration** → **Dr.Web Server configuration** → **Network** tab → **Transport** tab → **Address** field.

By default, the following parameters are set to "listen" by Dr.Web Server:

- **Address**: empty value—use *all network interfaces* for this computer, on which Dr.Web Server is installed.
- **Port**: `2193`—use port `2193`.

Port 2193 is registered with IANA for Dr.Web Enterprise Management Service.

For the proper functioning of the entire Dr.Web Enterprise Security Suite anti-virus network, it is sufficient for Dr.Web Server to listen to at least one TCP-port known to all clients.

Configuring Dr.Web Agent

During Dr.Web Agent installation, you can set the Dr.Web Server address (IP-address, NetBIOS or domain name of the computer running Dr.Web Server) directly in the installation parameters:

```
drwinst /server <Dr.Web_Server_Address>
```

It is recommended that you use Dr.Web Server name in the FQDN format as the Dr.Web Server address, registered in the DNS service when installing Dr.Web Agent. This will make it easier to configure the anti-virus network in case of moving Dr.Web Server to another computer.

By default, the `drwinst` command launched without parameters will scan the network for Dr.Web Servers and will try to install Dr.Web Agent from the first found Dr.Web Server (*Multicast* mode using the Dr.Web Server Detection Service).

Thus, the Dr.Web Server address becomes known to Dr.Web Agent during installation.

You can change the Dr.Web Server address in the Dr.Web Agent settings manually later.

4.2.2. Dr.Web Server Detection Service

When using this type of connection, the client does not know the address of Dr.Web Server beforehand. Each time before establishing a connection, the client searches through the network for Dr.Web Server. To find it, the client sends a broadcast query and waits for a response containing the Dr.Web Server address. After receiving the response, the client establishes a connection to Dr.Web Server.

For this to work, Dr.Web Server must *listen* for such queries.

There are several ways to set up such a connection. The most important thing is to match the Dr.Web Server search method on the client side with the Dr.Web Server response part.

By default, Dr.Web Enterprise Security Suite uses the *Multicast over UDP* mode:

1. Dr.Web Server is registered in a multicast group with an address specified in the Dr.Web Server settings.
2. Dr.Web Agents, when searching for Dr.Web Server, send multicast queries to the group address specified in step 1.

By default, Dr.Web Server listens for any queries coming to `udp/231.0.0.1:2193` (similarly to direct connections).

You can set this parameter in the Dr.Web Server settings: **Administration** → **Dr.Web Server configuration** → **Network** → **Transport** → **TCP/IP**. Empty value instructs to use the default address indicated above.

4.2.3. SRV Protocol

Clients running Windows OS support the SRV client network protocol (its format is described in the **Appendices**, section Appendix D. The Specification of Network Addresses).

Access to Dr.Web Server via the SRV records is implemented as follows:

1. During the Dr.Web Server installation, it is registered in the Active Directory domain, the installer registers a corresponding SRV record on the DNS server.

   SRV record is registered on the DNS server according to the RFC2782 (see https://datatracker.ietf.org/doc/html/rfc2782).

2. When requesting a connection to Dr.Web Server, a user specifies access via the `srv` protocol.

   For example, to launch the Dr.Web Agent installer:

   - with explicit specification of the `myservice` service name:

```
drwinst /server "srv/myservice"
```

- without specifying the service name. In this case, the SRV records are searched for the default name—`drwcs`:

```
drwinst /server "srv/"
```

3. Transparently for the user, the client uses the SRV protocol's features to access Dr.Web Server.

If Dr.Web Server is not specified directly, the default name of the service is `drwcs`.

4.3. Providing a Secure Connection

4.3.1. Traffic Encryption and Compression

The encryption mode is used to ensure the security of data transmitted over an insecure channel and to prevent the possible disclosure of valuable information and tampering with the software downloaded to the protected stations.

Dr.Web Enterprise Security Suite anti-virus network uses the following cryptographic means:

- Electronic digital signature (GOST R 34.10-2001).
- Asymmetric encryption (VKO GOST R 34.10-2001 – RFC 4357).
- Symmetric encryption (GOST 28147-89).
- Cryptographic hash function (GOST R 34.11-94).

Dr.Web Enterprise Security Suite anti-virus network encrypts the traffic between Dr.Web Server and the following clients:

- Dr.Web Agents.
- Dr.Web Agent installers.
- Neighbor Dr.Web Servers.
- Dr.Web Proxy-servers.

Since traffic between components, especially between Dr.Web Servers, can be significant, the anti-virus network supports traffic compression. Configuration of the compression policy and the compatibility of such settings between different clients is similar to the encryption settings.

Settings Compatibility policy

The encryption and compression policy is set separately for each component of the anti-virus network; furthermore, settings of other components should be compatible with the Dr.Web Server settings.

When coordinating encryption and compression settings on Dr.Web Server and a client, please note that certain combinations are incompatible and, if selected, will result in disconnecting the client from Dr.Web Server.

Table 4-1 shows which settings ensure that the connection between Dr.Web Server and the clients will be encrypted/compressed (+), or non-encrypted/uncompressed (–) and which combinations are incompatible (**Error**).

Table 4-1. Compatibility of the encryption and compression policy settings

Client settings	Dr.Web Server settings		
	Yes	**Possible**	**No**
Yes	+	+	Error
Possible	+	+	–
No	Error	–	–

Traffic encryption places a significant load on computers that are close to the minimum system requirements for the components installed on them. Therefore, if traffic encryption is not needed to provide additional security, you can disable this mode.

To disable encryption, you should first switch Dr.Web Server and then other components to the **Possible** mode in order to avoid the creation of incompatible client-server pairs.

Using the compression mode will reduce traffic, but will considerably increase the memory usage and the CPU load on computers, more than the encryption.

Connecting through Dr.Web Proxy Server

If you want to connect clients to Dr.Web Server via Dr.Web Proxy Server, you should consider the encryption and compression settings on all three components. In this case:

- Settings of Dr.Web Server and the Proxy Server (here it plays the role of a client) need to comply with table 4-1.
- Settings of the client and the Proxy Server (here it plays the role of Dr.Web Server) need to comply with table 4-1.

The ability connect through the Proxy Server depends on the version of Dr.Web Server and the client supporting certain encryption technologies:

- If Dr.Web Server and the client support TLS encryption that is used in version 13.0, it is enough to meet the above requirements to establish a working connection.
- If one of the components does not support TLS encryption: Dr.Web Server and/or the client are version 10 or earlier which provides GOST encryption, then an additional check is performed according to the table 4-2.

Table 4-2. Compatibility of the encryption and compression policy settings when using the Proxy Server

Client connection settings	Dr.Web Server connection settings			
	Nothing	**Compression**	**Encryption**	**All**
Nothing	Normal mode	Normal mode	Error	Error
Compression	Normal mode	Normal mode	Error	Error
Encryption	Error	Error	Transparent mode	Error
All	Error	Error	Error	Transparent mode

Legend

Dr.Web Server and client connection settings	
Nothing	Neither compression nor encryption is supported
Compression	Only compression is supported
Encryption	Only encryption is supported
All	Both, compression and encryption are supported
Resulting connection	
Normal mode	Established connection implies the operation in the normal mode, i. e., with command processing and caching
Transparent mode	Established connection implies the operation in the transparent mode, i. e., without command processing and without caching. This mode uses the lowest version of encryption protocol supported by all the components: e. g. if one of the components (Dr.Web Server or Dr.Web Agent) supports version 13, and the other only supports version 10, then the latter version is used
Error	Connection of the Proxy Server both to Dr.Web Server and the client will be terminated

If Dr.Web Server and Dr.Web Agent have different version: for example, one is version 13, and the other is version 10 or earlier, then the following limitations apply to the connections established though the Proxy Server:

- Data can be cached on the Proxy Server only if both connections to Dr.Web Server and to the client are established without the encryption.

- Encryption will be used only if both connections to Dr.Web Server and to the client are established using the encryption and the same compression parameters (compression is used for both connections or not used for both of them).

Encryption and compression settings on Dr.Web Server

Setting the encryption and compression policies of Dr.Web Server

1. Select **Administration** in the main menu of the Control Center.
2. In the window that opens, select **Dr.Web Server configuration** in the control menu.
3. On the **Network** → **Transport** tab, select the necessary option in the **Encryption** and **Compression** drop-down lists:
   - **Yes**—enforces traffic encryption (or compression) for all clients (set by default for encryption, if the parameter was not modified during Dr.Web Server installation).
   - **Possible**—enables traffic encryption(or compression) for those components which are configured to support it.
   - **No**—encryption (or compression) is not supported (set by default for compression, if the parameter has not been modified during the Dr.Web Server installation).

When configuring encryption and compression on Dr.Web Server, please consider the capabilities of the clients that will be connected to this Dr.Web Server. Not all clients support traffic encryption and compression.

Encryption and compression settings on Dr.Web Proxy Server

Centralized management of encryption and compression settings for Proxy Server

If the Proxy Server is not connected to Dr.Web Server for centralized management of its settings, configure the connection as described in section Connecting Dr.Web Proxy Server to Dr.Web Server.

1. Open the Control Center of the Dr.Web Server which controls the Proxy Server.
2. Select **Anti-virus network** in the main menu of the Control Center, in the hierarchical list of the opened window, click the name of the Proxy Server whose settings you want to edit or its primary group if the Proxy Server settings are inherited.
3. In the control menu that opens, select **Dr.Web Proxy Server**. This opens the settings section.
4. Go to the **Listen** tab.
5. In the **Client connection parameters** section, in the **Encryption** and **Compression** drop-down lists, select the traffic encryption and compression modes for the data transmission channels between the Proxy Server and the connected clients: Dr.Web Agents and Dr.Web Agent installers.

6. In the **Dr.Web connection parameters** section, you can specify the list of Dr.Web Servers to which the traffic will be redirected. Select the required Dr.Web Server in the list and click on the toolbar to edit the settings for connection to the selected Dr.Web Server. In the window that opens, in the **Encryption** and **Compression** drop-down lists, select the traffic encryption and compression modes for the data transmission channel between the Proxy Server and the specified Dr.Web Server.
7. Click **Save** to save all the settings.

Local management of encryption and compression policies for Proxy Server

If the Proxy Server is connected to the managing Dr.Web Server for remote configuration, then the Proxy Server configuration file will be rewritten according to the settings received from Dr.Web Server. In this case, you should configure the settings remotely from Dr.Web Server or disable the option that allows receiving the configuration from this Dr.Web Server.

Description of the `drwcsd-proxy.conf` configuration file is given in the **Appendices**, in F4. Dr.Web Proxy Server Configuration File.

1. On the computer with the Proxy Server installed, open the `drwcsd-proxy.conf` configuration file.
2. Edit the encryption and compression settings for connections with clients and Dr.Web Servers.
3. Restart the Proxy Server:
   - For Windows OS:
     - If the Proxy Server runs as a Windows service, restart the service using the conventional means.
     - If the Proxy Server runs in console, press CTRL+BREAK.
   - For Unix-like OS:
     - Send the `SIGHUP` signal to the Proxy Server daemon.
     - Execute the following command:

     For Linux OS:

     ```
     /etc/init.d/dwcp_proxy restart
     ```

     For FreeBSD OS:

     ```
     /usr/local/etc/rc.d/dwcp_proxy restart
     ```

Station-side encryption and compression settings

Centralized management of station-side encryption and compression policies

1. Select **Anti-virus Network** in the Control Center main menu, then click the name of a group or a station in the hierarchical list of the opened window.
2. In the control menu that opens, select **Connection parameters**.
3. On the **General** tab, in the **Compression mode** and **Encryption mode** drop-down lists, select one of the following:
   - **Yes**—enables obligatory traffic encryption (or compression) to Dr.Web Server.
   - **Possible**—enables encryption (or compression) of traffic to Dr.Web Server if the Dr.Web Server settings do not prohibit it.
   - **No**—encryption (or compression) is not supported.
4. Click **Save**.
5. The changes will take effect as soon as the settings will be propagated to stations. If stations are offline at the time when the settings are changed, the changes will be applied as soon as stations connect to Dr.Web Server.

Windows

Encryption and compression settings can be set during Dr.Web Agent installation:

- When installed remotely from the Control Center, the encryption and compression mode is set directly in the **Network installation** section.
- When installed locally, the GUI installer does not allow you to change the encryption and compression settings; however, these settings can be configured using the command line switches when the installer is launched (see the **Appendices**, section G1. Network Installer).

After Dr.Web Agent is installed, you cannot change the encryption and compression settings locally on the station. The default mode is **Possible** (if no other value was set during the installation), that is, the use of encryption and compression depends on the settings of Dr.Web Server. However, the settings of Dr.Web Agent can be changed using the Control Center (see above).

Android

Encryption and compression are not supported. Connection will be impossible if the **Yes** value for encryption and/or compression is specified on Dr.Web Server or Dr.Web Proxy Server (for connection via Dr.Web Proxy Server).

Linux

You cannot change the encryption and compression settings during installation. The default mode is **Possible**.

After installation, you can change encryption and compression settings locally on the station only using the command line mode. A description of the command line mode and the corresponding switches can be found in the **Dr.Web Desktop Security Suite (Linux) User Manual**.

Station-side settings can also be changed using the Control Center (see above).

macOS

You cannot change the encryption and compression settings locally on the station. The default mode is **Possible**, that is, the use of encryption and compression depends on the settings of Dr.Web Server.

Station-side settings can be changed using the Control Center (see above).

4.3.2. Tools to Ensure Secure Connection

During the installation of Dr.Web Server, certain tools are created to ensure a secure connection between the components of the anti-virus network.

Dr.Web Server private encryption key drwcsd.pri

It is stored on Dr.Web Server and is not shared with other components of the anti-virus network.

If the private key is lost, the connection between components of the anti-virus network must be restored manually (all keys and certificates must be generated and distributed to all components of the network).

The private key is used as follows:

a) *Creating pubic keys and certificates.*

   The public encryption key and the certificate are automatically generated from the private encryption key during Dr.Web Server installation. Additionally, you can create a new private key or use the existing one (for example, from the previous Dr.Web Server installation). You can also create encryption keys and certificates at any time using the `drwsign` Dr.Web Server utility (see the **Appendices**, section G7.1. Digital keys and certificates generation utility).

   Information on public keys and certificates is given below.

b) *Authenticating Dr.Web Server.*

Dr.Web Server is authenticated by remote clients on the basis of an electronic digital signature (once during each connection).

Dr.Web Server digitally signs a message using a private key and sends the message to a client. The client verifies the signature of the received message using the certificate.

c) *Decrypting the data*.

If the traffic between Dr.Web Server and clients is encrypted, the decryption of the data sent by a client is performed on Dr.Web Server using the private key.

Dr.Web Server public encryption key *.pub

It is available to all components of the anti-virus network. A public key can always be generated from a private key (see above). Each time you generate it from the same private key you will get the same public key.

Starting with Dr.Web Server version 11, a public key is used for connection with previous versions of clients. The rest of the functionality is transferred to a certificate, containing, among other things, a public encryption key.

Dr.Web Server certificate drwcsd-certificate.pem

It is available to all components of the anti-virus network. A certificate contains a public encryption key. Certificates can be generated from a private key (see above). Each time a certificate is generated from the same private key, a new certificate is created.

Clients connected to Dr.Web Server, are associated with a specific certificate, so if a client loses its certificate, it can be restored only if the same certificate is used by another network component: in this case, the certificate can be copied to a client from Dr.Web Server or from the other client.

Certificates are used as follows:

a) *Authenticating Dr.Web Server*.

Dr.Web Server is authenticated by remote clients based on an electronic digital signature (once during each connection).

Dr.Web Server digitally signs a message using the private key and sends the message to a client. The client verifies the signature of the received message using the certificate (specifically, the public key specified in the certificate). The previous version of Dr.Web Server used the public key directly.

A client must have one or more trusted certificates from Dr.Web Servers to which a client can connect.

b) *Encrypting the data*.

When the traffic between Dr.Web Server and clients is encrypted, the encryption of the data is performed by a client using a public key.

c) *Implementation of a TLS session between Dr.Web Server and remote clients*.

d) Authenticating the Proxy Server.

Dr.Web Proxy Server is authenticated by remote clients on the basis of an electronic digital signature (once during each connection).

The Proxy Server digitally signs its certificates using the private key and the certificate of the Dr.Web Server. The client that trusts the Dr.Web Server certificate will automatically trust the certificates signed by it.

Web server private key

It is stored on Dr.Web Server and is not shared with other components of the anti-virus network. Its usage details are given below.

Web server certificate

It is available to all components of the anti-virus network.

It is required to implement a TLS session between a web server and a browser (over HTTPS).

During the Dr.Web Server installation, a self-signed certificate based on the web server's private key is generated which is not accepted by web browsers because it is not issued by a well-known certificate authority.

To ensure a secure connection (HTTPS), you must do one of the following:

- Add the self-signed certificate to Trusted Certificates or to Exclusions for all stations and web browsers on which the Control Center is opened.
- Obtain a certificate signed by a well-known certificate authority.

4.3.3. Connecting Clients to Dr.Web Server

In order to connect to Dr.Web Server, a client must have a Dr.Web Server certificate regardless of whether the traffic between Dr.Web Server and the client is encrypted or not.

The following clients can connect to Dr.Web Server: Dr.Web Agents, their installers, neighboring Dr.Web Servers, and Dr.Web Proxy Servers.

Dr.Web Agents

For Dr.Web Agents to work in centralized mode with a connection to Dr.Web Server, one or more trusted certificates from Dr.Web Servers, to which Dr.Web Agent can connect, must be present on the station.

A certificate that was used during installation and certificates received centrally from Dr.Web Server are stored in the registry; however, the certificate files themselves are not used.

A single copy of the certificate can be added to the Dr.Web Agent installation folder (but not to the registry) and to the shared list of certificates using a command line switch. This certificate is used, among other things, to be able to connect to Dr.Web Server in case of an error in the central settings.

If the certificate is missing or invalid, Dr.Web Agent will not be able to connect to Dr.Web Server; however, it will remain operational and will update using the Mobile mode if it is allowed for this station.

Dr.Web Agent installers

When installing Dr.Web Agent, a Dr.Web Server certificate must be present on a station together with the selected installation file.

If you run the installation package generated in the Control Center, the certificate is included in the installation package and you do not need to additionally specify the certificate file.

After Dr.Web Agent is installed, the certificate data is written to the registry and the certificate file itself is no longer used.

If the certificate is missing or invalid, the installer will not be able to install Dr.Web Agent (applies to all types of the Dr.Web Agent installation files).

Neighboring Dr.Web Servers

When establishing a connection between neighboring Dr.Web Servers, it is necessary to specify the certificate of the Dr.Web Server to which a connection is established on each Dr.Web Server to be configured (see the **Administrator Manual**, section Setting Connections between Several Dr.Web Servers).

