Dr.WEB

Enterprise Security Suite

Administrator Manual

Dr.Web Enterprise Security Suite
Version 13.0
Administrator Manual
3/5/2025

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

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.

Convention	Comment
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:

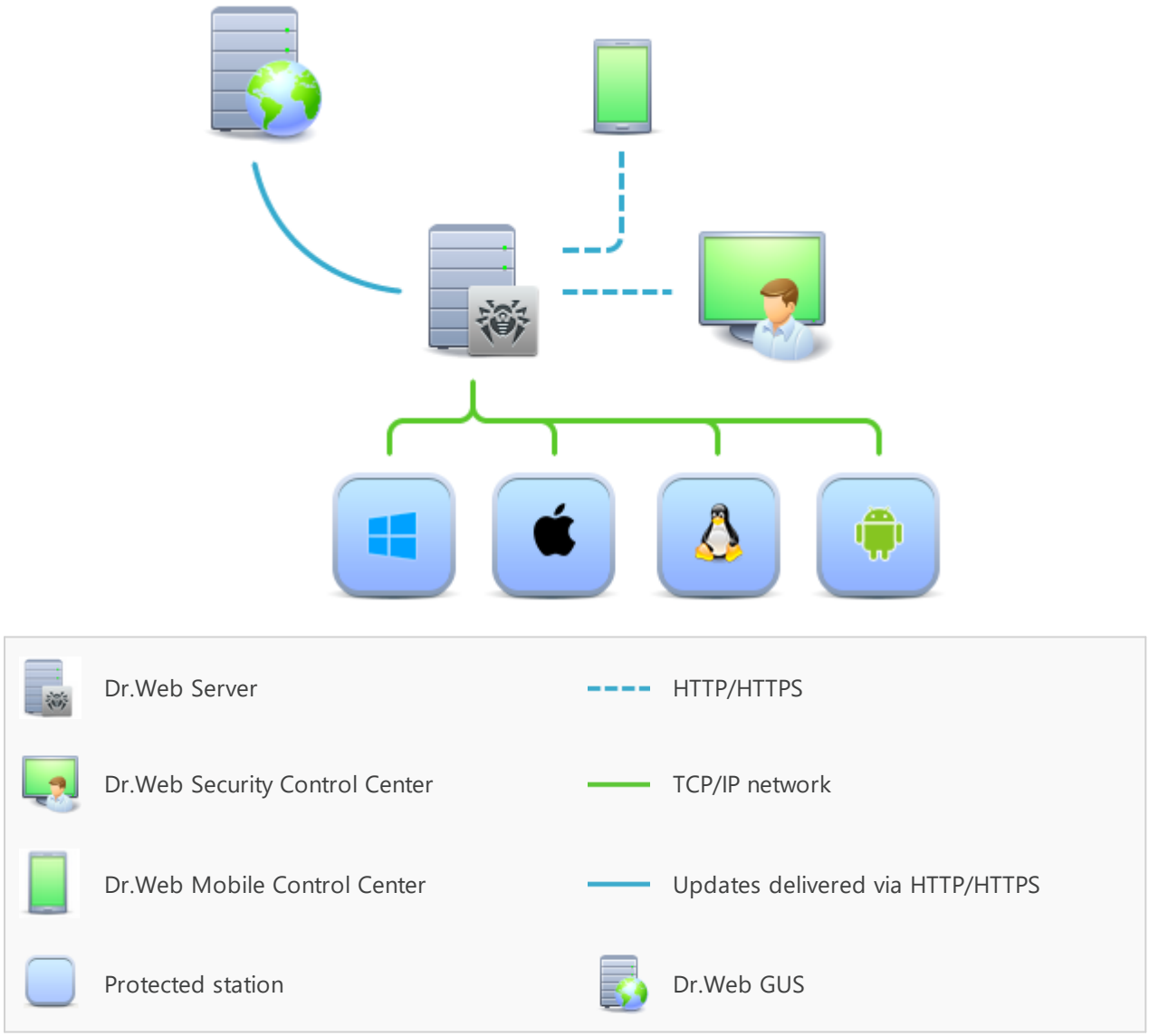
- ACL—Access Control List,
- CDN—Content Delivery Network,
- DB, DBMS—Database, Database Management System,
- DFS—Distributed File System,
- DN—Distinguished Name,
- DNS—Domain Name System,
- Dr.Web GUS—Dr.Web Global Update System,
- FQDN—Fully Qualified Domain Name,
- GUI—Graphical User Interface, a 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 the **Installation Manual**, 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 the **Installation Manual**, 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.
- Streamlined administration based on grouping of anti-virus network workstations (see detailed information in Chapter 7: Integrated Workstations Management).
- 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 (for detailed information see Chapter 8: Administration of Workstations).
- 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 (see detailed information in section Anti-Virus Scanning of Stations).

- 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 (for detailed information see section Viewing Workstation Statistics).
- 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 (see detailed information in Chapter 6: Anti-Virus Network Administrators).
- 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 (for detailed information see section License Manager).
- 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 (for detailed information see Chapter 10: Configuring Dr.Web Server).

Detailed information on installation options for anti-virus protection is given in the **Installation 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 the **Installation Manual**, 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

Protects computers from unauthorized external access and prevents leaks of sensitive data via the internet. Monitors connection attempts and data transfer via the internet and blocks suspicious 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

Protects a mobile device from unauthorized external access and prevents sensitive data from leaking over the internet. Monitors connection attempts and data transfer over the internet and blocks suspicious connections on both 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. 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/. Your request will be considered individually. If it is approved, an archive with license key files will be sent to the specified email address.

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

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

3.1. Licensing Details

1. Dr.Web Server does not require a license.

The Dr.Web Server UUID, which was stored in the Dr.Web Server license key in the previous versions of Dr.Web Enterprise Security Suite, is stored in the Dr.Web Server configuration file starting from version 10.

- When a new Dr.Web Server is installed, a new UUID is generated.
- When Dr.Web Server is upgraded from an earlier version, its UUID is automatically taken from the configuration file of the previous version and written to the configuration file of Dr.Web Server being installed.

When updating a cluster of Dr.Web Servers, the license key is received by the Server which is used for database updates. For other Dr.Web Servers it is necessary to add license keys manually.

2. License keys only apply for protected stations. You can assign a license either to individual stations or to station groups: in this case, a license key is valid for all stations that inherit it from this group. To assign a key file simultaneously to all stations of the anti-virus network, for which no personal settings of the license key are specified, assign the license key to the **Everyone** group.
3. A license key file can be set during the installation of Dr.Web Server (see **Installation Manual**, section Installing Dr.Web Server).

   However, Dr.Web Server can be installed without a license key. A license can be added later either locally or received via the inter-server communication.
4. Using the inter-server communication, any number of licenses associated with the keys at this Dr.Web Server can be donated to a neighboring Dr.Web Server for a specified time period.
5. You can use several different licenses, for example with different expiration dates or different sets of anti-virus components for protected stations. Each license key can be

assigned to several licensing objects (groups and stations) simultaneously. Several license keys can be simultaneously assigned to one licensing object.

6. Please consider the following when assigning multiple keys to an object:
   a) If several keys are assigned to an object, each for a different set of anti-virus components, then the list of components, that can be installed on this object, is defined as those that are enabled by all said keys. For example, if two keys are assigned to a group of stations, one with Anti-spam support and the other without Anti-spam support, then the Anti-spam module cannot be installed on the stations.
   b) Licensing terms for an object are determined by all the keys assigned to it. If the keys have different expiration dates, then you need to manually remove or renew a key after it expires. If the expired key imposed limitations on the installation of anti-virus components, please change the licensing settings for the object in the Installable Components section.
   c) The number of licenses associated with an object is determined as the sum of licenses in all the keys assigned to this object. Please note, that the licenses can be donated via the inter-server connection to a neighboring Dr.Web Server (see para. 4). In this case, you should subtract the licenses donated to a neighboring Dr.Web Server from the total number of licenses.

License keys are managed using the License Manager.

When specifying a license key in the License Manager, all information about this license is saved in the database.