If at least one certificate is missing or invalid, you will not be able to establish a multi-server connection.

Dr.Web Proxy Servers

To connect the Proxy Server to Dr.Web Server with the option of remote control via the Control Center, you need to have a certificate on the station where the Proxy Server is installed. In this case the Proxy Server can also support encryption.

If the certificate is missing, the Proxy Server will continue to work; however, remote control, encryption and caching will not be available.

When upgrading an entire anti-virus network from a previous version that uses public keys to a new version that uses certificates, no other additional actions are required.

It is not recommended to install Dr.Web Agent bundled with Dr.Web Server version 11 and connect it to Dr.Web Server version 10 and vice versa.

4.4. Integration of Dr.Web Enterprise Security Suite with Active Directory

If the Active Directory service is used in the protected local network, you can configure the integration of Dr.Web Enterprise Security Suite components with this service.

Integration of Dr.Web Enterprise Security Suite with Active Directory is based on the methods described below.

All of the following methods are independent of each other and can be used both individually or in combination.

Registration of Dr.Web Server in the Active Directory domain to access Dr.Web Server using the SRV protocol

When installing Dr.Web Server, you can use the installer to register Dr.Web Server in the Active Directory domain. During registration, an SRV record corresponding to Dr.Web Server is created on the DNS server. Further, clients can access Dr.Web Server using this SRV record.

For more details, see the Installing Dr.Web Server for Windows OS and SRV Protocol.

Synchronization of anti-virus network structure with the Active Directory domain

It is possible to configure automatic synchronization of the anti-virus network structure with stations in the Active Directory domain. In this case, Active Directory containers which contain computers, become groups of anti-virus network to which workstations are assigned.

For this purpose, the **Synchronization with Active Directory** task is provided in the Dr.Web Server schedule. The administrator must create this task using the Dr.Web Server Task Manager.

For more details, see the **Administrator Manual**, section Setting Dr.Web Server Schedule.

Authentication of Active Directory users on Dr.Web Server as administrators

Users with Active Directory accounts can authenticate to Dr.Web Server to manage the anti-virus network. To do this, please use one of the following methods:

- LDAP/AD authentication. This method is available for Dr.Web Servers running on all supported OS. The access of users to Dr.Web Server is configured through corresponding Active Directory attributes in the Control Center. Direct access to the domain controller and to the Active Directory snap-in is not required, no additional configuration through Active Directory is required.
- Microsoft Active Directory. This method is available for Dr.Web Servers running on Windows OS included in the target domain. Users and user groups with access to Dr.Web Servers are configured directly in the Active Directory snap-in. Initial configuration using additional utilities is required. The `drweb-modify-ad-schema-<package_version>-<build>-<OS_version>.exe` and `drweb-aduac-<package_version>-<build>-<OS_version>.msi` packages are available in the Dr.Web Server repository, in **Dr.Web enterprise products**.

When choosing a method, you should take into account the Dr.Web Server operating system and the means of configuring authorized users.

For more details, see the **Administrator Manual**, section Authentication of Administrators.

Remote installation of Dr.Web Agents on stations in the Active Directory domain

Dr.Web Agent can be remotely installed on stations in the Active Directory domain. To do this:

a) As an administrator install a special Dr.Web Agent for Active Directory installer to a shared target directory. The `drweb-<package_version>-<build>-esuite-agent-activedirectory.msi` package is available in the Dr.Web Server repository, in **Dr.Web enterprise products**.

b) Configure appropriate Active Directory policies for automatic package installation on domain stations.

For more details, see the Installing Dr.Web Agent Software via Active Directory.

Locating stations in the Active Directory domain

Stations in the Active Directory domain can be located using the Network Scanner. It is possible to detect Dr.Web Agent on the located stations, and if it is not present, to install it remotely via the Control Center.

This approach to remote installation of Dr.Web Agent can be used together with the automatic package installation via the Active Directory policies (described above).

For more details, see the **Administrator Manual**, section Network Scanner.

Locating users in the Active Directory domain

Users in the Active Directory domain can be located to create their personal profiles and more accurately configure the Office Control and Application Control.

For more details, refer to the **Administrator Manual on managing stations under Windows**.

Chapter 5: Installation of Dr.Web Enterprise Security Suite Components

Before installing Dr.Web Enterprise Security Suite components, please refer to the Creating the Anti-virus Network.

5.1. Installing Dr.Web Server

Installing Dr.Web Server is the first step in setting up an anti-virus network. Until it is successfully installed, no other anti-virus network components can be installed.

The Dr.Web Server installation procedure depends on the Dr.Web Server version (for Windows OS or for Unix-like OS).

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

If the Dr.Web Server software is already installed on your computer, refer to sections Upgrading Dr.Web Server for Windows OS or Upgrading Dr.Web Server for Unix-like OSs, respectively.

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

The name of the Dr.Web Server installation folder must be in the same language as specified in the Windows language settings for non-Unicode programs. Otherwise, the Dr.Web Server installation will not be completed.

Alternatively, you can use English for the name of your installation folder.

Dr.Web Security Control Center is installed together with Dr.Web Server, which is used to manage the anti-virus network and configure Dr.Web Server.

By default, Dr.Web Server runs automatically after its installation on Windows OS and must be started manually on Unix-like OS.

5.1.1. Installing Dr.Web Server for Windows OS

The installation of Dr.Web Server for Windows OS is described below.

Before installing Dr.Web Server, please consider the following:

The distribution file and other files requested during the program installation should reside on local drives of the computer on which the Dr.Web Server software is installed; these files should be made available to the **LOCALSYSTEM** user.

Dr.Web Server should be installed by a user with administrator privileges on the computer.

After Dr.Web Server is installed it is necessary to update all Dr.Web Enterprise Security Suite components (see **Administrator Manual**, section Manual Update of Dr.Web Server Repository).

Figure 5-1 shows the flowchart of Dr.Web Server installation procedure. The steps in the flowchart correspond to the detailed description of the installation procedure shown below.

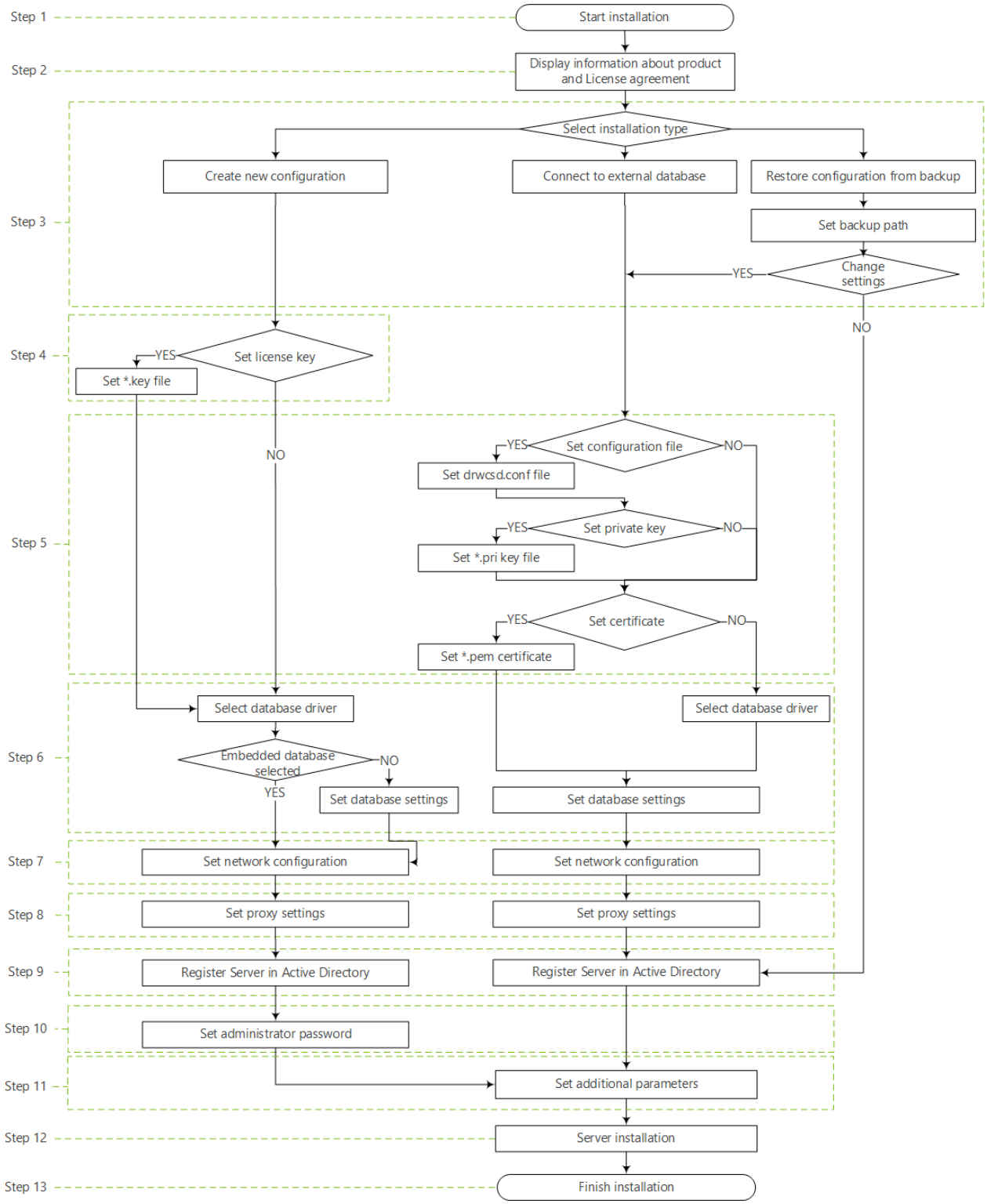


Figure 5-1. Dr.Web Server installation procedure flowchart (click any item in the flowchart to see its description)

Installing Dr.Web Server on a computer running Windows OS

1. Run the distribution file. The installation will check if a newer version of the distribution is available on GUS.

By default, the installer uses the language of the operating system. If necessary, you can change the installation language at any step by selecting the appropriate option in the right upper part of the installer window.

2. A window will open with information about the product being installed and a link to the text of the license agreement. After reading the agreement click **Next** to continue the installation.
3. In the next window, select the type of Dr.Web Server installation.
   - **Create new configuration**—this installation type creates a new Dr.Web Server configuration with default settings. The settings from the previous Dr.Web Server installations can't be used. This installation type initializes a new database regardless of the database type selected during setup. Click **Next**. Proceed to step 4.
   - **Connect to external database**—this type of installation means connecting to the existing external database of Dr.Web Server. This installation type upgrades the, existing external database from the previous Dr.Web Server installation. Click **Next**. Proceed to step 5.

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

   - **Restore configuration from backup**—all Dr.Web Server configurations will be restored from the specified backup of the previous Dr.Web Server installation. Specify the path to the backup.

     For this type of installation, the database dump from the backup will be imported and upgraded.

     - If necessary, you can manually change the settings from the backup. To do this, click **Change settings**—settings in steps 5-8 will be available.
     - If you do not need to change the settings manually, click **Next**. The configuration from the backup is used automatically. The private encryption key and certificate are extracted from the backup. To continue the installation, a configuration file is required. If the Wizard is unable to restore any settings from the backup, a window with these settings is displayed for you to specify them manually. Proceed to step 9.
4. If you selected the **Create new configuration** option in step 3, specify the licensing settings in the **License** window:
   - Select the **Configure licensing later** option to continue the Dr.Web Server installation without a license key.

     Note: a license is required to organize the anti-virus protection. License keys should be added after the Dr.Web Server installation using the License Manager, or the necessary number of licenses should be donated via interserver connection from a neighboring Dr.Web Server.
   - Select the **Specify the path to the license key** option to specify the Dr.Web Agent license key file during the Dr.Web Server installation.

You can use demo key files for evaluation purposes. Click **Request the demo key** to go to the Doctor Web official website and obtain demo license key files (see Demo key file).

5. If you selected the **Connect to external database** option in step 3, or if you selected **Change settings** when restoring a configuration from the backup, you can specify the following settings in the **Dr.Web Server configuration** window:
   - **Dr.Web Server configuration file**—path to the configuration file with Dr.Web Server settings from the previous installation (`drwcsd.conf`).
   - **Dr.Web Server private encryption key**—path to the Dr.Web Server private encryption key file from the previous installation. This will automatically generate the public key file (the public key content will be the same as the previous public key) and the certificate if it is not specified in the field below (at each generation from the same private key you will get a new certificate).
   - If you use an existing private encryption key, you can specify the previously used certificate file in the **Use existing Dr.Web Server certificate** field. This will allow already installed Dr.Web Agents to connect to the new Dr.Web Server, because clients connected to Dr.Web Server are bound to a specific certificate (a new certificate is generated from the same private key each time). Otherwise, after installation, it is necessary to copy a new certificate to all workstations where Dr.Web Agents were previously installed.

   Certificate must match the private encryption key.

   If no files are specified, a new configuration is created with default settings, new encryption keys, and a certificate.
6. The **Database driver** window allows you to set the parameters of the used database depending on the installation type:
   - If you selected the **Create new configuration** option in step 3, select the driver type to use:
     - Select the **SQLite (embedded database)** option to use the features built into Dr.Web Server. No additional parameters are required.
     - The other options imply usage an external DB. To configure access to a DB you should specify appropriate parameters. DBMS parameters are described in the **Appendices** (see Appendix A. The Description of the DBMS Settings. The Parameters of the DBMS Driver).
   - If in step 3 you selected the **Connect to external database** option or set the **Change settings** flag for the **Connect to external database** option:
     - If you specified the path to Dr.Web Server configuration file in step 5, the data will be taken from it automatically. Edit the data if necessary.
     - If you did not specify the path to the Dr.Web Server configuration file in step 5, select the external database driver and specify the settings of the external database to which Dr.Web Server should connect.

7. If at step 3 you have selected the **Create new configuration** or the **Connect to external database** option or set the **Change settings** flag for the **Connect to external database** option, the **Network Configuration** window will open. You can set a network protocol for the Dr.Web Server (only one network protocol can be specified; additional protocols can be configured later).
   - In the **Interface** and **Port** fields, specify the appropriate values for accessing the Dr.Web Server.

   By default, the `2193` port is used.

   Addresses should be specified in the network address format described in the **Appendices**, section. Appendix D. The Specification of Network Addresses.

   - Set the **Enable Dr.Web Server detection service** if you want the Dr.Web Server to respond to broadcast and multicast requests from other Dr.Web Servers using the IP address and service name specified in the corresponding fields below.
8. If at step 3 you have selected the **Create new configuration** or the **Connect to external database** option or set the **Change settings** flag for **Connect to external database** option, the **Proxy server** window will open where you can set the proxy server parameters when connecting to Dr.Web Server.

   To connect to the Dr.Web Server through the proxy server, set the **Use proxy server** flag.

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

   Specify the following parameters to connect to the proxy server:
   - **Proxy server address**—the address of the proxy server (required field),
   - **User name**, **Password**—user name and the password for accessing the proxy server, if the proxy server supports authorized connection.
   - In the **Authorization method** drop-down list, select the necessary method of authorization at proxy server, if the proxy server supports authorized connection.
9. If the computer where Dr.Web Server is installed is included in the Active Directory domain, the next window will prompt you to register the Dr.Web Server in the Active Directory domain. During registration in the Active Directory domain, the SRV record corresponding to the Dr.Web Server is created on the DNS server. Later, clients will be able to access Dr.Web Server using this SRV record.

   Specify the following registration parameters:
   - Set the **Register Dr.Web Server in the Active Directory** flag.
   - In the **Domain** field, specify the name of the Active Directory domain to which Dr.Web Server should be registered. If the domain is not specified, the domain in which the computer running Dr.Web Server is registered is used.

- In the **User name** and **Password** fields, enter the credentials of the Active Directory domain administrator.
- **DNS server** addresses are retrieved automatically and their number depends on the specified DNS servers.

10. If you selected the **Create new configuration** option in step 3, the **Administrator password** window opens. Specify the password for the anti-virus network administrator who is created by default with the admin login and a full set of permissions to manage the anti-virus network. For the other types of installation, the password of the main administrator from the database of the previous Dr.Web Server installation is used.
11. The next window informs you that the Wizard is ready to install Dr.Web Server. If necessary, you can configure additional installation parameters. To do this, click **Additional parameters** at the bottom of the window and specify the following settings:
    - On the **General** tab:
        - In the **Dr.Web Security Control Center interface language** drop-down list, select the default interface language for Dr.Web Security Control Center.
        - In the **Dr.Web Agent interface language** drop-down list, select the default interface language for Dr.Web Agent and anti-virus package components to be installed on stations.
        - Set the **Share Dr.Web Agent installation folder** flag to change the usage mode and the name of the Dr.Web Agent shared installation folder (by default, the name of the hidden shared resource is selected).

          See detailed information about the shared resource in **Appendices**, F6. Share.conf Configuration File.
        - Set the **Launch Dr.Web Server after installation is complete** flag to start Dr.Web Server automatically after the installation.
        - Set the **Update repository after installation is complete** flag to automatically update the Dr.Web Server repository after the installation is completed.
        - Set the **Restrict access to Dr.Web Server** flag to restrict local access to Dr.Web Server. Dr.Web Agent Installers, Dr.Web Agents and other Servers (for existing anti-virus network created with Dr.Web Enterprise Security Suite) will not be able to access Dr.Web Server. You can change these settings later in the Dr.Web Security Control Center menu **Administration** → **Dr.Web Server configuration** → **Modules** tab.
        - Set the **Send statistics to Doctor Web company** flag to send statistics about events related to threats to the Doctor Web company.
    - On the **Path** tab:
        - In the **Dr.Web Server installation folder** field, specify the folder in which Dr.Web Server will be installed. To change the default folder, click **Browse** and select the required folder.
        - In the **Dr.Web Server backup folder** field, specify the folder where Dr.Web Server critical data should be backed up according to the Dr.Web Server schedule tasks. To change the default folder, click **Browse** and select the required folder.

- On the **Log** tab, you can specify the settings for logging Dr.Web Server operation.

  After the additional parameter setup is finished, click **OK** to apply these changes or **Cancel** if no changes were made or to cancel all specified changes.

12. Click **Install** to begin the installation. No further actions are required by the installer.
13. When the installation is completed, click **Finish**.

As a rule, Dr.Web Server can be managed using Dr.Web Security Control Center, which acts as an interface to Dr.Web Server.

The installation wizard creates the **Dr.Web Server** folder in the **Programs** main menu of Windows OS. The folder contains the following items for configuring and managing Dr.Web Server:

- The **Server control** folder contains the commands for starting, restarting and shutting down Dr.Web Server, as well as the commands for setting up the logging parameters and other Dr.Web Server commands described in detail in **Appendix** G3. Dr.Web Server.
- The **Web interface** item opens Dr.Web Security Control Center and connects to the Dr.Web Server installed on this computer (at https://localhost:9081).
- The **Documentation** item opens the administrator documentation in HTML format.