3.2. Donating Licenses Using Inter-server Connections

In an anti-virus network with several Dr.Web Servers, an optional number of licenses can be donated between Dr.Web Servers for a certain period of time.

To be able to donate the licenses between Dr.Web Servers, please configure inter-server connections as described in section Setting Connections between Several Dr.Web Servers.

Licenses can be donated for the following types of neighbor relationships:

- The parent Dr.Web Server donates licenses, the child Dr.Web Server receives licenses according to the license allocation settings (cannot be changed).
- Donating licenses between peer Dr.Web Servers. In this case, set the **Send** flag in the **Licenses** section of the connection settings for the Dr.Web Server that donates licenses; and set the **Receive** flag for the Dr.Web Server that receives licenses.

Configuring the donor Dr.Web Server

1. Open the Control Center of the Dr.Web Server on the anti-virus network that will donate licenses to neighboring Dr.Web Servers.

2. Select **Administration** in the main menu of the Control Center, then select **License Manager** in the control menu.
3. Add a license key, as described in the License manager section, if no key has been added earlier. The number of licenses in the key must correspond to the total number of stations protected by both this Dr.Web Server and all Dr.Web Servers that will get licenses from this key.

   Generally, you can have only one license key, the licenses from which will be allocated to all Dr.Web Servers.
4. Count the number of licenses that you can donate to neighboring Dr.Web Servers using this key. Note that neighboring Dr.Web Servers can also donate a number of licenses to other Dr.Web Servers. In this case, you need to donate a total number of licenses from the key installed on the parent Dr.Web Server that is equal to the number of licenses to be allocated further along the chain. Please note, that the parent Dr.Web Server will not be able to use the donated licenses until the end of the license allocation period and their return.
5. Configure the donation of licenses to neighboring Dr.Web Servers from the license key, as described in the License Manager section.

   In the **License expiration date** field, specify the expiration date for the donated licenses. The donation period can be either less than or equal to the validity period of the license itself. At the end of the specified period, all licenses will be reclaimed from neighboring Dr.Web Servers and returned to the pool of available licenses associated with the initial license key. If necessary, you can edit this period at any time, as described in the License Manager section.
6. If necessary, the settings of license donation can be changed. For this, open the **Dr.Web Server configuration** section.
7. On the **Licenses** tab, configure the following settings for the Dr.Web Server that donates licenses:
   - **Automatic renewal period of donated licenses**—a period of time for which licenses originating from the key on this Dr.Web Server are donated. After this period, the donated licenses are automatically renewed for the same period. Automatic renewal takes place before the expiration of the license donation period specified in the License Manager at step 5.
     This mechanism ensures that the licenses are returned to the parent Dr.Web Server in case the child Dr.Web Server is shut down and can't return the donated licenses.
   - **License synchronization period**—an interval at which the information about donated licenses is synchronized between Dr.Web Servers. License synchronization is used to verify that the number of licenses donated by the parent Dr.Web Server and received by the child Dr.Web Server is the same. This mechanism helps to detect malfunctions and fraud during licenses donation.
   - **Period of report creation**—an interval at which Dr.Web Server generates reports on the license keys used. If a report on license usage is generated by a child Dr.Web Server, it is then sent to the main Dr.Web Server. Created reports are additionally sent at each connection to Dr.Web Server (including its restart), and also when the number of donated

licenses is changed at the main Dr.Web Server. The setting is specified on the parent Dr.Web Server but is also used by the child Dr.Web Server when sending the reports.

- **Period of active stations counting**—a period of time during which the number of active stations will be counted and then included in the license usage report. If set to "0", all stations will be included in the report regardless of their activity status. The setting is specified on the parent Dr.Web Server but is also used by the child Dr.Web Server when sending the reports.

8. Save the changes and restart Dr.Web Server.

Configuring the recipient Dr.Web Server

1. Open the Control Center of the anti-virus network Dr.Web Server that will receive licenses from a neighboring Dr.Web Server.
2. If necessary, change the license allocation settings. To do this, open the **Dr.Web Server configuration** section.
3. On the **Licenses** tab, specify the **Interval for preliminary renewal of accepted licenses**—a time interval before the expiration of the scheduled renewal period for the license received from a neighboring Dr.Web Server. Starting from this period this Dr.Web Server will request the preliminary automatic renewal of these licenses.

   The use of this option depends on the type of connection selected in the **Connection options** setting in the configuration of the neighboring Dr.Web Server (see Setting Connections between Several Dr.Web Servers):

   - For the periodic connection: if the reconnection period specified in the connection options is greater than the **Automatic renewal period of donated licenses** specified on the donor Dr.Web Server, then the automatic renewal of these licenses will be initiated before the **Automatic renewal period of donated licenses** expires.
   - For the permanent connection: this option is not used.
4. Save the changes and restart Dr.Web Server.

3.3. Automatic License Renewal

Dr.Web Enterprise Security Suite license can be automatically renewed.

Automatic renewal of licenses implies the following:

- When a license key expires, it can be automatically replaced with a previously purchased license key.
- Automatic renewal is applicable to a specific license key for which the renewal has been purchased.
- The license key for the automatic renewal will be stored on the Doctor Web company servers until its expiration date.

Automatic license renewal procedure

The automatic license renewal procedure is initiated in the following cases:

- When the administrator clicks the **Check for updates and replace license keys** button on the toolbar in the License Manager of the Control Center.
- When the **Update repository** task from the Dr.Web Server schedule is running. Make sure that the **Update license keys** flag is set in the task settings.

> The license key is updated automatically only if the license to be renewed belongs to this Dr.Web Server, that is it was added manually or received via the automatic update. The automatic update procedure is not initiated for licenses received from neighboring Dr.Web Servers via the inter-server communications.

The automatic license renewal procedure consists of the following stages:

1. Checking the availability of a license key on Doctor Web company servers (GUS).
2. Downloading a license key from the GUS to Dr.Web Server and adding it to the database and the License Manager.
3. Allocating the new license key to the objects of the previous key.

Depending on the results of each stage, the procedure can be successfully completed at any of them.

The following results of the automatic update are possible:

1. *The license key for automatic update is absent on GUS.*

   No actions are performed.
2. The license key for automatic update is available on GUS. The list of components to be licensed is different in the current and the new keys (the new key does not apply to some components licensed by the key currently in use) or/and the new license key has fewer licenses than the current license key.

   A new license is downloaded from the Doctor Web company servers, it is then added to the License Manager and the Dr.Web Server database but not allocated to licensing objects. In this case, it is necessary to allocate a license key manually.

   The administrator will receive the **License key cannot be automatically updated** notification. The specific reason why the license key cannot be automatically propagated, is included in the notification.
3. The license key for automatic update is available on GUS. The list of components to be licensed is the same between the current and the new license key, or the new key is intended to license more components than the current key, alternatively, the number of licenses in the new license key exceeds or is equal to the number of licenses in the current license key.

A new license is downloaded from the Doctor Web servers, it is then added to the License Manager and the Dr.Web Server database and allocated to all licensing objects to which the previous license has been allocated, including neighboring Dr.Web Servers.

The old license is removed when it is not in use by any of the child Dr.Web Servers. Thus, if the child Dr.Web Server was offline at the moment of the automatic update, the old license will be stored until this child Dr.Web Server is connected.

The old license is stored until the administrator manually removes it in the following cases:

- If the license received during the automatic update cannot be allocated to the child Dr.Web Server (Dr.Web Server is always offline).
- If the child Dr.Web Server uses the old protocol version that does not support automatic updates. In this case, licenses will be donated to a neighboring Dr.Web Server but will not be propagated.

The administrator receives the **License key automatically updated** notification. Update notifications are sent from each Dr.Web Server that has received a new license.

All notifications that are sent to administrator, are managed in the **Administration** → **Notifications configuration** section.

The **Automatic update of a license key** user hook is executed after sending each notification.

Manual license renewal

If you purchased a license key for automatic renewal of your current key, you do not need to manually add a new key in the License Manager. Depending on the situation (variant 2 in the procedure above), you may need to allocate it to the licensing objects manually.