The structure of the Dr.Web Server installation folder is described in the **Administrator Manual**, section Dr.Web Server.

5.1.2. Installing Dr.Web Server for Unix-like OS

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

Installing Dr.Web Server for Unix-like OS

1. Use the following command to start Dr.Web Server installation:

   `./<distribution_file>.tar.gz.run`

You can use command line switches to launch the installation package. Command line parameters are given in the **Appendices**, section H6. Dr.Web Server Installer for Unix-like OS

The default administrator name is **admin**.

2. Next, the text of the license agreement will be displayed. To proceed with the installation, you must accept the license agreement.
3. To use the settings from the previous installation saved in the backup, enter the path to the backup folder (or press ENTER to use the default folder, which is `/var/tmp/drwcs`). To install Dr.Web Server without using the settings from the previous installation, enter 0.

4. If an additional distribution kit (extra) is detected in the system, you will be prompted to delete it before Dr.Web Server installation is started. You will not be able to continue the installation without deleting the extra distribution kit.
5. Now the program components will be installed on your computer. During the installation, you may be asked to confirm several actions using the administrator credentials.
6. During the installation, a random password is generated for the main administrator. After the installation is completed, this password is displayed in the console, together with the Dr.Web Server installation summary.

During the installation of Dr.Web Server for **FreeBSD** OS an rc script `/usr/local/etc/rc.d/drwcsd` is created.

Use the following commands:

- `/usr/local/etc/rc.d/drwcsd stop`—to manually stop Dr.Web Server,
- `/usr/local/etc/rc.d/drwcsd start`—to manually start Dr.Web Server.

Please note that no license key is specified during Dr.Web Server installation. License keys should be added after Dr.Web Server installation using the License Manager.

Configuring Astra Linux version 1.6 for installing Dr.Web Server in the CSE Mode

If Dr.Web Server is installed on Astra Linux version 1.6 operating in the CSE (Closed Software Environment) mode, you may not be able to run the installer because the public encryption key of Dr.Web Server is missing from the list of trusted keys. In this case, you should reconfigure the CSE mode, and restart the installer.

Reconfiguring CSE mode

1. Install the `astra-digsig-oldkeys` package from the OS installation disk, if it is not yet installed.
2. Place the Dr.Web Server public encryption key into the `/etc/digsig/keys/legacy/keys` directory (create the directory if it does not exist).
3. Run the following command:

```
# update-initramfs -k all -u
```

4. Restart the operating system.

Configuring Astra Linux Special Edition with PostgreSQL using mandatory access control

To configure PostgreSQL to work with mandatory access control, set the value of the `ac_ignore_socket_maclabel` parameter to `false` in the `/etc/postgresql/<DB_version>/main/postgresql.conf` file. After the parameter is set, the DBMS server will check the security flag of the incoming connection and transmit only the information with the flag not higher than the incoming connection flag.

```
ac_ignore_socket_maclabel = false
```

5.2. Installing Dr.Web Agent

Dr.Web Agent should be installed under the Administrator account of the respective computer.

No other anti-virus software (including other versions of Dr.Web anti-virus programs, firewalls or content filters) should be installed on the workstations of an anti-virus network managed by Dr.Web Enterprise Security Suite.

To guarantee proper operation of Dr.Web Agent on server editions of Windows OS starting from Windows Server 2016, disable Windows Defender manually using group policies.

Dr.Web Agent can be installed on a workstation as follows:

1. Locally.

   Dr.Web Agent can be installed locally on a user's computer or mobile device by an administrator or user.

2. Remotely.

   Dr.Web Agent can be installed remotely using the Control Center via LAN. This type of installation is performed by an anti-virus network administrator. Therefore, no user intervention is required.

Dr.Web Agent installation on top of Dr.Web standalone product on stations running Windows OS

If the Dr.Web Agent installer is launched to install Dr.Web Agent either locally or remotely on a station with a standalone product, the installed product will switch from the standalone mode to the centralized protection mode. After connection and authorization on Dr.Web Server, the stations can receive updates, new settings and a list of components to be installed, then a reboot may be required.

When installing Dr.Web Agent on LAN servers and cluster computers, please note the following:

- When installing Dr.Web Agents on computers used as terminal servers (**Terminal Services** are installed on Windows OS), in order to ensure operation of Dr.Web Agents in user terminal sessions, it is recommended to install Dr.Web Agents locally, using the Add or Remove Programs Wizard in **Control Panel** of the Windows OS. Remote installation in this case may cause Remote Desktop Protocol errors.
- It is not recommended to install SpIDer Gate, Office Control, SpIDer Mail and Dr.Web Firewall components on servers that perform important network functions (domain controllers, license distribution servers and etc.) to avoid possible conflicts between network services and internal components of Dr.Web anti-virus.
- Installation of Dr.Web Agent in a cluster must be performed separately for each cluster node.
- The operating principles of cluster-based Dr.Web Agents and anti-virus package are similar to those installed on a standard LAN server, therefore it is not recommended to install SpIDer Gate, SpIDer Mail and Dr.Web Firewall components on cluster nodes.
- If access to the quorum resource of a cluster is severely limited, it is recommended to exclude it from the SpIDer Guard scanning and to regularly scan the resource with Scanner either manually or by scheduling such scans.

5.2.1. Installation Files

Installation Packages

Personal Installation Package

After creating a new station account in the Control Center, a personal installation package for Dr.Web Agent installation is generated. It contains the Dr.Web Agent installer and a set of parameters to connect and authenticate the station to Dr.Web Server.

Personal installation packages are available for protected stations running any of the operating systems supported by Dr.Web Enterprise Security Suite. The installation packages are created in the Control Center based on the Dr.Web Agent installer. Parameters used to connect and authorize the station to Dr.Web Server are included in the personal installation package.

To obtain Dr.Web Agent installers for operating systems other than Windows, download the corresponding Dr.Web enterprise products from the GUS servers to the repository after installing Dr.Web Server.

Detailed information on using the Dr.Web Server repository can be found in the **Administrator Manual**, Administration of Dr.Web Server Repository.

Download link for Dr.Web Agent personal installation package for a specific station is available:

1. Immediately after creating a new station (see step **11** in section Creating a new station account).
2. At any time after creating a new station:
   - in the station properties,
   - in the **Selected objects** section, when selecting a station in the hierarchical list.

Group installation package

A group installation package of Dr.Web Agent is created in the Control Center for installation on stations of a specific user group. A single group installation package is intended for installation of Dr.Web Agent on all stations running the same OS.

The group installation package contains the Dr.Web Agent installer, a set of parameters for connection to Dr.Web Server, an identifier and password of a user group to which the station will be added, after Dr.Web Agent is installed. Please note that neither the parameters for station authorization on Dr.Web Server, nor the anti-virus components are included in the group installation package.

The download link for the group installation package is available in the user group properties.

Installers

The Dr.Web Agent installer differs from the installation package in that the former does not contain the parameters for connecting and authorizing the station on Dr.Web Server.

The following Dr.Web Agent installers are provided:

- For stations running Windows OS, two type of installers are available:
  - `drwinst.exe` *network installer* only installs Dr.Web Agent. After connecting to Dr.Web Server, it downloads Dr.Web Agent and installs necessary components of the anti-virus package. The network installer is capable of both local and remote installation of Dr.Web Agent.

    The `drwinst.exe` network installer is located in the `webmin/install/windows` folder (a hidden shared resource by default) within the Dr.Web Server installation folder. Network availability of this resource can be set in step 11 of Dr.Web Server installation. You can also change this resource in the future, as necessary.
  - `drweb-<agent_version>-<build>-esuite-agent-full-windows.exe` *full installer* installs both Dr.Web Agent and the anti-virus package.
- For stations running Android OS, Linux OS, or macOS, there are Dr.Web Agent installers available, similar to the standalone version installer.

Dr.Web Agent installers are available on the installation page of Dr.Web Security Control Center.

To obtain Dr.Web Agent installers for operating systems other than Windows, as well as the full installer for Windows, download the corresponding Dr.Web enterprise products from the GUS servers to the repository after installing Dr.Web Server.

Detailed information on using the Dr.Web Server repository can be found in the **Administrator Manual**, Administration of Dr.Web Server Repository.

Installation Page

Immediately after installing Dr.Web Server, you can download the following files from the Dr.Web Security Control Center installation page:

1. Dr.Web Agent for Windows installer.
2. Dr.Web Server certificate (`drwcsd-certificate.pem`).

After a quick setup, a number of additional installers will be available on the page. Installers for protected stations running any of the operating systems supported by Dr.Web Enterprise Security Suite are located in the appropriate folders.

The installation page can be accessed from any computer with network access to Dr.Web Server at:

http://<*Dr.Web_Server_address*>:<*port_number*>/install/

where <*Dr.Web_Server_address*> is the IP address or domain name of the computer where Dr.Web Server is installed. The <*port_number*> should be `9080` (or `9081` for https).

Configuring the list of products available on the installation page

1. Select **Administration** from the main menu and then **General repository configuration** from the control menu.
2. Go to the **Dr.Web installation packages** → **Dr.Web enterprise products** tab.
3. Press the arrow to the left of the required product name to specify the operating system and bitness. After checking the boxes next to all required products, click **Save**.
4. Update the repository from the **Repository state** section in the control menu.
5. Once the download from GUS and the repository update are complete, the installers for the selected products are available on the installation page:

5.2.2. Local Installation of Dr.Web Agent

Local installation of Dr.Web Agent is performed directly on the user's computer or mobile device. May be performed either by administrator of by user.

You must update the Dr.Web Server repository before the first installation of the Agent (see **Administrator Manual**, p. Manual Update of Dr.Web Server Repository, p. **Checking for Updates**).

Stations under Android OS, Linux OS, macOS

For local installation of Dr.Web Agent on stations under Android OS, Linux OS, macOS the following means are available:

- Personal installation package created in the Control Center.
- Group installation package created in the Control Center.
- Installer of Dr.Web Agent.

When you choose the type of installing package, please note the following features:

a) When the personal installation package is created, Dr.Web Agent installer is provided for installation, and parameters for connecting to Dr.Web Server and for authorization of the station at Dr.Web Server are provided in the configuration file.

b) When installing Dr.Web Agent via the installer, parameters for connecting to Dr.Web Server and for authorization of the station at Dr.Web Server are not provided.

Stations under Windows OS

For local installation of Dr.Web Agent on stations under Windows OS, the following means are available:

- Personal installation package created in the Control Center `drweb_es_<OS>_<station>.exe`.
- Group installation package created in the Control Center `drweb_es_<OS>_<group>.exe`.
- Full installer of Dr.Web Agent `drweb-<agent_version>-<build>-esuite-agent-full-windows.exe`.
- Network installer of Dr.Web Agent `drwinst.exe`.

When you choose the type of installing package, please note the following features:

a) For installation via the personal installation package, parameters for connecting to Dr.Web Server and for authorization of the station at Dr.Web Server are included into the personal installation package. Installation via the personal installation package is performed on base of the network installer from which Dr.Web Agent only is installed. After connecting to Dr.Web Server, Dr.Web Agent downloads and installs the anti-virus package components.

b) For installation via the group installation package, parameters for connecting to Dr.Web Server and also the identifier and the password of the user group into which the station will be included after the Dr.Web Agent installation, are included into the installation package. But parameters for the authorization of the station at Dr.Web Server and anti-virus components are not included into the group installation package composition. After Dr.Web

Agent is installed, Dr.Web Agent connects to Dr.Web Server, during that, it is determined whether free stations are available in the user group, the group installation package of which has been used. If free stations are available, parameters for the authorization of the station at Dr.Web Server are granted automatically.

c) Network installer performs the installation of Dr.Web Agent only. After connecting to Dr.Web Server, Dr.Web Agent downloads and installs necessary anti-virus package components. At this, parameters for connecting to Dr.Web Server and for authorization of the station at Dr.Web Server are not provided.

d) For installation via the full installer, Dr.Web Agent and anti-virus package are installed at a time. At this, parameters for connecting to Dr.Web Server and for authorization of the station at Dr.Web Server are not provided.

Comparative characteristics of installation files

Installation file		Dr.Web Agent installation	Anti-virus package installation	Dr.Web Server connection parameters	Dr.Web Server authorization parameters
Installation package	Personal	+	–	+	+
	Group	+	–	+	–
Installer	Network	+	–	–	–
	Full	+	+	–	–

To obtain installation packages and installers for operating systems other that Windows OS, as well as the full installer for Windows, download the corresponding Dr.Web enterprise products from the GUS servers to the repository after installing Dr.Web Server.

You can find the detailed information on how to handle the Dr.Web Server repository in the **Administrator Manual**, the Administration of Dr.Web Server Repository section.

You can also launch all types of the Dr.Web Agent installation files from the command line using the switches given in the **Appendices** document, p. G1. Network Installer.

5.2.2.1. Installing Dr.Web Agent via the Personal Installation Package

To install Dr.Web Agent on protected stations via the personal installation package

1. Via the Control Center, create an account for a new station on Dr.Web Server.

2. Send the link to the Dr.Web Agent personal installation package for the corresponding operating system of the computer or mobile device to the station user if the user is installing Dr.Web Agent software on their own.

   For easy delivering of installation and configuration files, you can use the **Mailing of installation files** function (detailed information is given in the **Administrator Manual**, p. Mailing of Installation Files) to email messages with corresponding files.

3. Install Dr.Web Agent on the workstation.

   Local installation of Dr.Web Agent on workstations is described in the **User Manual** for corresponding OS.

   Dr.Web Agent must be installed by a user with the administrator rights on the computer.

   If some anti-virus software is already installed on a workstation, then the personal installation package attempts to remove it before the installation starts. If the attempt fails, the user will have to uninstall the anti-virus software from the computer.

4. For stations under macOS, configure parameters of connection to Dr.Web Server locally.

   After installation of Dr.Web Agent on stations under other supported systems via the personal installation package, additional configuring is not required. Parameters of connection to Dr.Web Server and authorization parameters are included into a personal installation package directly. After the Dr.Web Agent installation is complete, the station automatically connects to Dr.Web Server.

Creation of a New Station Account

To create a station account or several station accounts, use Dr.Web Security Control Center.

When creating a station account, please note the name of Dr.Web Server specified in the following sections of the Control Center:

1. **Administrating** → **Web server configuration** → the **Dr.Web Server address** field. This parameter value is used when generating the link on the Dr.Web Agent installation package.

   If the parameter value is not specified, when the DNS name (if available) or IP address of a computer on which the Control Center is opened, is used as a Dr.Web Server name to generate the link on Dr.Web Agent personal installation package download.

2. **Administrating** → **Dr.Web Server configuration** → the **Network** tab → the **Download** tab → the **Dr.Web Server address** field. This parameter value is specified in the Dr.Web Agent installation packages and defines to which Dr.Web Server Dr.Web Agent connects during installation.

If the parameter value is not specified, when creating an installation package of Dr.Web Agent, the name of the Dr.Web Server to which the Control Center connected is used. In this case, the Control Center must be connected to Dr.Web Server using the IP-address of the domain for which you create an account (Dr.Web Server address must not be specified as a loopback—`127.0.0.1`).

To create a new station account via Dr.Web Security Control Center

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. In the toolbar, click **Add a network object** → **Create station** option. A pane for the new station account creation will be opened in the right part of the Control Center window.
3. In the **Number** entry field, specify the number of accounts to be created.
4. In the **Identifier** 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 Dr.Web Server, this name can be automatically changed to the station name which is specified locally.
6. In the **Password** and **Confirm Password** fields you can specify a password for accessing Dr.Web Server by a station. If the password is not specified, it will be generated automatically.

When creating more than one account, **Identifier**, **Name** and **Password** (**Confirm Password**) fields are set automatically and cannot be changed at the stage of station creation.

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.

- In the **Membership** list, you can configure the list of user groups to which the station will be added.

  By default, a newly created station is included in the **Everyone** group. If custom groups are available, you can include the newly created station in these groups without limiting the number of groups the station can be included in. To do this, click **Edit**, set the flags next to the user group names in the **Membership** list and click **Apply**.

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

  To set a primary group for the station you are creating, click the appropriate group icon in the **Membership** list. A number **1** icon overlay will appear on the group icon.

- In the **Policy** list, you can set a policy from which the created station will inherit its settings.

The list becomes available when the **Use policies** flag is set in the **Administration** → **Dr.Web Server configuration** section on the **General** tab.

By default, the policy is not set. To specify the policy, click , set the flag next to the necessary policy and click **Apply**. The station inherits its settings from the current version of this policy. A station cannot have more than one policy assigned to it.

- In the **Profile** list, you can set an Application Control profile which will be applied to the station being created.

  By default, the profile is inherited from the parent group of the station. To select a profile for the station, click **Edit** , set the flag next to the profile you need and click **Apply**. Multiple profiles can be applied to a station.

9. In the **Dr.Web Proxy Server** section, you can configure the settings of Dr.Web Proxy Server connected with this station.

If you want to install Dr.Web Proxy Server on the creating station, set the **Create linked Dr.Web Proxy Server** flag and specify the parameters of Dr.Web Proxy Server. The parameters are the same as when creating a Dr.Web Proxy Server.

When creating a station account, a Dr.Web Proxy Server account will be created in the Control Center. After the settings are transferred to the station, Dr.Web Proxy Server will be installed on this station in the background. Dr.Web Agent will connect to Dr.Web Server only through the installed Dr.Web Proxy Server. The Proxy Server usage will be transparent for the user.

10. Specify parameters of the **Security** section, if necessary. Parameters of this section are described in the **Administrator Manual**, in the Security section.
11. Specify parameters of the **Location** section, if necessary.
12. Click **Save** in the upper right corner. The opened pane contains information about successful creation of a station, its ID and the following links:

- The **Installation package** item contains the link for downloading the Dr.Web Agent personal installation package for this station.
- In the **Configuration file** item—the link for downloading the file with settings of connection to Dr.Web Server for stations under Android, macOS and Linux operating systems.

After a new station has been created, before the operating system of a station is set, in the section of distribution kit downloading, the links are presented separately for all OS that are supported by Dr.Web Enterprise Security Suite.

Link for the Dr.Web Agent personal installation package downloading is also available:

- in station properties after its creation,
- in the **Selected objects** section for the station selected in hierarchical list.

To obtain personal installation packages for operating systems other than Windows, download the corresponding Dr.Web enterprise products from the GUS servers to the repository after installing Dr.Web Server.

You can find the detailed information on how to handle the Dr.Web Server repository in the **Administrator Manual**, the Administration of Dr.Web Server Repository section.

- The **Password** item contains the password to access this station to Dr.Web Server. To view the password, click .
- The **Proxy Server password** item contains the password to access the Proxy Server to Dr.Web Server, if the station is created with the connected Proxy Server (see step 9).
- The **Install** button is intended for remote installation of Dr.Web Agent Software via Dr.Web Security Control Center.