On the other hand, if you have used the License Manager to manually add a new key for automatic renewal prior to performing the automatic license renewal procedure, as described in variant 3 (see the procedure above), then the task will only propagate a new license key. In this case, the following variants are possible:

a) A new license key has been allocated manually to all objects licensed by the previous key. In this case, no changes are made during the execution of the update task.

b) A new license key has not been allocated to all objects licensed by the previous key. In this case, during the execution of the update task, a new key will be allocated to all other objects of the previous key that still have not yet received the update.

   If a new license key has been manually allocated to objects that were not in the list of the previous key, then after execution of the task, a new key will remain allocated to these objects as well. In this case, the following variants are possible:

   - The number of licenses is sufficient for all licensing objects: for objects licensed with the previous key and for objects manually assigned to a new key. This situation can occur if a

new key contains more licenses. In this case no changes will be made during the update task.

- The number of licenses is not sufficient for all licensing objects assigned to the previous key, because licenses were manually assigned to other objects. Objects that did not receive a license will not be updated, however the previous key will be deleted anyway and the objects will remain unlicensed. When a license becomes available, all unlicensed objects will receive a new license key. In this case, the actions depend on the type of licensing objects:
  - If stations protected by this Dr.Web Server have not received licenses from a new key, then the available licenses are checked each time a station tries to connect to Dr.Web Server. If a license is available, it will be allocated to this station.
  - If a neighboring Dr.Web Server has not received licenses from a new key, then the available licenses are checked automatically approximately every minute. If there are licenses available, they will be donated to neighboring Dr.Web Servers.

License Key file

Please note the following features of automatic update:

- During the automatic update, a new license is downloaded from Doctor Web company servers, its information is stored in the Dr.Web Server database and is displayed in the License Manager. No license key file is created.
- To get a license key file, use the **Administration** → **License Manager** → **Export key** option. Also, a license key file can be obtained by executing the **Automatic update of a license key** user hook.
- When a license is revoked, its information is deleted from the License Manager and from the Dr.Web Server database; however, the license key file remains in the Dr.Web Server folder.

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 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 the **Installation Manual**, 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.

   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.

   For detailed guidelines on managing administrative groups and permissions see 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 the **Installation Manual**, 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 the **Installation Manual**, section Installing Dr.Web 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 the **Installation Manual**, 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 the **Installation Manual**, Installing Dr.Web Server for Unix-like OSs).

On successful connection to Dr.Web Server, the main window of the Control Center opens (for detailed description refer to 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 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 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 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 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 Configuring 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 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 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 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 Manual**, 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 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 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 the **Installation Manual**, 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, the following tools are created to ensure a secure connection between the components of the anti-virus network:

1. **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.

2. **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.

3. **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.

4. **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.

5. **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 Agent**

  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 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.

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

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

1. **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 **Installation Manual**, sections Installing Dr.Web Server for Windows OS and SRV Protocol.

2. **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 Setting Dr.Web Server Schedule.

3. **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 Authentication of Administrators.

4. **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 **Installation Manual**, section Installing Dr.Web Agent Software via Active Directory.

5. **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 in section 4.

   For more details, see the Network Scanner.

6. **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: Components of an Anti-Virus Network and Their Interface

5.1. Dr.Web Server

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

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

Dr.Web Server is a memory-resident component. Dr.Web Server software is developed for various OS (see **Installation Manual**, System Requirements).

Basic Functions

Dr.Web Server performs the following tasks:

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

Collecting Information on Anti-Virus Network

Communicating with Dr.Web Agents, Dr.Web Server collects and logs information on operation of the anti-virus packages. Information is logged in the general log file implemented as a database. In small networks (no more than 400–600 computers) an embedded database can be used. In larger networks it is recommended to use an external database.

The embedded DB is intended for use in networks where about 400–600 stations are connected to Dr.Web Server. If the hardware configuration of the computer on which Dr.Web Server is installed and the load level of other executing tasks permit, between 1000 and 1500 stations can be connected.

Otherwise, you must use an external DB. Depending on the configuration and the load level of the computer running Dr.Web Server, the external DB may be used on the same or on a dedicated computer.

If you use an external DB in an anti-virus network with more than 10 000 stations, it is recommended to follow these minimal system and hardware requirements:

- 3 GHz processor CPU,
- at least 6 CPU cores,
- at least 4 GB RAM for Dr.Web Server and at least 8 GB RAM for the DB server,
- Unix-like OS.

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

- versions of the anti-virus packages on protected computers,
- time and date of the anti-virus software installation and update on workstations with the software versions,
- time and date of virus databases updates with its versions,
- OS versions of protected computers, processor type, location of OS system folders, etc.,
- configuration and settings of anti-virus packages operation,
- information on events related to threats, including names of detected threats, detection dates, actions, results of curing, etc.

Dr.Web Server notifies the administrator on events related to threats on protected computers by email or through the Windows OS standard broadcast notification system. You can set the alerts as described in p. Setting Alerts.

Web Server

Web server is a part of Dr.Web Security Control Center and performs the following general functions:

- authentication and authorization of administrators in the Control Center;
- automation of Control Center pages operation;
- support for dynamically generated pages of Control Center;
- support for HTTPS-protected client connections.

5.1.1. Dr.Web Server Management under Windows OS

Dr.Web Server Interface and Management

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

Elements for configuration and management Dr.Web Server are placed during the installation to the **Programs** main Windows OS menu, to the **Dr.Web Server** folder:

- The **Dr.Web Server control** folder contains the following commands:
  - **Detailed logging**—set the **All** level of detail for the Dr.Web Server operation log.
  - **Start**—start the Dr.Web Server service.
  - **Stop**—stop the Dr.Web Server service.
  - **Reload repository**—reread the Dr.Web Server repository from disk.
  - **Reload templates**—reread the administrator notifications templates.
  - **Restart**—restart the Dr.Web Server service.
  - **Verify database**—start the verification of the embedded database.
  - **Default logging**—set the **Information** level of detail for the Dr.Web Server operation log.

  After the execution of the **Detailed logging** and **Default logging** commands, the service must be restarted to apply changes. For this, run the **Restart** command.

  Extended logging settings are available in the Log section of the Control Center.

  Corresponding commands are described in detail in the **Appendices** document, G2. Dr.Web Agent for Windows.
- The **Web interface** item opens Dr.Web Security Control Center and connects to Dr.Web Server installed at this computer (at the http://localhost:9080).
- The **Documentation** item opens administrator documentation in HTML format.

Dr.Web Server folder has the following structure:

Default installation folder (can be changed during the installation): `C:\Program Files\DrWeb Server`

- `bin`—Dr.Web Server executable files.
- `ds-modules`—unpacked script modules.
- `etc`—general configuration files of anti-virus network components.
- `fonts`—fonts for PDF documents.

- `var`—contains the following subfolders:
  - `backup`—backups of DB and other critical data.
  - `extensions`—scripts of user hooks meant to automate the performance of certain tasks.
  - `file-cache`—file cache.
  - `installers-cache`—cache to store Dr.Web Agent personal and group installation packages when stations are created via the Control Center. Created at installation packages creation.
  - `plugins`—temporary plug-ins objects.
  - `objects`—Control Center objects cache.
  - `reports`—temporary folder for generating and storing reports. Created when necessary.
  - `repository`—repository folder to store actual updates of virus databases, anti-virus packages files and anti-virus network components. It contains subfolders for the program components software which include subfolders for their versions depending on the OS. The folder should be accessible for writing to the user under which Dr.Web Server is launched (the **LocalSystem** as a rule).
  - `sessions`—Control Center sessions.
  - `tmp`—temporary files.
  - `twin-cache`—unpacked virus databases for backward compatibility with previous versions of Dr.Web Agents. Also, can contain other unpacked repository files, e.g., the Dr.Web Agent installer.
  - `upload`—folder to download temporary files which are specified via the Control Center. Created at large files downloading.
- `vfs`—packed script modules and language packages.
- `webmin`—Control Center elements.
- `websockets`—web sockets scripts.

Backup folder (can be changed during the deinstallation): <*installation_drive*>`:\Drweb Backup`.