13. Installation of Dr.Web Anti-virus on workstations is described in the **User Manual** for corresponding OS.

Configuring Parameters of Connection to Dr.Web Server for Stations under macOS

1. In Dr.Web Anti-virus application menu, click **Preferences** and select **Mode**.
2. Set the **Enable centralized protection mode** flag.
3. Parameters of connection to Dr.Web Server, such as IP address and authorization parameters at Dr.Web Server, are specified automatically from the `install.cfg` configuration file that resides in the personal installation package.

   To use this file:

   a) Click **Other activation types** in the License Manager.

   b) Drag the configuration file to the opened window or click the dotted area to select the file.

   If the file is mounted, fields for entering the connection settings will be specified automatically.

5.2.2.2. Installing Dr.Web Agent via the Group Installation Package

To install Dr.Web Agent on protected stations via the group installation package

1. Via the Control Center, create a new user group on Dr.Web Server (detailed description of groups creation is given in the **Administrator Manual**, p. Creating and Deleting Groups). Also, you can use the existing group you have created before.
2. If necessary, in the License Manager assign the personal license key for the group. Otherwise, the group inherits a license key from its parent group.

3. Via the Control Center, create accounts for new stations on Dr.Web Server. Add new station accounts to the user group from step 1 and make this group primary to them. You can create as many stations within the user group as many available licenses are available for this group.

   If the **Create station accounts automatically** flag is set in the **Administration** → **Dr.Web Server configuration** section of the Control Center, the new station accounts are added automatically. In this case you do not need to create the new accounts manually.

4. In the group properties, the link for the group installation package becomes available. Installation packages are divided by available operating systems: one installation package for each operating system.
5. Send the link to the Dr.Web Agent installation package for the corresponding operating system of the computer or mobile device to the station users if they are installing the Dr.Web Agent software on their own. The same group installation package for the corresponding operation system is sent to all users.
6. Install Dr.Web Agent on the workstations.

   Local installation of Dr.Web Agent on workstations is described in the **User Manual** for corresponding OS.

   Dr.Web 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.

7. After Dr.Web Agent is installed, Dr.Web Agent connects to the Dr.Web Server specified in the group installation package. At first connection to Dr.Web Server, it is determined whether free stations are available in the user group, the group installation package of which has been used for the Dr.Web Agent installation. The number of free stations is defined by the number of accounts in this group, which have not expired. At each connection of a group installation package, the number of free stations is recalculated to provide the actual information.
   a) If free stations are available, parameters for the authorization of the station at Dr.Web Server are granted automatically. This procedure does not require any additional administrator intervention.
   b) If free stations are not available in this group, the installation is terminated with corresponding notification of a user.

   If the **Create station accounts automatically** flag is set in the **Administration** → **Dr.Web Server configuration** section of the Control Center, the parameters used to authorize the

station on Dr.Web Server are granted automatically once Dr.Web Agent installed from the group installation package connects to Dr.Web Server.

5.2.2.3. Installing Dr.Web Agent via the Installer

The Dr.Web Agent installer, unlike the installation package, does not include parameters for connecting to Dr.Web Server and for authorization of the station at Dr.Web Server.

Dr.Web Agent installers are available on the installation page of Dr.Web Security Control Center.

To obtain installers for operating systems other that Windows OS, as well as the full installer for Windows, download the corresponding Dr.Web enterprise products from the GUS servers to the repository after installing Dr.Web Server.

You can find the detailed information on how to handle the Dr.Web Server repository in the **Administrator Manual**, the Administration of Dr.Web Server Repository section.

Local Installation on Stations under Android OS, Linux OS, macOS

Under Android OS, Linux OS, macOS, an installer for installing Dr.Web Agent is available, similar to the installer of the standalone version.

Local installation of Dr.Web Agent on workstations is described in the **User Manual** for a corresponding OS.

If you perform the installation via the installer without the configuration file, you must specify the Dr.Web Server address to connect on station manually.

You can either specify authorization parameters manually or leave them blank. At this, the following variants of connection to Dr.Web Server are available:

Setup option	Authorization parameters
Specified manually	Attempt of automatic authorization according to the specified parameters is performed.
Not specified	Authorization mode on Dr.Web Server depends on the Dr.Web Server settings for connecting new stations (for more details, see the **Administrator Manual**, p. New Stations Approval Policy).

To specify authorization parameters manually, you must create a new station account in the Control Center first. At this, the installation package become available, which contains configuration file with connection and authorization parameters. It is recommended to use installation package instead of the installer.

Local Installation on Stations under Windows OS

The following types of Dr.Web Agent installers are provided:

- `drwinst.exe` *Network installer* performs the installation of Dr.Web Agent only. After connecting to Dr.Web Server, the Dr.Web Agent downloads and installs necessary anti-virus package components.
- `drweb-<agent_version>-<build>-esuite-agent-full-windows.exe` *Full Installer* performs the installation of Dr.Web Agent and anti-virus package at a time.

If you use these installers, you can either specify parameters of authorization and connection to Dr.Web Server manually or leave them blank.

To specify authorization parameters manually, you must create a new station account in the Control Center first. At this, the installation package become available. If there is no need to install via the full distribution kit or via the network installer, it is recommended to use installation package instead of the installer.

The following variants of connection to Dr.Web Server are available:

Setup option	Dr.Web Server address	Authorization parameters
Specified manually	The station addresses to the specified Dr.Web Server directly.	Attempt of automatic authorization according to the specified parameters is performed.
Not specified	Dr.Web Agent searches for Dr.Web Server in the network based on the Dr.Web Server detection service. Attempt to connect to the first found Dr.Web Server is performed.	Authorization mode on Dr.Web Server depends on the Dr.Web Server settings for connecting new stations (for more details, see the **Administrator Manual**, p. New Stations Approval Policy).

The **User Manual** for Windows OS describes Dr.Web Agent installation via the full installer and via the installation package.

It is recommended to perform the installation via the network installer by the anti-virus network administrator.

Local Installation via the Network Installer under Windows OS

The `drwinst.exe` Agent network installer is provided to install Dr.Web Agent under Windows OS only.

If the network installer is run in the normal installation mode (i.e. without the `/instMode remove` 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*—runs if the background mode switch is specified.
2. *Graphical mode*—default mode. Runs if the background mode switch is not specified.

With the network installer, you can also install Dr.Web Agent on a workstation remotely via Dr.Web Security Control Center (see p. Remote Installation of Dr.Web Agent).

To install Dr.Web Agent on a workstation in the background mode

1. From the workstation, on which you want to install the anti-virus software, enter the network folder of the Dr.Web Agent installation (by default at the Dr.Web Server installation, it is the `webmin/install/windows` folder of the Dr.Web Server installation folder, further it can be changed) or download from the installation page of the Control Center the `drwinst.exe` executable file and `drwcsd-certificate.pem` certificate. Run the `drwinst.exe` file with the `/silent yes` background mode switch.

   By default, if the `drwinst.exe` file launched without the Dr.Web Server connection parameters, it will use the *Multicast* mode to scan the network for Dr.Web Servers and will try to install Dr.Web Agent from the first found Dr.Web Server.

   When you use the *Multicast* mode to find active Dr.Web Servers, the Dr.Web Agent installation is performed from the first found Dr.Web Server. At this, if the public encryption key does not match the Dr.Web Server encryption key, installation will be failed. In this case, directly specify the Dr.Web Server address (as described below).

   If you need to install Dr.Web Agent on the same computer on which Dr.Web Server is installed, you must directly specify the Dr.Web Server address in the installer launch parameters, because Dr.Web Server may not be found when searching via multicast request.

   The `drwinst.exe` file also may be used with the optional command line switches:

   - If the *Multicast* mode is not used, it is recommended that you specify Dr.Web Server name in the FQDN format directly (it must be registered on the DNS service):

```
drwinst /silent yes /server <Dr.Web_Server_DNS_name>
```

It is recommended that you use the name of Dr.Web Server in the FQDN format as the Dr.Web Server address, registered in the DNS service. This will simplify the process of setting up an anti-virus network when reinstalling Dr.Web Server on another computer. In this case, if Dr.Web Server address changed, it will be enough to update it in the DNS server settings for the name of the computer with installed Dr.Web Server, and all agents will automatically connect to the new server.

1. If there is a local DNS server in the network, create names for Dr.Web Server and Dr.Web Proxy Server (e.g. `drwebes.company.lan`).
2. Specify Dr.Web Server name in the FQDN format in the settings of Dr.Web agents.
3. It is recommended that you add the Dr.Web Server address in the Dr.Web Agent settings in addition to the name in the FQDN format and keep it up to date when it changes. In this case, if the server name cannot be used, the agent will attempt to connect using the server address.

It makes the configuration of the anti-virus network easier especially in case you reinstall Dr.Web Server on a different computer.

- You can explicitly specify the Dr.Web Server address as follows:

```
drwinst /silent yes /server 192.168.1.3
```

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

The complete list of Network Installer parameters is describe in the **Appendices** document, p. G1. Network Installer.

2. After the installation is completed, the software of Dr.Web Agent is installed on a computer (anti-virus package is not installed yet).
3. After the station has been approved at Dr.Web Server (if it is required by the Dr.Web Server settings), the anti-virus package will be automatically installed.
4. Restart the computer on Dr.Web Agent request.

To install Dr.Web Agent on a workstation in the graphical mode

From the workstation, on which you want to install the anti-virus software, enter the network folder of the Dr.Web Agent installation (by default at the Dr.Web Server installation, it is the `webmin/install/windows` folder of the Dr.Web Server installation folder, further it can be changed) or download from the installation page of the Control Center the `drwinst.exe` executable file and `drwcsd-certificate.pem` certificate. Run the `drwinst.exe` file.

A window of the Installation wizard of Dr.Web Agent will be opened. Further actions on the Dr.Web Agent installation on the stations via the graphical mode of the network installer are similar to the actions on the installation via the installation package, but without the Dr.Web Server connection settings, if they have not been specified in the corresponding command line switch.

Installation of Dr.Web Agent on workstations is described in the **Dr.Web Agent for Windows User Manual**.

5.2.3. Remote Installation of Dr.Web Agent

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

Remote installation is available:

- Via the Control Center.
- Via the Active Directory service, if the service is used in the LAN.

Remote installation of Dr.Web Agents is possible only on workstations running Linux OS and Windows OS (see chapter System Requirements) except Starter and Home editions.

To install the anti-virus software on workstations, you must have administrator rights on the correspondent workstations.

5.2.3.1. Installing Dr.Web Agent Software via Dr.Web Security Control Center

- Remote Installation of Dr.Web Agent on Windows OS
- Remote Installation of Dr.Web Agent on Unix-like OS

5.2.3.1.1. Remote Installation of Dr.Web Agent on Windows OS

The following means of remote Dr.Web 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 Dr.Web Agents on them.

2. Installation using the Network Installation tool.

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

3. Installation on stations with specified ID.

   Allows to install Dr.Web Agents for selected accounts (including all new accounts) with specified ID and password for the Dr.Web 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 Dr.Web Server must be added to the trusted sites of browser, on which you open Control Center for remote installation.

Using the Network Scanner

In Dr.Web Security Control Center, the anti-virus network hierarchical list displays only those computers which are already included into the anti-virus network. Dr.Web Enterprise Security Suite 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 Dr.Web Agent software on workstations, it is recommended to use Network Scanner (see **Administrator Manual**, p. Network Scanner) which searches for computers by IP addresses.

Network installation is available only to administrators with the **View groups of stations properties** permission granted for the entire anti-virus network (for more on administrator permissions, see the **Administrator Manual**, Administrators Permissions).

To install Dr.Web Agent via the Network Scanner

1. Open the Network Scanner. To do this, on the **Administration** menu of Dr.Web Security Control Center, select **Network scanner**. A **Network scanner** window with no data loaded will be opened.
2. Set the parameters to search for stations in the network. Detailed description of the parameters is given in the **Administrator Manual**, the Network Scanner section.
3. Click **Start Scanner**. The catalog (hierarchical list) of computers demonstrating where Dr.Web Enterprise Security Suite 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 5-1. Icons of the Network scanner

Icon	Description
Workgroups	
	The work groups containing inter alia computers on which Dr.Web Enterprise Security Suite anti-virus software can be installed.
	Other groups containing protected or unavailable by network computers.

Icon	Description
Workstations	
	Active station with installed anti-virus software.
	Active station with unknown state of anti-virus software (there is no anti-virus software on a station or it was not detected).

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

5. In the **Network scanner** window, select an unprotected computer (or several unprotected computers by pressing CTRL or SHIFT buttons).
6. On the toolbar, click  **Install Dr.Web Agent**.
7. The **Network Installation** window will be opened to configure the Dr.Web Agent remote installation task.
8. In the **Addresses of stations** field, specify IP addresses or DNS names of computers on which Dr.Web Agent will be installed. If you set several stations, use ";" or "," as a separator (number of spaces around a separator is irrelevant).

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

   Addresses should be specified in the network addresses format described in the **Appendices** document, p. Appendix D. The Specification of Network Addresses.

9. By default the **Dr.Web Server** field displays IP address or DNS name of Dr.Web Server to which Dr.Web Security Control Center is connected. If necessary, specify the Dr.Web Server address from which the anti-virus software will be installed. If you set several Dr.Web Servers, use ";" or "," as a separator (number of spaces around a separator is irrelevant). Leave this field blank to use Dr.Web Server detecting service (*Multicast* mode).

   Remote installation of Dr.Web Agent is not available on the computer with Dr.Web Server installed, from which the installation is launched.

   Addresses should be specified in the network addresses format described in the **Appendices** document, p. Appendix D. The Specification of Network Addresses.

   It is recommended that you use the name of Dr.Web Server in the FQDN format as the Dr.Web Server address.

10. In the **Simultaneous installations** field, specify the maximum number of stations to perform parallel installation.
11. Set the **Install Dr.Web Agent for Windows software** flag to continue with the settings specific to remote installation on Windows OS.

12. By default the Dr.Web Agent software is installed to the `%ProgramFiles%\DrWeb` folder. If necessary, specify another location in the **Dr.Web Agent Installation folder** field.

    It is recommended to specify the full path for unique identification of installation folder location. It is allowed to use environment variables in the path.

13. In the **Language** drop-down list, select the language of interface for Dr.Web Anti-virus which will be installed on stations.

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

    When working with a large amount of data, the duration of installation may exceed the session time. If the session expires before the installation is complete, the process will be terminated automatically and Dr.Web Agent will not be installed.

15. If necessary, set the **Register Dr.Web Agent in the system list of installed software** flag.

16. In the **Installable components** section, select the components of anti-virus package which will be installed on stations.

17. In the **Compression** and **Encryption** sections, specify the parameters of traffic compression and encryption used by the Network Installer during installation of Dr.Web Agent and anti-virus package. These settings also will be used by Dr.Web Agent for interaction with Dr.Web Server after the installation.

18. In the **Authorization on remote stations** section, specify the parameters of authorization to access the remote computers on which Dr.Web Agent will be installed:

    - **User**—user name for authorization on stations where remote installation will be performed. For domain users, domain name must be specified in the following format: <domain>\<user> or <user>@<domain>. For local users, station name or workgroup name must be specified in the following format: <station>\<user> or <group>\<user>.
    - **Password**—user password on remote computer.

    You can set several administrator accounts. To add one more account, click  and specify authorization parameters fields. Similarly, for each new record.

    During Dr.Web 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. In the **Restart options** section, set the **Restart the station** flag and set the reboot time or period in the drop-down list (including the **Immediately after installation** option).

    - **Immediately after installation**—the station will be restarted after Dr.Web Agent is installed.
    - **At a specified hour**—according to the time of the system in which the administrator launched the browser and set the parameters.
    - **Within a specified period**—according to local station time.

20. After you specify all necessary parameters, click **Install**.

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

The installation uses the network installer of the current Dr.Web Server that is located in the `webmin\install\windows` folder of the Dr.Web Server installation folder and SSL certificate `drwcsd-certificate.pem` located in the `etc` folder of the Dr.Web Server installation folder.

If there are no remote installation packages of Dr.Web Agent in the Dr.Web Server repository, contact Doctor Web technical support: https://support.drweb.com/.

21. Dr.Web Agent will be installed on selected workstations. After a workstation is approved at Dr.Web Server (if required by Dr.Web Server settings, see also **Administrator Manual** New Stations Approval Policy), the anti-virus package will be automatically installed.
22. Restart the remote computers if Dr.Web Agent requests.

Using the Network Installation Tool

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

Network installation is available only to administrators with the **View groups of stations properties** permission granted for the entire anti-virus network (for more on administrator permissions, see the **Administrator Manual**, Administrators Permissions).

To install Dr.Web Agent via network

1. Select the **Administration** item in the main menu. Then select the **Network installation** item in the control menu.
2. Further steps are similar to **8–22** above.

Installation for Accounts with Specified ID

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 Agent** pane opens. Click **OK**.
3. The Network Scanner window opens.
4. Further steps are similar to **2–22** above.
5. After installation is complete, check if icons of corresponding stations are changed in the hierarchical list.

When using existing station account:

1. In the hierarchical list of anti-virus network, select a new station or group of stations, for which Dr.Web Agents are not installed, or the **New** group (for installation on all new accounts).
2. Click **Install Dr.Web Agent** on the toolbar.
3. The Network Scanner window opens.
4. Further steps are similar to **2–22** above.
5. After installation is complete, check if icons of corresponding stations are changed in the hierarchical list.

Dr.Web Agent installation on stations with selected ID is also available of group administrators.

See the **Appendices** document, the Remote Installation Troubleshooting section, if an error has occurred.

Additional settings

- If the workstations are inside a domain and the domain administrative account is used for the installation, you must turn on file and printer sharing on workstations. See the table for the location of this option for different Windows OS versions.
- If the remote stations are outside a domain, or if the local account is used during the installation, then for some of Windows OS, the extra configuration of the remote stations 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 Dr.Web Agent manually.

After you configure remote workstation, it is recommended to return all changed settings to the values set before editing to not violate the basic policy of operating system security.