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

General Configuration Files

File	Description	Default folder
`agent.key` (name may vary)	Dr.Web Agent license key	`etc`

File	Description	Default folder
certificate.pem	SSL certificate	
database.conf	default database settings with which Dr.Web Server was installed. Required to return to default settings if other database settings are used. Created after the first editing of the **Dr.Web Server Configuration** → **Database** section.	
download.conf	network settings for generating of the Dr.Web Agent installation packages	
drwcsd.conf (name may vary)	Dr.Web Server configuration file	
drwcsd.conf.distr	Dr.Web Server configuration file template with default parameters	
drwcsd.pri	private encryption key	
enterprise.key (name may vary)	Dr.Web Server license key file. The file is saved if it presented after the upgrade from the previous versions. For the new Dr.Web Server 13.0installation, the file is absent	
frontdoor.conf	configuration file for the Dr.Web Server remote diagnostic utility	
http-alerter-certs.pem	certificates for verification the apple-notify.drweb.com host for sending push notifications	
private-key.pem	RSA private key	
yalocator.apikey	API key for the Yandex.Locator extension	
webmin.conf	Control Center configuration file	
auth-ads.conf	configuration file for administrators external authorization via Active Directory	
auth-ldap.conf	configuration file for administrators external authorization via LDAP	
auth-ldap-rfc4515.conf	configuration file for administrators external authorization via LDAP using the simplified scheme	
auth-radius.conf	configuration file for administrators external authorization via RADIUS	
database.sqlite	embedded database	var

File	Description	Default folder
`*.pub`	public encryption key	**Administration** → **Encryption keys** in the Control Center

Start and Stop Dr.Web Server

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

Also you can start or start, restart or stop Dr.Web Server by one of the following ways:

- General case:
  - Using the corresponding command, located in the **Start** → **Programs** → **Dr.Web Server** menu.
  - Via the services management tools in the **Administrative Tools** section at the **Control Panel** of Windows OS.
- Stop and restart via the Control Center:
  - In the **Administration** section, use buttons:  to restart,  to stop.
- Using the console commands run from the `bin` subfolder of the Dr.Web Server installation folder (see also the **Appendices** document, G3. Dr.Web Server):
  - `drwcsd start`—start Dr.Web Server.
  - `drwcsd restart`—total restart of the Dr.Web Server service.
  - `drwcsd stop`—normal shutdown of Dr.Web Server.

Please note, if you need Dr.Web Server to read environment variables, the service must be rebooted via the services management tools or via the console command.

5.1.2. Dr.Web Server Management under Unix-like OS

Interface and Dr.Web Server Management

Dr.Web Server has no interface. As a rule, Dr.Web Server can be managed via Dr.Web Security Control Center, which acts as an interface for Dr.Web Server.

Dr.Web Server installation folder has the following structure:

`/opt/drwcs/` for Linux OS and `/usr/local/drwcs` for FreeBSD OS:

- `bin`—Dr.Web Server executable files.

- `doc`—license agreements files.
- `ds-modules`—unpacked script modules.
- `fonts`—fonts for PDF documents.
- `lib`—libraries set for the Dr.Web Server operation.
- `vfs`—packed script modules and language packages.
- `webmin`—Control Center elements.
- `websockets`—web sockets scripts.

`/var/opt/drwcs/` for Linux OS and `/var/drwcs` for FreeBSD OS:

- `backup`—backups of DB and other critical data.
- `coredump`—Dr.Web Server crash dumps. Created at dumps appearance.
- `etc`—general configuration files of anti-virus network components.
- `extensions`—scripts of user hooks meant to automate the performance of certain tasks.
- `installers-cache`—cache to store Dr.Web Agent personal and group installation packages when stations are created via the Control Center. Created at installation packages creation.
- `file-cache`—file cache.
- `log`—Dr.Web Server log files.
- `plugins`—temporary plug-ins objects.
- `objects`—Control Center objects cache.
- `reports`—temporary folder for generating and storing reports. Created when necessary.
- `repository`—repository folder to store actual updates of virus databases, anti-virus packages files and anti-virus network components. The folder contains subfolders for the program components software which include subfolders for their versions depending on the OS. The folder should be accessible for writing to the user under which Dr.Web Server is launched (the **drwcs** as a rule).
- `run`—Dr.Web Server process ID.
- `sessions`—Control Center sessions.
- `tmp`—temporary files.
- `twin-cache`—unpacked virus databases for backward compatibility with previous versions of Dr.Web Agents. Also, can contain other unpacked repository files, e.g., the Dr.Web Agent installer.
- `upload`—folder to download temporary files which are specified via the Control Center. Created at large files downloading.