To install Dr.Web 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 Dr.Web Agent:

OS	Configuration	
Windows XP	Setup the mode of access to shared files	Modern view: **Start** → **Settings** → **Control Panel** → **Appearance and Themes** → **Folder Properties** → the **View** tab → clear the **Use Simple Sharing (recommended)** flag.
		Classical view: **Start** → **Settings** → **Control Panel** → **Folder Properties** → the **View** tab → clear the **Use Simple Sharing (recommended)** flag.
	Set the mode of network authentication model in the local policies	Modern view: **Start** → **Settings** → **Control Panel** → **Performance and Maintenance** → **Administrative Tools** → **Local Security Policy** → **Security Settings** → **Local Policies** → **Security Options** → **Network Access: Sharing and security model** → **Classic - local users authenticate as themselves**.
		Classical view: **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Local Security Policy** → **Security Settings** → **Local Policies** → **Security Settings** → **Network Access: Sharing and security model** → **Classic - local users authenticate as themselves**.
	Disable the Windows Firewall on the station before remote installation.	
Windows Server 2003	Disable the Windows Firewall on the station before remote installation.	
Windows Vista Windows Server 2008	Enable the File sharing option	Modern view: **Start** → **Settings** → **Control Panel** → **Network and Internet** → **Network and Sharing Center** → **Sharing and discovery** → **File Sharing** → **Enable**.
		Classical view: **Start** → **Settings** → **Control Panel** → **Network and Sharing Center** → **Sharing and discovery** → **File Sharing** → **Enable**.
	Set the mode of network authentication model in the local policies	Modern view: **Start** → **Settings** → **Control Panel** → **System and Maintenance** → **Administrative Tools** → **Local Security Policy** → **Security Settings** → **Local Policies** → **Security Options** → **Network Access: Sharing**

OS	Configuration	
		and security model → Classic - local users authenticate as themselves.
		Classical view: **Start → Control Panel → Administrative Tools → Local Security Policy → Security Settings → Local Policies → Security Settings → Network Access: Sharing and security model → Classic - local users authenticate as themselves**.
	Add the **LocalAccountTokenFilterPolicy** key: a) In the registry editor, open the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System** branch. If the **LocalAccountTokenFilterPolicy** record does not exist, in the **Edit** menu, select **Add** and specify the **DWORD** value. Enter the **LocalAccountTokenFilterPolicy** value and press ENTER. b) In the **LocalAccountTokenFilterPolicy** item context menu, select **Change**. c) In the **Value** field, set the **1** value and click **OK**. Reboot is not required.	
Windows 7 Windows Server 2008 R2	Turn on file and printer sharing	Modern view: **Start → Control Panel → Network and Internet → Network and Sharing Center → Change advanced sharing settings → File and Printer Sharing → Turn on file and printer sharing**.
		Classical view: **Start → Control Panel → Network and Sharing Center → Change advanced sharing settings → File and Printer Sharing → Turn on file and printer sharing**.
	Set the mode of network authentication model in the local policies	Modern view: **Start → Control Panel → System and Security → Administrative Tools → Local Security Policy → Security Settings → Local Policies → Security Options → Network Access: Sharing and security model → Classic - local users authenticate as themselves**.
		Classical view: **Start → Control Panel → Administrative Tools → Local Security Policy → Security Settings → Local Policies → Security Settings → Network Access: Sharing and security model → Classic - local users authenticate as themselves**.
	Add the **LocalAccountTokenFilterPolicy** key: a) In the registry editor, open the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies**	

<table>
<tr><th>OS</th><th colspan="2">Configuration</th></tr>
<tr><td></td><td colspan="2">\System branch. If the LocalAccountTokenFilterPolicy record does not exist, in the Edit menu, select Add and specify the DWORD value. Enter the LocalAccountTokenFilterPolicy value and press ENTER.
b) In the LocalAccountTokenFilterPolicy item context menu, select Change.
c) In the Value field, set the 1 value and click OK.
Reboot is not required.</td></tr>
<tr><td rowspan="4">Windows 8

Windows 8.1

Windows Server 2012

Windows Server 2012 R2

Windows 10</td><td rowspan="2">Turn on file and printer sharing</td><td>Modern view:

Settings → Control Panel → Network and Internet → Network and Sharing Center → Change advanced sharing settings → File and Printer Sharing → Turn on file and printer sharing.</td></tr>
<tr><td>Classical view:

Settings → Control Panel → Network and Sharing Center → Change advanced sharing settings → File and Printer Sharing → Turn on file and printer sharing.</td></tr>
<tr><td rowspan="2">Set the mode of network authentication model in the local policies</td><td>Modern view:

Settings → Control Panel → System and Security → Administrative Tools → Local Security Policy → Security Settings → Local Policies → Security Options → Network Access: Sharing and security model → Classic - local users authenticate as themselves.</td></tr>
<tr><td>Classical view:

Settings → 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.</td></tr>
<tr><td colspan="2">Add the LocalAccountTokenFilterPolicy key:
a) In the registry editor, open the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System branch. If the LocalAccountTokenFilterPolicy record does not exist, in the Edit menu, select Add and specify the DWORD value. Enter the LocalAccountTokenFilterPolicy value and press ENTER.
b) In the LocalAccountTokenFilterPolicy item context menu, select Change.
c) In the Value field, set the 1 value and click OK.
Reboot is not required.</td></tr>
</table>

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.

5.2.3.1.2. Remote Installation of Dr.Web Agent on Unix-like OSs

Before installation:

1. Configure SSH access from the Dr.Web Server host computer to the computer on which Dr.Web Agent will be installed (remote installation is performed via SSH).
2. Mark Dr.Web Agent packages for download to the Dr.Web Server repository in the **General repository configuration** section of the Control Center. To do that, select the **Administration** item in the main menu, then **General repository configuration** in the control menu. In the **Dr.Web installation packages** section, select the **Dr.Web enterprise products** tab, then **Dr.Web Desktop Security Suite (Linux)** and/or, if necessary, **Dr.Web Server Security Suite (Unix)**. Select the OS and platform.

   Download only the packages you need and use. Downloading all the packages will take up more time and additional disk space.

3. Download the Dr.Web Agent packages to the repository. They are downloaded twice an hour in accordance with the Dr.Web Server Task Scheduler. You can also force a repository update. To do that, select the **Administration** item in the main menu, then **Repository state** in the control menu, then select **Check for updates**.

   To check if the Dr.Web Agent packages are downloaded, select the **Administration** item in the main menu, then **Enterprise products** in the control menu.

After that you can start the installation.

Use the **Network installation** tool from Dr.Web Security Control Center to remotely install the Dr.Web Agent software on computers running a Unix-like OS.

During the installation of Dr.Web Agent, a folder with the distribution package and the installation log is created on the station. The path to this folder is specified in the web interface when the installation is started (**Administration → Network installation**, the **Temporary directory** parameter).

If you encounter problems using the default value for the temporary files folder, check the mounting options for this folder in the OS file system and use a different folder where programs are allowed to run.

To install Dr.Web Agent via network

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

2. In the **Addresses of stations** field, specify IP addresses or DNS names of computers Dr.Web Agent will be installed to. When specifying several stations at a time, use ";" or "," as a separator (number of spaces around a separator is irrelevant).

   Addresses should be specified in the network address format described in the **Appendices** document, p. Appendix D. The Specification of Network Addresses.

3. By default, the **Dr.Web Server** field displays IP address or DNS name of Dr.Web Server to which Dr.Web Security Control Center is connected. If necessary, specify the Dr.Web Server address from which the anti-virus software will be installed. When specifying several Dr.Web Servers at a time, use ";" or "," as a separator (number of spaces around a separator is irrelevant). Leave this field blank to use Dr.Web Server detecting service (*Multicast* mode).

   Dr.Web Agent cannot be remotely installed on a computer with Dr.Web Server installed, where the installation is initiated from.

   Addresses should be specified in the network address format described in the **Appendices** document, p. Appendix D. The Specification of Network Addresses.

   It is recommended that you use the name of Dr.Web Server in the FQDN format as the Dr.Web Server address.

4. In the **Simultaneous installations** field, specify the maximum number of stations the remote installation is allowed to be performed on.
5. Set the **Install Dr.Web Agent for UNIX software** flag to continue with the settings specific to remote installation on a Unix-like OS.
6. In the **Connection and authentication time-out (sec.)** field, specify the maximum wait time (in seconds) to establish connection and authenticate with remote stations.
7. In the **Installation package transfer time-out (sec.)** field, specify the maximum wait time (in seconds) to complete installation package transferring from Dr.Web Server.
8. In the **Package installation time-out (sec.)** field, specify the maximum wait time (in seconds) to complete package installation.

   When working with a large amount of data, the duration of installation may exceed the session time. If the session expires before the installation is complete, the process will be terminated automatically, and the packages will not be installed.

9. If you need to install the **Dr.Web Server Security Suite (Unix)** product instead of **Dr.Web Desktop Security Suite (Linux)**, select the corresponding item in the **Installation packages** section.
10. In the **Connecting to the remote stations via SSH using password** section, specify authorization parameters to access remote computers Dr.Web Agent will be installed to:
    - **User**—user name for authorization on stations where remote installation will be performed. For domain users, a domain name must be specified in the following format:

<domain>\<user> or *<user>@<domain>*. For local users, a station name or a workgroup name must be specified in the following format: *<station>\<user>* or *<group>\<user>*.

- **Password**—user password on a remote computer.

You can specify several accounts for authorization. To add one more account, click and specify authorization parameters.

During the Dr.Web Agent installation, the listed accounts will be used in order. If installation under any account is failed, the next account in the list is used and so on.

11. In the **Connecting to the remote stations via SSH using the SSH key pair** field, you can specify parameters of alternative way of authorization on remote computers using encryption keys:
    - **User**—user name for authorization on stations where remote installation will be performed. For domain users, a domain name must be specified in the following format: *<domain>\<user>* or *<user>@<domain>*. For local users, a station name or a workgroup name must be specified in the following format: *<station>\<user>* or *<group>\<user>*.
    - **Public SSH key**—path to the public SSH key file.
    - **Private SSH key**—path to the private SSH key file.
    - **Private SSH key password**—private SSH key password (optional).

Just as in the **Connecting to the remote stations via SSH using password** section, it is possible to specify several accounts at a time. For that, click and fill in the corresponding fields.

> If authorization parameters are filled in both **Connecting to the remote stations via SSH using password** and **Connecting to the remote stations via SSH using the SSH key pair** sections, the first ones to be used for the Dr.Web Agent installation will be the parameters of authorization via encryption keys.

12. The **Root privileges** section contains settings required to elevate user privileges on a remote computer up to a level required to install Dr.Web Agent.
    - Set the **Use sudo** or **Use su** flag to elevate privileges up to *root* user level for the time of the Dr.Web Agent installation.
    - In the **Password input time-out (sec.)** field, specify the maximum wait time (in seconds) for password input to allow using the *su* or *sudo* command.
    - In the **su/sudo password** field, enter the password to use when using the *su* or *sudo* command. By clicking , you can specify multiple passwords to cycle through. If you keep this field empty while the user password in the **Connecting to the remote stations via SSH using password** section is specified, the latter one will be tried to use with the command.
13. In the **Port** field of the **Connection settings** section, specify the SSH port number to use on computers for remote installation of Dr,Web Agent. By clicking the you can list multiple ports to use.
14. After you specify all necessary parameters, click **Install**.

15. Dr.Web Agent will be installed on selected workstations. After a workstation is approved at Dr.Web Server (if required by Dr.Web Server settings, see also **Administrator Manual** New Stations Approval Policy), the anti-virus package will be automatically installed.
16. Restart the remote computers if Dr.Web Agent requests.

5.2.3.2. Installing Dr.Web Agent Software via Active Directory

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

The Dr.Web Agent installation via Active Directory service is also available when using Distributed File System (see the **Appendices** document, p. Using DFS when Installing Dr.Web Agent via Active Directory section).

Dr.Web Agent Installation

To install Dr.Web Agent using the Active Directory

1. Download the Dr.Web Agent installer for networks with **Active Directory** from the installation page.

To have the Dr.Web Agent installer for Active Directory available for download from the installation page, first download it to the repository following the instructions from the **Installation page** subsection.

2. Install Dr.Web 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 Dr.Web Server, you do not have to upgrade Dr.Web Agent installer for networks with Active Directory. After upgrading the Dr.Web Server software, Dr.Web Agents and the anti-virus software will be upgraded on 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 Dr.Web Agent through Active Directory usually has the following format:

`drweb-<package_version>-<build>-esuite-agent-activedirectory.msi`

Parameters:

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

- `ESSERVERADDRESS=<DNS_name>`—set the address of Dr.Web Server to which Dr.Web Agent is to be connected. For the possible formats see the **Appendices** document, p. Appendix D. The Specification of Network Addresses.
- `ESSERVERPATH=<full_filename>`—specify the full path to the certificate of Dr.Web Server and the file name (by default `drwcsd-certificate.pem` in the `webmin/install` subfolder of the Dr.Web Server installation folder).
- `TARGETDIR`—the network folder for the Dr.Web 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, in the destination directory for Dr.Web Agent image (see the `TARGETDIR` parameter), you should not place installation files manually. The Dr.Web Agent Installer for networks with Active Directory (`<package_name>.msi`) and other files required for installation of Dr.Web Agents on workstations, will be placed into the destination folder automatically during administrative installation. If these files are present in the destination folder before the administration installation, e.g., from the previous installations, when the similar files will be rewritten.

If you need to perform administrative installation from different Dr.Web Servers, it is recommended that you specify different destination folders for each Dr.Web Server.

After deployment the administrative package, in the `<destination_directory>\Program Files\DrWeb` directory, only the `README.txt` file must resides.

Examples:

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

```
msiexec /a ESS_Agent.msi /qn ESSERVERADDRESS=192.168.14.1 ESSERVERPATH="C:
\Program Files\DrWeb Server\webmin\install\drwcsd-certificate.pem"
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 Dr.Web Agent image does not contain Dr.Web Agent Installer for networks with **Active Directory** (<*package_name*>.msi).

After deployment the administrative package, in the <*destination_directory*>\Program Files\DrWeb directory, only the README.txt file must reside.

1. Run the command

```
msiexec /a <path_to_installer>\<package_name>.msi
```

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

The Dr. Web Agent Installer uses the language specified in the language settings of a computer.

3. In the next window, specify the DNS name (preferred form) or the IP address of Dr.Web Server (see the **Appendices** document, p. Appendix D. The Specification of Network Addresses). Specify the location of the public key file of Dr.Web Server (drwcsd.pub). Click **Next**.
4. In the next window type the name of a network folder, to which the image of Dr.Web Agent is planned to be written. The path should be specified in the network addresses format even if the folder is a locally accessible resource; the folder 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 2003/2008/2012/2012R2 Server OS, in the **Start** → **Programs** menu for the Windows 2000 Server OS), select **Administrative Tools** → **Active Directory Users and Computers** (when you install Dr.Web Agent in the graphic mode, this window displays automatically).
2. In the domain containing the computers on which Dr.Web 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 Dr.Web 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 2008/2012/2012R2 Server OS: on the created **ESS** 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 at 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 2008/2012/2012R2 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 Dr.Web Agent installation package. To do this, specify the address of the network shared (resource which contains the Dr.Web Agent image you created during the administrative installation). The path should be specified in the network addresses format even if the folder is a locally accessible resource.
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 Dr.Web 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. Dr.Web Agent will be installed on selected computers at their next registration in the domain.

Policies Assignment in Consideration of Previous Dr.Web Agent Installations

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

1. **Dr.Web Agent is not installed on the station**.

   After policies assignment, Dr.Web Agent will be installed by general rules.

2. **Dr.Web Agent is already installed on the station without using the Active Directory service**.

   After Active Directory policy assignment, installed Dr.Web Agent will remain on the station.

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

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

3. **Dr.Web Agent is already installed on the station via the Active Directory**.

   Repeated assignment of a policy to a stations with Dr.Web Agent installed via the Active Directory service is not performed.

   Thus, policies assignment will not take any affect to the anti-virus software state on the station.

5.3. Installing Dr.Web Scanning Server

Dr.Web Scanning server can be installed only on Linux-based OSs and FreeBSD.

A Scanning server and the virtual machines it serves with Dr.Web Agent installed must be located within the same hypervisor.

1. Download the Dr.Web Scanning server installation package from the installation page on the station that you plan to appoint the Scanning server.
2. Download the certificate that will be used by the Scanning server for connecting to the Dr.Web Server. To do this, in the **Administration** section of the Control Center Menu select the item **Encryption keys**. Set the check box near the **Certificate** and press **Export**. Upload the certificate to the station that you plan to appoint the Scanning server.

   It is also possible to download the certificate from the installation page. It is located in the same directory as the Scanning server installation package.

3. Go to the directory where the installation package file has been downloaded and allow executing it:

```
# chmod +x <filename>.run
```

4. Launch the installation procedure:

```
# ./<filename>.run
```

5. Accept the conditions of the License Agreement.
6. After the installation connect to the Dr.Web Server the station that you plan to appoint the Scanning server by executing the following command:

```
# drweb-ctl esconnect <Dr.Web_Server_address> --Certificate
<path_to_the_certificate_file>
```

After executing this command, the connection should be approved automatically or by the anti-virus network administrator, depending on the settings of Dr.Web Server.

You can also connect to Dr.Web Server in a different way: create the account of the station that you plan to appoint the Scanning server; once the account is created, you will get the login (the station ID) and the password for connection. Perform the following command to connect:

```
# drweb-ctl esconnect <Dr.Web_Server_address> --login <station_ID> --password
<password> --Certificate <path_to_the_certificate_file>
```

It is recommended that you use the name of Dr.Web Server in the FQDN format as the Dr.Web Server address.

7. If the connection is successful, the station will be marked in the anti-virus network tree by the sign indicating that the Scanning server is active and ready for operation.

It is not required to install Dr.Web Agent on the station performing the functions of the Scanning server.

8. Make sure that the Scanning server is listening to ports 7090 and 18008 by executing the following command:

```
# netstat -l
```

The output must contain the following lines:

```
tcp 0 0 0.0.0.0:7090 0.0.0.0:* LISTEN

udp 0 0 0.0.0.0:18008 0.0.0.0:*
```

For detailed information on configuring the Scanning server and connecting stations to it refer to Dr.Web Enterprise Security Suite **Administrator Manual**, Chapter Connecting Stations to the Scanning Server.

5.4. Installing NAP Validator

Dr.Web NAP Validator checks the status of anti-virus software on protected workstations.

It is installed on the computer where a configured NAP server is deployed.

Installing NAP Validator

1. Run the installation file. In the dialog window, select the language you want to use during installation. 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**.
4. In the window that opens, specify the Dr.Web Server IP address and port in the **Address** and **Port** fields, and click **Next**.
5. Click **Install**. No further user input is required.
6. When installation is completed, click **Finish**.

After installing Dr.Web NAP Validator, you should add Dr.Web Server to the group of trusted NAP servers. To do this:

1. Open the NAP server configuration component (run `nps.msc`).
2. In the **Remediation Servers Group** section, click **Add**.
3. In the dialog window, enter the name of the new remediation server and the IP address of Dr.Web Server.
4. Click **OK** to save changes.

5.5. Installing Dr.Web Proxy Server

One or more Proxy Servers can be included in the anti-virus network.

When selecting the computer on which to install Dr.Web Proxy Server, remember that Dr.Web Proxy Server should be accessible from all networks and segments that require data redirection between them.

Dr.Web Proxy Server cannot be installed on the same station with Dr.Web Server.

Dr.Web Proxy Server can be installed on Windows OS as follows:

- Automatically during the installation of Dr.Web Agent for Windows

  The installation is performed using a personal Dr.Web Agent installation package, which is created with the settings for the installation of the linked Dr.Web Proxy Server. In this case, Dr.Web Proxy Server is installed automatically in the background.
- Automatically on a station where Dr.Web Agent for Windows is installed

  Configure the linked Dr.Web Proxy Server installation for the selected station in the Control center. Dr.Web Proxy Server will be automatically installed on the station in the background.
- Manually using graphical installer

  The installation is performed manually by the administrator on any suitable network station. No other components of the anti-virus network can be installed on this station.

You can install Dr.Web Proxy Server on Unix-like OS only manually using the installer.

5.5.1. Creating Dr.Web Proxy Server Account

The administrator must create Dr.Web Proxy Server accounts on each Dr.Web Server to which the Dr.Web Proxy Server will connect (and forward the traffic).

Creating Dr.Web Proxy Server account using Dr.Web Security Control Center

1. For the parent group where Dr.Web Proxy Server will be created, specify the settings as described in the **Administrator Manual**, section Remote configuration of proxy server. In this case, the specified settings will be inherited by Dr.Web Proxy Server upon connection. You can specify these settings after Dr.Web Proxy Server account is created (both for the parent group in the case of inheritance, and individually for Dr.Web Proxy Server itself), but before Dr.Web Proxy Server connects to the account being created.

   If the settings are not specified before connecting Dr.Web Proxy Server, the configuration file will not be downloaded. Dr.Web Proxy Server uses the current configuration until the configuration is set on the connected Dr.Web Server, if Dr.Web Server is allowed to manage the configuration.
2. Select **Anti-virus network** from the main menu of the Control Center.
3. The actions required to set up Dr.Web Proxy Server depend on whether you want to install Dr.Web Proxy Server on an existing station with Dr.Web Agent or separately:

№	Actions	Install together with Dr.Web Agent	Install separately
a)	1. In the anti-virus network tree, select a station to install the linked Dr.Web Proxy Server. 2. On the properties pane of the selected station, go to the **Proxy Server** section.	+	–
b)	1. In the anti-virus network tree, select a station to install the linked Dr.Web Proxy Server. 2. On the toolbar, select **Add a network object** → **Create Proxy Server**.	+	+
c)	1. Make sure, no station is selected in the anti-virus network tree. 2. On the toolbar, select **Add a network object** → **Create Proxy Server**.	+	+

If you create Dr.Web Proxy Server account for installation on a station with Dr.Web Agent, Dr.Web Proxy Server installation will be performed automatically by Dr.Web Agent in the background mode after Dr.Web Proxy Server account is created (see also Installing Dr.Web Proxy Server as Part of Dr.Web Agent for Windows Installation).

If you create Dr.Web Proxy Server account for separate installation (without connection to Dr.Web Agent), Dr.Web Proxy Server should be installed manually by the administrator from the installation package included in the Dr.Web Server distribution kit.

4. In the **Identifier** field, a unique identifier of the created account is generated automatically. You can edit it if necessary.
5. In the **Name** field, specify the name of Dr.Web Proxy Server that will be displayed in the anti-virus network tree.

The name specified during the setup is automatically replaced with the computer name after Dr.Web Proxy Server is connected to Dr.Web Server.

6. In the **Password** and **Confirm Password** fields, you can specify a password for the Proxy Server to access Dr.Web Server. If the password is not specified, it will be generated automatically.

The identifier and password used to set up Dr.Web Proxy Server are the same for all Dr.Web Servers. You must create Dr.Web Proxy Server accounts with the same credentials on all Dr.Web Servers to which Dr.Web Proxy Server connects (see Connecting Dr.Web Proxy Server to Dr.Web Server).

You will not be able to edit the identifier after Dr.Web Proxy Server account is created.

7. In steps 3.b) and 3.c), the **Station** field specifies the existing station with the Dr.Web Agent installed to connect to this Dr.Web Proxy Server.

   In step 3.b), the **Station** field is automatically filled with the identifier of the selected station.

   In step 3.c), the **Station** field is empty.

   - To specify a station where Dr.Web Proxy Server will be installed, click  and in the window that opens, select the existing station from the anti-virus network tree.
   - Leave the **Station** field blank to not link Dr.Web Proxy Server to any station and connect the manually installed Dr.Web Proxy Server. If the **Station** field is already filled, click  to remove the connected station.
8. In the **Membership** section, you can specify a group to which the created Dr.Web Proxy Server should belong. To change the group, set the flag next to the required group in the displayed list.

   The Proxy Server can be included in one group only.

   You can select the pre-configured **Proxies** group and its subgroups.
9. Click **Save**.

   A windows will appear informing you that Dr.Web Proxy Server has been successfully created. It also contains the password to connect to Dr.Web Server. To view the password, click  .

To connect Dr.Web Proxy Server to Dr.Web Server, the Administrator will need the identifier and password of Dr.Web Proxy Server account created in the Control Center:

- When installing the proxy server using graphical installer.
- Manually after the Proxy Server installation (only for Unix-like OS).

5.5.2. Installing Dr.Web Proxy Server as a Part of Dr.Web Agent for Windows Installation

Installing Dr.Web Proxy Server as part of Dr.Web Agent for Windows installation

1. Specify Dr.Web Proxy Server settings as described in the **Administrator Manual**, section Remote configuration of Dr.Web Proxy Server. The settings must be specified for the group in which you plan to create Dr.Web Proxy Server. In this case, the specified settings will be inherited by Dr.Web Proxy Server when it is created. You can also specify these settings after Dr.Web Proxy Server is created (either for a group in which case the settings will be inherited, or individually for Dr.Web Proxy Server), but before Dr.Web Proxy Server is linked to the account being created.

If the settings are not configured before Dr.Web Proxy Server is linked to its account, Dr.Web Proxy Server uses the settings provided by the installer. With these settings Dr.Web Proxy Server can connect only to the Dr.Web Server from which it was installed.

2. Create a station account via the Control Center as described in the Installing Dr.Web Agent via the Personal Installation Package section. When creating the station, set the **Create linked Dr.Web Proxy Server** flag and configure the available settings. In particular, specify the group with the settings from step 1 where you want to place Dr.Web Proxy Server.

   You can change Dr.Web Proxy Server name and identifier only when creating its account.

3. Launch the Dr.Web Agent installation on the station using the personal installation package created in step 2.
4. After the installation, Dr.Web Agent will automatically download Dr.Web Proxy Server installer from Dr.Web Server and start it on the same station in the background. The Dr.Web Server certificate, address, and credentials for connection to Dr.Web Server are automatically written to the corresponding Dr.Web Proxy Server configuration files. Dr.Web Proxy Server settings for traffic forwarding will contain only the Dr.Web Server from which the installation was performed.
5. After installation, Dr.Web Proxy Server connects to the Dr.Web Server from which the installation was performed, to download the complete configuration file. If the Dr.Web Server settings were not specified in step 1, the configuration file will not be downloaded. The configuration specified by the installer will be used until the connected Dr.Web Server is configured.
6. Dr.Web Agent connects to Dr.Web Server only through the installed Dr.Web Proxy Server. Dr.Web Proxy Server usage will be transparent for the user.

5.5.3. Installing Dr.Web Proxy Server Using Installer

You must have administrative rights on the computer to install Dr.Web Proxy Server.

Installing Dr.Web Proxy Server in Windows OS

1. Create a Dr.Web Proxy Server account from the Control Center as described in the Creating Dr.Web Proxy Server Account section.
2. Download the Dr.Web Proxy Server installer from the installation page.
3. Copy the certificate of the Dr.Web Server to which Dr.Web Proxy Server will be connected (see Connecting Dr.Web Proxy Server to Dr.Web Server) and the Dr.Web Proxy Server installer to the station where you want to install it.
4. Run the Dr.Web Proxy Server installer. The **Installation of Dr.Web Proxy Server** window containing information about the product being installed will open. Click **Next**.
5. Set the following parameters in the **Network listening settings** section of the Dr.Web Proxy Server general settings window:

- In the **Listening address** field, specify the IP address that Dr.Web Proxy Server will listen on. By default, all network interfaces (network adapters) of the computer are listened on.

Addresses must be specified in the network address format described in the **Appendices**, Appendix D. Specification of Network Addresses.

- In the **Port** field, specify the port number on which Dr.Web Proxy Server will listen. By default, it is port `2193`.
- Set the **Enable discovery** flag to enable the Dr.Web Proxy Server discovery mode. This mode allows clients to discover Dr.Web Proxy Server functioning as Dr.Web Server during multicast requests.
- Set the **Enable multicasting** flag for Dr.Web Proxy Server to respond to multicast requests addressed to Dr.Web Server.
  - In the **Multicast group address** field, specify the IP address of a multicast group to which Dr.Web Proxy Server will belong. The specified interface will be listened to by Dr.Web Proxy Server for interaction with clients during active Dr.Web Server searches. If you leave this field blank, Dr.Web Proxy Server will not be included in any multicast group. The default multicast group in which Dr.Web Server is included is `231.0.0.1`.

In the **Client connection settings** section:

- In the **Compression mode** drop-down list, select the compression mode for data traffic between Dr.Web Proxy Server and the served clients: Dr.Web Agents and Dr.Web Agent installers. In the **Level** field, select the compression level (from 1 to 9).
- In the **Encryption mode** drop-down list, select the encryption mode for data traffic between Dr.Web Proxy Server and the served clients: Dr.Web Agents and Dr.Web Agent installers.

  For detailed information on encryption and compression refer to section Traffic Encryption and Compression.

Click **Next**.

6. Configure the connection forwarding settings:
   - Enter the address of the Dr.Web Server to which connections established by Dr.Web Proxy Server should be forwarded and click  . Dr.Web Proxy Server will connect to this Dr.Web Server after installation to receive its configuration. The certificate of this Dr.Web Server was copied to the station in step 3.

Addresses must be specified in the network address format described in the **Appendices**, Appendix D. The Specification of Network Addresses.

   - In the **Encryption** drop-down list, select the encryption mode for data traffic between Dr.Web Proxy Server and the specified Dr.Web Server.
   - In the **Compression** drop-down list, select the compression mode for traffic between Dr.Web Proxy Server and each of the specified Dr.Web Servers. In the **Level** drop-down list, select the compression level (from 1 to 9).

To add one more Dr.Web Server to the traffic forwarding list, enter its address in the field, click  and specify the encryption and compression settings.

To remove the last added Dr.Web Server from the traffic forwarding list, click  .

After the installation is completed, Dr.Web Proxy Server connects to the first Dr.Web Server from this section to receive the settings.

If the Dr.Web Proxy Server configuration is specified on Dr.Web Server, all the settings specified in the installer will be replaced with the new configuration received from Dr.Web Server.

After specifying the forwarding settings, click **Next**.

7. A window with Dr.Web Server connection settings for remote control will open.

   The connection will established with the first Dr.Web Server specified for traffic forwarding in step 6.

   - In the **Server certificate** field, specify the certificate file copied to the station in step 3. To select the file, click **Browse**.
   - In the **Identifier** and **Password** fields, specify the credentials of the account created on Dr.Web Server in step 1.

   Click **Next**.

8. Specify the Dr.Web Proxy Server caching settings in the **Caching configuration** window:

   Set the **Enable caching** flag to cache data transferred by Dr.Web Proxy Server and specify the following parameters:

   - In the **Revision deletion period (minutes)** field, specify the interval at which old revisions should be deleted from the cache if their number exceeds the maximum number of revisions that are kept. The value is set in minutes. The default value is 60 minutes.
     - In the **Number of revisions to keep** field, specify the maximum number of revisions of each product to remain in the cache after the purge. By default, the last 3 revisions are kept, and the older revisions are deleted.
   - In the **Unused files unloading period (minutes)** field, specify the time interval in minutes for unloading unused files from the memory. The default value is 10 minutes.

   After specifying the caching settings, click **Next**.

9. A window with the message that Dr.Web Proxy Server is ready for installation will open.

   If you want to change other installation parameters, particularly the Dr.Web Proxy Server installation folder and the path for storing files used by Dr.Web Proxy Server, click **Additional parameters**.

   To start the installation of Dr.Web Proxy Server, click **Install**.

10. When the installation is finished, click **Exit**.

11. After the installation, Dr.Web Proxy Server connects to the first Dr.Web Server specified in step 6 to receive the complete configuration file. If the settings on Dr.Web Server are not

specified, the configuration file will not be downloaded. The configuration specified by the installer will be used until the connected Dr.Web Server is configured.

Installing Dr.Web Proxy Server in Unix-like OS

1. Download the Dr.Web Proxy Server installer from the installation page.
2. Run Dr.Web Proxy Server installer by executing the following command:

   `./<distribution_file>.tar.gz.run`
3. Accept the license agreement to continue the installation.
4. Specify the path to the Dr.Web Server certificate. You can also add the certificate after Dr.Web Proxy Server installation (see Connecting Dr.Web Proxy Server to Dr.Web Server).
5. If necessary, you can use the configuration files from the previous Dr.Web Proxy Server installation:
   - To use the default backup stored in `/var/tmp/drwcsd-proxy`, press ENTER.
   - To use the backup from a different directory, specify the path to the backup manually.
   - You can also install Dr.Web Proxy Server with the default settings without using the backup configuration from the previous version. To do this, press 0.
6. After Dr.Web Proxy Server installation, if necessary, you can edit the corresponding configuration files manually (see Connecting Dr.Web Proxy Server to Dr.Web Server).

Start and stop

During the software installation in **FreeBSD** OS, an rc script `/usr/local/etc/rc.d/dwcp_proxy` is created. Use the commands:

- /usr/local/etc/rc.d/dwcp_proxy stop—to stop Dr.Web Proxy Server manually;
- /usr/local/etc/rc.d/dwcp_proxy start—to start Dr.Web Proxy Server manually.

During the installation in **Linux** OS, an init script /etc/init.d/dwcp_proxy is created to start and stop Dr.Web Proxy Server.

5.5.4. Connecting Dr.Web Proxy Server to Dr.Web Server

Dr.Web Proxy Server can be connected to Dr.Web Server to remotely configure settings and to support traffic encryption.

Connection settings

The following are required to connect Dr.Web Proxy Server to Dr.Web Server:

- **Dr.Web Server certificate** `drwcsd-certificate.pem`.

  The Proxy Server must have all certificates of all Dr.Web Servers to which it connects and to which the client traffic is forwarded.

- The Dr.Web Server certificate is required to connect to Dr.Web Server for remote configuration and to support encryption of traffic between Dr.Web Server and Dr.Web Proxy Server.
- The Proxy Server certificate is signed by the Dr.Web Server certificate and private key (the procedure is performed automatically on Dr.Web Server after the connection is established, and no administrator intervention is required) and is required to connect Dr.Web Agents and to support encryption of traffic between Dr.Web Agents and Dr.Web Proxy Server.

All the Dr.Web Server certificates are stored on Dr.Web Proxy Server in the `drwcsd-proxy-trusted.list` configuration file in the following format (certificates records are separated by one or more empty lines):

```
[<certificate_1>]

[<certificate_2>]

[<certificate_3>]
...
```

- **Dr.Web Server address.**

  Dr.Web Proxy Server connects to all Dr.Web Servers that are specified in its configuration file for forwarding the client traffic. However, it is allowed to accept settings only from a specific set of connected Dr.Web Servers that are marked as managing. If more that one Dr.Web Server is marked as managing, then Dr.Web Proxy Server connects to all the Dr.Web Servers in rotation until it gets the first valid (not empty) configuration.

- **Identifier and password to access Dr.Web Server.**

  Credentials are available after creating Dr.Web Proxy Server account using the Control Center (see Creating Dr.Web Proxy Server Account).

  Dr.Web Proxy Server identifier and password are used in a single copy. You must create Dr.Web Proxy Server accounts with the same credentials on all Dr.Web Servers to which Dr.Web Proxy Server connects.

  Credentials are stored on Dr.Web Proxy Server in the `drwcsd-proxy.auth` configuration file in the following format:

```
[<Proxy_server_ID>]
[<Proxy_server_password>]
```

Connecting Dr.Web Proxy Server to Dr.Web Server

In order to connect to Dr.Web Proxy Server, you must enable the corresponding protocol on Dr.Web Server. To do this, set the **Dr.Web Proxy Server protocol** flag in the Control

Center in the **Administration** → **Dr.Web Server configuration** → **Modules** section, save the settings and restart Dr.Web Server.

Automatic connection to Dr.Web Server when installing in Windows OS

- If Dr.Web Proxy Server is installed as part of the Dr.Web Agent installation or if it is installed on the station where the Dr.Web Agent is installed, then the connection to Dr.Web Server is established automatically.
- If Dr.Web Proxy Server is installed via the graphical installer in Windows OS, then the connection to Dr.Web Server is established automatically using the credentials specified by the administrator in the installer settings.

  After installing Dr.Web Proxy Server, the files for the connection to Dr.Web Server are located by default in the following folder: `C:\ProgramData\Doctor Web\drwcs\etc`.

Manual connection for installation in Unix-like OS

1. Install Dr.Web Proxy Server for Unix-like OS according to the procedure described in the Installing Dr.Web Proxy Server Using Installer section.
2. Create Dr.Web Proxy Server account using the Control Center as described in the Creating Dr.Web Proxy Server Account section.
3. Copy the Dr.Web Server certificate to the computer where Dr.Web Proxy Server is installed.
4. In the `drwcsd-proxy-trusted.list` configuration file, specify the certificate copied to the computer in step 3: copy and paste the contents of the certificate file into the configuration file according to the format above.
5. In the `drwcsd-proxy.auth` configuration file, specify the Dr.Web Server connection settings for the account created in step 2 according to the format above.

   The `drwcsd-proxy-trusted.list` and `drwcsd-proxy.auth` files must be located in the following directories:

   - for Linux OS: `/var/opt/drwcs/etc`
   - for FreeBSD OS: `/var/drwcs/etc`

   Set the following permissions for the files

```
drwcsd-proxy-trusted.list 0644 drwcs:drwcs

drwcsd-proxy.auth 0600 drwcs:drwcs
```

Quick connection using the command line

This option is especially relevant for Unix-like OS, as it eliminates the need to edit configuration files manually. A single command can be used to connect to another server, reset settings, or in case if you have problems with the existing connection to the server.

Use the following commands:

- Windows OS:

```
drwcsd-proxy deploy <server-address> <server-certificate> <proxy-login> <proxy-password>
```

- Linux OS:

```
/etc/init.d/dwcp_proxy deploy <server-address> <server-certificate> <proxy-login> <proxy-password>
```

- FreeBSD OS:

```
/usr/local/etc/rc.d/dwcp_proxy deploy <server-address> <server-certificate> <proxy-login> <proxy-password>
```

On successful connection:

- The username and the password are written to the Dr.Web Proxy Server `drwcsd-proxy.auth` configuration file.
- The Dr.Web Server certificate is written to the `drwcsd-proxy-trusted.list` configuration file.
- A new private key `drwcsd-proxy.pri` is generated.
- The new certificate is generated, signed on the server and added to the list of signed certificates (`drwcsd-proxy-signed.list`).
- The configuration file is downloaded from the server and added to the `drwcsd-proxy.conf` configuration file.

5.6. Installation Error Codes

If errors occur during the installation, the following error codes are returned:

Error code	Description
0	Installation successfully completed
1	Incorrect command format
2	Unknown error
3	Insufficient rights to complete the operation (writing to the registry, creating files, or any other operation required for installation)
4	Dr.Web Agent is already installed
5	Installation is already running

Error code	Description
7	Installation canceled
9	Server time-out
11	Insufficient rights to uninstall the application
12	The operating system version is out of date
13	Incompatible application detected
14	Unable to install, reboot is required (the system will wait for the reboot before the next installation attempt)
15	Unsupported operating system architecture. Only x86 and x86_64 are supported
16	Operating system does not support SHA-2 algorithm
50	The standalone version can't be removed in the background

Check the log entries to determine the cause of the error. The error codes given are general, the same error may occur for different reasons.

Chapter 6: Removal of Dr.Web Enterprise Security Suite Components

6.1. Removing Dr.Web Server

6.1.1. Removing Dr.Web Server for Windows OS

To remove Dr.Web Server or Dr.Web Security Control Center Extension 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**.

Dr.Web Server software can also be removed using standard Windows OS tools via the **Control Panel → Add or Remove Programs**.

When removing Dr.Web Server, configuration files, encryption keys and embedded database are back up only if you set the **Back up Dr.Web Server critical data** option.

6.1.2. Removing Dr.Web Server for Unix-like OS

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

To uninstall Dr.Web Server version 10 or later

Dr.Web Server OS	Action
FreeBSD	Run the script: `/usr/local/etc/drweb.com/software/drweb-esuite.remove`
Linux	Run the script: `/etc/opt/drweb.com/software/drweb-esuite.remove`

When uninstalling Dr.Web Server on **FreeBSD** and **Linux** OS, all Dr.Web Server operations will be immediately terminated; the database, key, and configuration files will be copied to the `/var/tmp/drwcs` default backup folder (a list of backed up files is given in the Upgrading Dr.Web Server for Unix-like OSs section).

To prevent a backup copy from being created when uninstalling Dr.Web Server, declare the `SKIP_BACKUP` variable with any value (for example, `SKIP_BACKUP="x"`) in the `common.conf` file. The file is located in the following folder:

- Linux OS: `/var/opt/drwcs/etc`
- FreeBSD OS: `/var/drwcs/etc`

If the file does not exist yet, create it.

6.2. Removing Dr.Web Agent

Dr.Web Agent can be removed from protected stations in the following way:

- For stations under Windows OS:
  - Remotely via the Control Center.
  - Locally on station.
  - Via the Active Directory service, if Dr.Web Agent was installed using this service.
- For stations under Android OS, Linux OS, macOS—locally on stations.

Removing of Dr.Web Agent on workstations under Android OS, Linux OS, macOS is described in the **User Manual** for corresponding OS.

6.2.1. Removing Dr.Web Agent for Windows OS

Uninstalling Dr.Web Agent and Anti-Virus Package Remotely

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

If you uninstall Dr.Web 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 **Anti-virus network** item in the main menu of Dr.Web Security Control Center.
2. In the opened window, select the necessary group or specific anti-virus stations.
3. Click **General** → **Uninstall Dr.Web Agent** in the anti-virus network tree toolbar.
4. In the opened **Dr.Web Agent uninstallation** window, you can select one of the options for automatic restart once Dr.Web Agent is removed on selected stations, if necessary:

- **Immediately after uninstallation** prescribes for a station to restart 5 minutes after Dr.Web Agent is removed.
- **At a specified hour** allows you to set a specific time for station restart, in increments of 1 hour.
- **Within a specified period** lets you set a time period for station restart to happen.

If any of the restart options is selected, the station user will get a timely pop-up notification from Dr.Web Agent.

Restart option	User notification
Not selected	A station is not restarted after Dr.Web Agent is removed. No notification is shown.
Immediately after uninstallation	The notification is shown 5 minutes before the restart, stating the exact time when the station will restart.
At a specified hour	• **First notification** The notification is shown immediately after Dr.Web Agent is removed. The message contains the exact time of the scheduled restart. • **Second notification** The notification is shown 5 minutes before the restart, stating the exact time when the station will restart. • **If the station could not be reached at the specified hour** The notification is shown 15 minutes after re-establishing connection with the station. The message notifies of the upcoming restart in the next 5 minutes, stating the exact time.
Within a specified period	• **First notification** The notification is shown immediately after Dr.Web Agent is removed. The message contains the exact time of the scheduled restart within the specified period. • **Second notification** The notification is shown 5 minutes before the restart, stating the exact time when the station will restart. • **If the station could not be reached within the specified period** The notification is shown 15 minutes after re-establishing connection with the station. The message notifies of the upcoming restart on the next day, stating the exact time within the specified period.

5. The Dr.Web Agent software and the anti-virus package will be removed from the workstations selected.

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

Uninstalling Dr.Web Agent and Anti-Virus Package Locally

To remove Dr.Web Agent and the anti-virus package locally, this option must be allowed at Dr.Web Server in the **Permissions** section (see **Administrator Manual**, Permissions of Station Users).

You can remove the station anti-virus software (Dr.Web Agent and anti-virus package) by the two ways:

1. By means of standard Windows OS services.
2. By using a Dr.Web Agent installation file.

If Dr.Web Agent and anti-virus package are uninstalled via the standard Windows OS services or via the Dr.Web 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 Dr.Web Agent by using the graphical installer and set the **Register Dr.Web Agent in the system list of installed software** flag.

If Dr.Web 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 yes` switch was used for installation.

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

Removing by Using Dr.Web Agent Installation Files

The procedure depends on the type of the Dr.Web Agent installation file:

- `win-es-agent-setup.exe` **client module**:

  Run the `win-es-agent-setup.exe` file with the `/instMode remove` parameter. Additionally, you can use the `/silent no` parameter if you want to control the process.

  The `win-es-agent-setup.exe` file is located in the following folder by default:

  - Windows XP OS and Windows Server 2003 OS:

    `%ALLUSERSPROFILE%\Application Data\Doctor Web\Setup\`

  - Windows Vista OS and later and Windows Server 2008 OS and later:

    `%ALLUSERSPROFILE%\Doctor Web\Setup\`

  An example for Windows 7, where `%ALLUSERPROFILE%` corresponds to `c:\ProgramData`:

```
C:\ProgramData\Doctor Web\Setup\win-es-agent-setup.exe /instMode
remove /silent no
```

- `drweb_es_<OS>_<station>.exe` **personal installation package**:

  Run the `drweb_es_<OS>_<station>.exe` file of the currently installed version.

- `drweb-<agent_version>-<build>-esuite-agent-full-windows.exe` **full installer**:

  Run the `drweb-<agent_version>-<build>-esuite-agent-full-windows.exe` file of the currently installed version.

- `drwinst.exe` **network installer**:

  Run the `drwinst.exe` installer with the `/instMode remove` parameter from the installation folder of the Dr.Web Agent (`C:\Program Files\DrWeb` by default). Additionally, you can use the `/silent no` parameter if you want to control the process.

  For example:

```
drwinst /instMode remove /silent no
```

When you launch the `drweb_es_<OS>_<station>.exe` installation package, the `drweb-<agent_version>-<build>-esuite-agent-full-windows.exe` full installer or the `drwinst.exe` network installer, the `win-es-agent-setup.exe` client module launches and performs the removal directly.

The `win-es-agent-setup.exe` client module launched without parameters, detects installed product and launches the change/remove mode. To launch the remove mode directly, use the `/instMode remove` switch.

6.2.2. Removing Dr.Web Agent through Active Directory

To be able to uninstall Dr.Web Agent, the permission to do so must be enabled on Dr.Web Server in the **Permissions** section (see the **Administrator Manual**, Permissions of Station Users).

1. Open the group policy editor. To do this:
   - In Windows 2000/2003 Server:
     a) In the Windows Control Panel, select **Administrative Tools** → **Active Directory Users and Computers**.
     b) Select the organizational unit you created when installing Dr.Web Agents in the corresponding domain.
     c) In the context menu of the organizational unit, select **Properties** and go to the **Group Policy** tab.
     d) Select the list item with the corresponding group policy name and double-click it. The **Group Policy Object Editor** window opens.
   - In Windows Server 2008/2012/2012 R2 and later:

a) Open **Start** → **Administrative Tools** → **Group Policy Management**.

b) Select the organizational unit you created when installing Dr.Web Agents in the corresponding domain.

c) Select the list item with the corresponding group policy name.

d) In the context menu of this policy, select **Edit**. The **Group Policy Management Editor** window opens.

2. In the **Group Policy Object Editor (Group Policy Management Editor)** window, go to the package settings for the group policy:
   - In Windows 2000/2003 Server: in the hierarchical tree, select **Computer Configuration** → **Software Settings** → **Software Installations** → **Package**.
   - In Windows Server 2008/2012/2012 R2 or later: in the hierarchical tree, select **Computer Configuration** → **Policies** → **Software Settings** → **Software Installations** → **Package**.
3. In the context menu of the Dr.Web Agent package, select **All tasks** → **Uninstall** → **OK**.

   In Windows 2000/2003 Server: click **OK** on the **Group Policy** tab.

Dr.Web Agent will be uninstalled from the stations at the next registration in the domain.

6.3. Removing Dr.Web Scanning Server

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

When removing the Scanning Server make sure that there are no stations interacting with it in the anti-virus network. Otherwise these stations will be left without protection.

1. On the virtual machine performing function of the Scanning Server go to the directory `/opt/drweb.com/bin`.
2. Run the script `uninst.sh`.
3. To initiate the removal, enter *Yes* or *Y* in response to the question "Do you want to continue?". To exit the uninstaller, type *No* or *N*. In this case, removal of Dr.Web Scanning Server will be canceled.
4. An automatic uninstallation procedure will be launched after you confirm it. During this procedure, information about the removal process will be displayed on the screen and entered into the uninstallation log.
5. Once the process is completed, the uninstallation program will automatically terminate.

6.4. Removing Dr.Web Proxy Server

The Proxy Server can be uninstalled by one of the following ways:

1. Locally.

Local deinstallation is performed by administrator directly on the computer with the Proxy Server installed.

2. Remotely.

   Remote deinstallation of the Proxy Server is performed in the Control Center via LAN and available only if the Proxy Server is connected to Dr.Web Server.

6.4.1. Local Removing Dr.Web Proxy Server

Dr.Web Proxy Server can be removed locally from a computer only if it was previously installed locally as well, using the installer. Otherwise, proceed to the Remote Removing Dr.Web Proxy Server section and follow those instructions.

For Windows OS

When the Proxy Server is uninstalled, its configuration files are not deleted and remain in the `%ALLUSERSPROFILE%\Doctor Web\` folder.

Dr.Web Proxy Server can be uninstalled from Windows OS using either standard operating system tools or the installer.

Removal with Standard Tools

Use **Control Panel** → **Add or Remove Programs** (**Programs and components** for Windows 2008 or later).

Removal with the Installation Files

The procedure depends on the type of the Dr.Web Proxy Server installation file:

- `proxy-setup.exe` **client module**:

  Run the `proxy-setup.exe` file followed by the `/instMode remove` parameter. Use the additional `/silent no` parameter if you want to control the process.

  The default location of the `proxy-setup.exe` file:

  - Windows XP and Windows Server 2003:

    `%ALLUSERSPROFILE%\Application Data\Doctor Web\Setup\drweb-win-proxy\`

  - Windows Vista or a later; on Windows Server 2008 and later:

    `%ALLUSERSPROFILE%\Doctor Web\Setup\drweb-win-proxy\`

  An example of this command for Windows 10, where `%ALLUSERPROFILE%` corresponds to `c:\ProgramData`:

```
C:\ProgramData\Doctor Web\Setup\drweb-win-proxy\proxy-setup.exe /instMode
remove /silent no
```

- `drweb-proxy-<package_version>-<build>-windows-nt-<bitness>.exe` **installer**:

  Download the `drweb-proxy-<package_version>-<build>-windows-nt-<bitness>.exe` file from the installation page and run it. Follow the instructions.

For Unix-like OSs

When the Proxy Server is uninstalled, its configuration files are automatically backed up to `/var/tmp/drwcsd-proxy`.

Proxy Server OS	Action
FreeBSD	Run the script: `/usr/local/etc/drweb.com/software/drweb-proxy.remove`
Linux	Run the script: `/etc/opt/drweb.com/software/drweb-proxy.remove`

6.4.2. Remote Removing Dr.Web Proxy Server

Remote deinstallation of the Proxy Server is available when the Proxy Server is connected to Dr.Web Server (see Connecting Dr.Web Proxy Server to Dr.Web Server).

To delete Dr.Web Proxy Server that is installed on the connected station

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. Open the station properties section by one of the following ways:
   a) Click the name of the station in the hierarchical list of the anti-virus network. A panel with properties of the station will be automatically opened in the right part of the Control Center.
   b) Click **Properties** in the control menu. A window with the station properties will be opened.
3. In the station properties window, go to the **Dr.Web Proxy Server** section.
4. Click **Delete Dr.Web Proxy Server**.
5. After you click **Save**, Dr.Web Proxy Server will be deinstalled from the station. Proxy Server account—deleted from Dr.Web Server.

Chapter 7: Upgrading Dr.Web Enterprise Security Suite Software and Its Components

Upgrading Dr.Web Server from versions 12 to version 13 is available via the Control Center. The procedure is described in the **Administrator Manual**, in the Updating Dr.Web Server and Restoring it from Backup section.

Before updating Dr.Web Enterprise Security Suite and its components, please note the following important features:

- Before updating, it is recommended to check the validity of TCP/IP protocol configuration for the internet access. Particularly, DNS service must be enabled and properly configured.
- Before upgrading Dr.Web Server, it is recommended that all of the Dr.Web Enterprise Security Suite components (Dr.Web Agent included) are upgraded to the latest version available at GUS.
- In multiserver anti-virus network configuration, consider that interserver updates transmission is not performed between Dr.Web Servers of 13 version and Dr.Web Servers of previous versions and interserver connection is used for transmission statistics only. To provide interserver updates transmission, you must upgrade all Dr.Web Servers. If Dr.Web Servers of previous version are required as a part of the anti-virus network to connect Dr.Web Agents installed on operating systems which are not supported by the 13 version (see Upgrading Dr.Web Agent), then Dr.Web Servers of versions 6 and Dr.Web Servers of the 13 version must receive updates independently.
- Upgrade of Dr.Web Server cluster from version 11 to version 13 shall be performed individually, meaning each cluster node shall be disconnected from the cluster, switched over to embedded database, updated and connected back to the cluster one by one.
- For the anti-virus network containing Dr.Web Proxy Server, at upgrade of the components up to the version 13, you must also upgrade the Proxy Server up to the version 13. Otherwise, Dr.Web Agents supplied within version 13 will not be able to connect to Dr.Web Server of version 13. It is recommended to perform the upgrade in the following order: Dr.Web Server → Dr.Web Proxy Server → Dr.Web Agent.
- At upgrading Dr.Web Server, all repository settings will not be transferred to the new version (will be reset to defaults), however they are backed up. If necessary, specify the repository settings manually after the Dr.Web Server upgrade.
- By default, after installing Dr.Web Server version 13, updates of the **Virus databases for Android**, **Content filter databases 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**, 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.

7.1. Upgrading Dr.Web Server for Windows OS

The following upgrade options are available:

If you need to upgrade from 6 or 10 version, upgrade to version 11 first, and then to version 13.

Before upgrading Dr.Web Server, please read the Upgrading Dr.Web Agent section.

Not all Dr.Web Server updates within version 13 have the distribution kit file. Some of them can be installed via the Control Center only.

Saving configuration files

When upgrading Dr.Web Server to version 13 using the installer, the configuration files are saved to the backup folder specified in the **Back up Dr.Web Server critical data** option during the upgrade (<*installation_drive*>:\`DrWeb Backup` by default).

The following configuration files are saved:

File	Description
`agent.key` (name may vary)	Dr.Web Agent license key file
`auth-ads.conf`	configuration file for external authorization of administrators via Active Directory
`auth-radius.conf`	configuration file for external authorization of administrators via RADIUS
`auth-ldap.conf`	configuration file for external authorization of administrators via LDAP
`auth-ldap-rfc4515.conf`	configuration file for simple external authorization of administrators via LDAP
`auth-ldap-rfc4515-check-group.conf`	template configuration file for simple external authorization of administrators via LDAP with Active Directory group membership verification
`auth-ldap-rfc4515-check-group-novar.conf`	template configuration file for simple external authorization of administrators via LDAP with Active Directory group membership verification using variables
`auth-ldap-rfc4515-simple-login.conf`	template configuration file for simple external authorization of administrators via LDAP
`auth-pam.conf`	configuration file for administrators external authorization via PAM

File	Description
`enterprise.key` (name may vary)	Dr.Web Server license key file. The file is saved if it was present after the upgrade from the previous versions. The file is missing when installing a new Dr.Web Server
`drwcsd-certificate.pem`	Dr.Web Server certificate
`download.conf`	network settings for generating Dr.Web Agent installation packages
`drwcsd.conf` (name may vary)	Dr.Web Server configuration file
`drwcsd.conf.distr`	template Dr.Web Server configuration file with default parameters
`drwcsd.pri`	private encryption key
`dbexport.gz`	database export
`drwcsd.pub` (name may vary)	public encryption key
`frontdoor.conf`	configuration file for the Dr.Web Server remote diagnostic utility
`openssl.cnf`	Dr.Web Server certificate for HTTPS
`webmin.conf`	Dr.Web Security Control Center configuration file
`yalocator.apikey`	API key for the Yandex.Locator extension

If necessary, save other important files (for instance, report templates stored in the `\var\templates` folder) in a different location from the Dr.Web Server installation folder.

Saving the database

Before upgrading, make sure that the Microsoft SQL DBMS has case-sensitive (`_CS`) and accent-sensitive (`_AS`) collation suffixes specified. Otherwise it will not be possible to update automatically.

Before upgrading, also make sure that the DBMS you use is supported by Dr.Web Server version 13. Otherwise it will not be possible to upgrade automatically. A list of supported DBMSs is available in the **Appendices**, Appendix A. The Description of the DBMS Settings. The Parameters of the DBMS Driver.

Before upgrading the Dr.Web Enterprise Security Suite software, it is recommended that you back up the database first.

To back up database

1. Stop Dr.Web Server.
2. Export the database to file:
   - for Dr.Web Server prior to version 13

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all exportdb <backup_folder>\esbase.es
```

   - for Dr.Web Server version 13 and later

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all modexecdb database-export <backup_folder>\esbase.es
```

For Dr.Web Servers with an external database, use the standard tools supplied with the database.

Make sure that the Dr.Web Enterprise Security Suite database export completed successfully. If a database backup copy is not available, Dr.Web Server cannot be restored in an emergency case.

Upgrading Dr.Web Server

To upgrade Dr.Web Server, run the distribution file.

By default, the installer uses the language of the operating system. If necessary, you can change the installation language at any step by selecting the corresponding option in the right upper part of the installer window.

If you use an external Dr.Web Server database, also select **Use existing database** during the upgrade.

1. When upgrading from versions 11, 12 and within version 13, a window notifying you of the previous Dr.Web Server version installed and offering a brief description of the upgrade process to a new version will open. To start configuring the upgrade procedure, click **Upgrade**.
2. The next window allows you to configure the backup of critical data before uninstalling Dr.Web Server of the previous version. It is recommended that you set the **Back up Dr.Web Server critical data** flag. If necessary, you can change the default backup folder

(<*installation_drive*>:\DrWeb Backup). Click **Uninstall** to start the uninstallation of Dr.Web Server of the previous version.

3. Once the previous version is uninstalled, the installation of the new version of Dr.Web Server starts. A window with information on the product and the link to the license agreement text will open. After you have read the agreement, select **I accept the terms of the license agreement** and click **Next** to continue the installation.
4. The following steps configure a Dr.Web Server that uses an existing database (same as the Installing Dr.Web Server process based on the configuration files from the previous installation). The installation wizard automatically locates the Dr.Web Server installation folder, its configuration files, and the location of the embedded database from the previous installation. If necessary, you can change the locations of the files which were found automatically by the installer.
5. To start the installation of Dr.Web Server version 13, click **Install**.

Once the upgrade of Dr.Web Servers within the anti-virus network is completed, you must do the following:

1. Configure encryption and compression settings for connected Dr.Web Servers (see the **Administrator Manual**, Setting Connections between Several Dr.Web Servers).
2. Clear the cache of the web browser that is used to connect to Dr.Web Security Control Center.

7.2. Upgrading Dr.Web Server for Unix-like OS

An upgrade of Dr.Web Server up to version 13 can be performed in the following ways:

- Upgrading Dr.Web Server of version 11 or later for the same package types is performed automatically for all Unix-like OSs. If needed, you can also perform the upgrade manually.
- Upgrading Dr.Web Server of version 12 or later is also available via the Control Center. The procedure is described in the **Administrator Manual**, in the Updating Dr.Web Server and Restoring from the Backup section.

Before upgrading Dr.Web Server, please read the Upgrading Dr.Web Agent section.

Updating Dr.Web Server within version 13 can be also performed via the Control Center. The procedure is described in the **Administrator Manual**, in the Updating Dr.Web Server and Restoring from the Backup section.

Not all Dr.Web Server updates within version 13 have the distribution kit file. Some of them can be installed via the Control Center only.

Saving configuration files

When uninstalling and automatically upgrading Dr.Web Server to version 13, the configuration files are saved to the default backup directory: `/var/tmp/drwcs/`.

When uninstalling Dr.Web Server, the following files are automatically saved:

File	Description
`agent.key` (the name may vary)	Dr.Web Agent license key file
`auth-ldap.conf`	configuration file for external authorization of administrators via LDAP
`auth-ldap-rfc4515.conf`	configuration file for simple external authorization of administrators via LDAP
`auth-pam.conf`	configuration file for external authorization of administrators via PAM
`auth-radius.conf`	configuration file for external authorization of administrators via RADIUS
`certificate.pem`	SSL certificate
`common.conf`	`configuration file (for some Unix-like OSs)`
`dbexport.gz`	database export (created during the Dr.Web Server uninstallation using the command `drwcs.sh xmlexportdb`)
`download.conf`	network settings for generating Dr.Web Agent installation packages
`drwcsd-certificate.pem`	Dr.Web Server certificate
`drwcsd.conf` (the name may vary)	Dr.Web Server configuration file
`drwcsd.pri`	private encryption key
`drwcsd.pub` (name may vary)	public encryption key
`enterprise.key` (name may vary)	Dr.Web Server license key file. The file is saved if it was present after the upgrade from the previous versions. The file is missing when installing a new Dr.Web Server
`frontdoor.conf`	configuration file for the Dr.Web Server remote diagnostic utility
`local.conf`	Dr.Web Server log settings
`private-key.pem`	RSA private key
`webmin.conf`	Dr.Web Security Control Center configuration file

File	Description
yalocator.apikey	API key for the Yandex.Locator extension

During an automatic upgrade, the following files are saved to the backup directory:

File	Description
auth-ldap.conf	configuration file for external authorization of administrators via LDAP
auth-ldap-rfc4515.conf	configuration file for simple external authorization of administrators via LDAP
auth-pam.conf	configuration file for external authorization of administrators via PAM
auth-radius.conf	configuration file for external authorization of administrators via RADIUS
db.backup.gz	database export (created during the Dr.Web Server upgrade using the command drwcs.sh exportdb)

Saving the database

Before upgrading the Dr.Web Enterprise Security Suite software, it is recommended that you back up the database first.

To back up database

1. Stop Dr.Web Server.
2. Export the database to file:
   - For FreeBSD:
     - for Dr.Web Server prior to version 13

```
# /usr/local/etc/rc.d/drwcsd exportdb /var/tmp/esbase.es
```

     - for Dr.Web Server version 13 and later

```
# /usr/local/etc/rc.d/drwcsd modexecdb database-
export /var/tmp/esbase.es
```

   - For Linux OS:
     - for Dr.Web Server prior to version 13

```
# /etc/init.d/drwcsd exportdb /var/tmp/esbase.es
```

     - for Dr.Web Server version 13 and later

```
# /etc/init.d/drwcsd modexecdb database-export /var/tmp/esbase.es
```

For Dr.Web Servers with an external database, use the standard tools supplied with the database.

Make sure that the Dr.Web Enterprise Security Suite database export completed successfully. If a database backup copy is not available, Dr.Web Server cannot be restored in an emergency case.

Automatic upgrade

Upgrading Dr.Web Server version 11 or later for the same package types is automatic for all Unix-like OSs.

The configuration files will be automatically converted and placed in the corresponding directories. Some configuration files are also stored in the backup directory.

Manual upgrade

If you cannot upgrade Dr.Web Server from version 11 or later over the installed package, uninstall the Dr.Web Server software of the previous versions saving a backup copy, and then install the software of version 13 using the saved backup copy.

To upgrade Dr.Web Server

1. Stop Dr.Web Server.
2. If you plan to use any files later (besides the files which are copied automatically during uninstallation of Dr.Web Server at step **3**), back up these files (for example, the report templates, etc) manually.
3. Uninstall the Dr.Web Server software (see Removing Dr.Web Server for Unix-like OS). You will be prompted to create backup copies of the files. To do this, specify the path to store the backup or accept the default path.
4. Install the new Dr.Web Server version 13 according to the general installation procedure (see Installing Dr.Web Server for Unix-like OS) using the backup copy from step **3**. All saved configuration files and the embedded database (if you use the embedded database) will be automatically converted to be used by Dr.Web Server version 13. Without the automatic conversion the database (if you use the embedded database) and some of the Dr.Web Server configuration files from the previous version cannot be used.

   If you saved some files manually, move them to the same directories where they were located in the previous version.

Set the user selected at the installation of the new Dr.Web Server version (**drwcs** by default) as the file owner for all backup files from the previous Dr.Web Server version (see step 4).

5. Launch Dr.Web Server.
6. Set up a repository upgrade and perform the full upgrade.

Once the upgrade of Dr.Web Servers within the anti-virus network is completed, configure encryption and compression settings for connected Dr.Web Servers (see the **Administrator Manual**, the Setting Connections between Several Dr.Web Servers section).

7.3. Upgrading Dr.Web Agent

Dr.Web Agent upgrade after Dr.Web Server upgrade is described for the following variants:

1. Upgrading Dr.Web Agents on Stations under Windows OS,
2. Upgrading Dr.Web Agents on Stations under Android OS,
3. Upgrading Dr.Web Agents on Stations under Linux and macOS.

7.3.1. Upgrading Dr.Web Agents on Stations under Windows OS

Upgrade of Dr.Web Agents Supplied with Dr.Web Enterprise Security Suite 10

Upgrade of Dr.Web Agents supplied with Dr.Web Enterprise Security Suite 10 is performed automatically.

After the automatic upgrade, the popup notification with restart request is displayed on a station; in the Control Center, restart request after the upgrade is displayed in the station status. Restart a station locally or remotely via the Control Center to complete the upgrade.

If the station was connected to Dr.Web Server via Dr.Web Proxy Server version 10 or earlier, you must upgrade the Proxy Server up to the version 13 or remove the Proxy Server before Dr.Web Agent upgrading.

Due to the end of support for version 10, a successful upgrade from version 10 to version 13 is not guaranteed. In this case, you should upgrade first to version 11, then to version 13.

Automatic Upgrade of Dr.Web Agents Supplied with Dr.Web Enterprise Security Suite 6

To perform automatic upgrade, the following conditions must be met:

1. Dr.Web Agents must be installed on computers under Windows OS which are supported for the installation of Dr.Web Agents for Dr.Web Enterprise Security Suite version 13.0 (see System Requirements).
2. For the automatic upgrade, the following actions are possible depending on the Dr.Web Server settings:
   a) Automatic upgrade is performed, if during the Dr.Web Server upgrade, encryption keys and network settings from the previous Dr.Web Server were saved.
   b) The manual configuration required during the automatic upgrade, if during the Dr.Web Server upgrade, new encryption keys and the Dr.Web Server network settings were specified.

Please note the following features during automatic upgrade:

1. After removing Dr.Web Agent, notification on reboot required is not displayed on a station. Administrator must initiate the station reboot.
2. Between the removal of an old Dr.Web Agent version and installing of a new version, stations will have no anti-virus protection.
3. After upgrading of Dr.Web Agent, the anti-virus software operation will be limited without the station restart. At this, the complete anti-virus protection of the station is not provided. User must restart the station on Dr.Web Agent demand.

Automatic upgrade of Dr.Web Agent is performed by the following procedure:

1. The old version of the Dr.Web Agent is uninstalled when upgrade is started.
2. The station is rebooted manually.
3. The new version of the Dr.Web Agent is installed. For this, the task in the Dr.Web Server schedule is automatically created.
4. After Dr.Web Agent upgrade is completed, the station automatically connects to Dr.Web Server. In the **Status** section of the Control Center, the notification on required restart will be displayed for the upgraded station. The station must be restarted.

Automatic upgrade of Dr.Web Agent with manual configuring is performed by the following procedure:

1. Configure settings for connection to the new Dr.Web Server and replace public encryption key on station manually.
2. After changing of the settings on the station and connecting the stations to Dr.Web Server, Dr.Web Agent upgrade process starts.
3. The old version of Dr.Web Agent is uninstalled when upgrade is started.
4. The station is rebooted manually.
5. The new version of Dr.Web Agent is installed. For this, the task in the Dr.Web Server schedule is automatically created.

6. After the Dr.Web Agent upgrade is completed, the station automatically connects to Dr.Web Server. In the **Status** section of the Control Center, the notification on required restart will be displayed for the upgraded station. The station must be restarted.

Manual Upgrade of Dr.Web Agents Supplied with Dr.Web Enterprise Security Suite 6

If installation of the new version of Dr.Web Agent during automatic upgrade failed for any reason, the next installation attempts are not performed. No anti-virus software will be installed on the station, and such station will be displayed as offline in the Control Center.

In such case, you must install the Dr.Web Agent by yourself. At this, after the new Dr.Web Agent installation, you must merge the new station and the old station in the Control Center, in the hierarchical tree of the anti-virus network.

If Upgrade is not Supported

If Dr.Web Agents are installed on stations under OS which are not supported for the installation of Dr.Web Agents for Dr.Web Enterprise Security Suite version 13.0, actions to upgrade are not performed.

Dr.Web Agents installed on unsupported OS cannot receive updates (including virus database updates) from the new Dr.Web Server. If Dr.Web Agents under unsupported OS are required, you must leave Dr.Web Server of previous version to which these Dr.Web Agents are connected as a part of the anti-virus network. At this, Dr.Web Servers of 6 versions and Dr.Web Servers of the 13.0 version must receive updates independently.

Recommendations on upgrading Dr.Web Agents, installed on the stations that implement significant LAN functions, specified in the **Appendices** document, Upgrading Dr.Web Agents on LAN servers.

7.3.2. Upgrading Dr.Web Agents on Stations under Android OS

Dr.Web Enterprise Security Suite 13.0 supports Dr.Web Agent for Android starting from version 12.2.

You can upgrade Dr.Web Agent for Android on mobile devices

1. Automatically. Starting from version 12.6.4, Dr.Web Agent for Android can upgrade on its own when Dr.Web Server notifies it about a new version available. To set up the automatic upgrade, make sure the Dr.Web Server repository configuration in the Control Center directs to update Dr.Web Mobile Security Suite (Android) (**Administration** → **General repository configuration** → **Dr.Web installation packages** → **Dr.Web enterprise products**), while the

settings for Android stations in the Control Center have the corresponding flag set (**Anti-virus Network** → a group of stations or a single station running Android OS → **Dr.Web Mobile Security Suite (Android)** → **Updates** → **Check for new version**).

2. Manually by installing an installation package of the new version on a mobile device. To do that, make sure the Dr.Web Server repository configuration in the Control Center directs to update Dr.Web Mobile Security Suite (Android) (**Administration** → **General repository configuration** → **Dr.Web installation packages** → **Dr.Web enterprise products**) and download the generated package from station properties or on the **Administration** → **Enterprise products** page in the Control Center.

Beginning from version 12, Dr.Web Mobile Security Suite (Android) can be updated from the Dr.Web Server provided that current version of the application was installed from the Dr.Web Server.

7.3.3. Upgrading Dr.Web Agents on Stations under Linux and macOS

Dr.Web Agents installed on stations under Linux-based OS and macOS connect to Dr.Web Server if the following conditions are met:

1. Dr.Web Agents must be installed on computers under operation systems which are supported for the installation of Dr.Web Agents for Dr.Web Enterprise Security Suite (see System Requirements).
2. Encryption keys and network settings from the upgraded Dr.Web Server must be set on the stations.

After connecting the stations to the updated Dr.Web Server:

1. Only virus databases will be updated on stations. Automatic upgrade of the anti-virus software itself is not performed.
2. If the last software version is installed on stations, no actions required.
3. If the software on stations is outdated, download installation package of Dr.Web Agent new version in the Control Center, in the station properties or on the installation page. Upgrade the station software manually as described in the corresponding **User Manual**.

7.4. Upgrading Dr.Web Proxy Server

7.4.1. Updating Dr.Web Proxy Server During Operation

The Proxy Server can be updated automatically during its operation.

If Dr.Web Server under Unix-like OS was previously updated from version 11.0 or 11.0.1, automatic update of Dr.Web Proxy Server is unavailable. To remove this restriction, in the

> **Administration → Detailed repository configuration → Dr.Web Proxy Server → Synchronization** section, in the **Update only following files** field, manually delete the `^win.*` prefix.
>
> If initially Dr.Web Server of version 11.0.2 was installed, restrictions on automatic update of Proxy Server do not apply.

Updates schedule depends on the settings of the Proxy Server proactive caching:

1. If the Proxy Server is not included into the list for the proactive caching (including if the caching is not used), when the Proxy Server updates will be downloaded and installed according to the automatic updates schedule.
2. If the Proxy Server is included into the list for the proactive caching, the Proxy Server updates will be automatically downloaded according to the proactive caching schedule. When a new revision of the Proxy Server is received, the update to this revision is performed according to the automatic updates schedule.

You can configure the automatic updates by one of the following ways:

- Via the Proxy Server settings in the Control Center of the managing Dr.Web Server, in the **Updates** section. Detailed description is given in the **Administrator Manual**, in the Remote Configuration of Dr.Web Proxy Server section.
- Via the Proxy Server configuration file `drwcsd-proxy.conf`. Detailed description is given in the **Appendices** document, F4. Dr.Web Proxy Server Configuration File.

7.4.2. Updating Dr.Web Proxy Server via the Installer

Dr.Web Proxy Server Configuration Files

File	Description
`drwcsd-proxy.conf`	Proxy Server configuration file (see the **Appendices** document, F4. Dr.Web Proxy Server Configuration File)
`drwcsd-proxy.auth`	credentials (ID and password) to access Dr.Web Servers
`drwcsd-proxy-trusted.list`	list of trusted certificates of Dr.Web Servers
`drwcsd-proxy-signed.list`	list of signed certificates of the Proxy Server
`drwcsd-proxy.pri`	private encryption key of the Proxy Server

Upgrading Proxy Server under Windows OS

Upgrade of the Proxy Server is performed automatically by the means of the installer.

1. Run the Proxy Server distribution file.
2. The opened window notifies you on the previous Proxy Server version installed and invites to upgrade to a new version. To start configuring upgrade procedure, click **Upgrade**.
3. The next window contains the information on uninstalling of the previous version of the Proxy Server. Click **Uninstall** to start the uninstalling process.
4. After the previous version of the Proxy Server is uninstalled, a new version starts the installation. The next window contains the information on the product. Click **Next**.
5. On the following steps, the upgrading Proxy Server is configured as at the Installing Dr.Web Proxy Server process based on the configuration files from the previous installation. The installation wizard automatically locates the Proxy Server installation folder and configuration files from the previous installation. If necessary, you can change settings from the files that were found automatically by the installer.
6. To start the installation of the Proxy Server, click **Install**.

Upgrading Proxy Server under Unix-like OS

To upgrade Proxy Server of version 11.0 and earlier

During Proxy Server upgrading, the configuration files are deleted. If necessary, save configuration files manually before the upgrading.

1. To start the upgrade process, run the Proxy Server distribution file:

   `./<distribution_file>.tar.gz.run`
2. If necessary, manually transfer the settings from the configuration files saved before the upgrade process to the new configuration files.

To upgrade Proxy Server from version 11.0.1

1. To start the upgrade process, run the Proxy Server distribution file:

   `./<distribution_file>.tar.gz.run`
2. During the uninstallation of the previous version, the configuration files of the Proxy Server will be automatically saved.
3. During the upgrade, you will be prompted to use configuration files from a previous Proxy Server installation, saved during the backup:
   - To use the default backup saved in `/var/tmp/drwcsd-proxy`, press ENTER.
   - To use the backup from the other directory, specify the path to the backup manually.
   - Also, you can install the Proxy Server with the default settings not using the backup configuration from the previous version. For this, press 0.