`/etc/opt/drweb.com/` for Linux OS and `/usr/local/etc/drweb.com` for FreeBSD OS:

- `software/drweb-esuite.remove`—script to remove Dr.Web Server.
- also additional files and folders are possible.

/usr/local/etc/rc.d/ for FreeBSD OS:

- drwcsd—script to start and stop Dr.Web Server.

/var/tmp/drwcs—backup after the Dr.Web Server removal.

General Configuration Files

File	Description	Default folder
agent.key (name may vary)	Dr.Web Agent license key	• for Linux OS: /var/opt/drwcs/etc • for FreeBSD OS: /var/drwcs/etc
certificate.pem	SSL certificate	
common.conf	configuration file (for some of Unix-like OS)	
database.conf	default database settings with which Dr.Web Server was installed. Required to return to default settings if other database settings are used. Created after the first editing of the **Dr.Web Server Configuration → Database** section.	
download.conf	network settings for generating of the Dr.Web Agent installation packages	
drwcsd.conf (name may vary)	Dr.Web Server configuration file	
drwcsd.conf.distr	Dr.Web Server configuration file template with default parameters	
drwcsd.pri	private encryption key	
enterprise.key (name may vary)	Dr.Web Server license key file. The file is saved if it presented after the upgrade from the previous versions. For the new Dr.Web Server 13.0 installation, the file is absent	
frontdoor.conf	configuration file for the Dr.Web Server remote diagnostic utility	
http-alerter-certs.pem	certificates for verification the apple-notify.drweb.com host for sending push notifications	
private-key.pem	RSA private key	
yalocator.apikey	API key for the Yandex.Locator extension	

File	Description	Default folder
`webmin.conf`	Control Center configuration file	
`auth-ldap.conf`	configuration file for administrators external authorization via LDAP	
`auth-ldap-rfc4515.conf`	configuration file for administrators external authorization via LDAP using the simplified scheme	
`auth-pam.conf`	configuration file for administrators external authorization via PAM	
`auth-radius.conf`	configuration file for administrators external authorization via RADIUS	
`database.sqlite`	embedded database	• for Linux OS: `/var/opt/drwcs` • for FreeBSD OS: `/var/drwcs`
`*.pub`	public encryption key	**Administration** → **Encryption keys** in the Control Center

Start and Stop Dr.Web Server

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

Also you can start or start, restart or stop Dr.Web Server by one of the following ways:

- Stop and restart via the Control Center:
  - In the **Administration** section, use buttons: to restart, to stop.
- Using the corresponding console command (see also the **Appendices** document, G3. Dr.Web Server):
  - Start:
    - for FreeBSD OS:
      ```
      # /usr/local/etc/rc.d/drwcsd start
      ```
    - for Linux OS:
      ```
      # /etc/init.d/drwcsd start
      ```
  - Restart:
    - for FreeBSD OS:
      ```
      # /usr/local/etc/rc.d/drwcsd restart
      ```
    - for Linux OS:
      ```
      # /etc/init.d/drwcsd restart
      ```

- Stop:
  - for FreeBSD OS:
    ```
    # /usr/local/etc/rc.d/drwcsd stop
    ```
  - For Linux OS:
    ```
    # /etc/init.d/drwcsd stop
    ```

Please note, if you need Dr.Web Server to read environment variables, the service must be rebooted via the console command.

5.2. Workstations Protection

Detailed description of anti-virus components settings which are configured via the Control Center, is given in the **Administrator Manual** on managing stations for corresponding operating system.

Protected computer with installed anti-virus package as per its functions in the anti-virus network is called a workstation of anti-virus network. Please note: according to its LAN functions, such computer can be both a workstation or mobile device and a LAN server.

Workstations are protected by Dr.Web anti-virus packages designed for correspondent operating systems.

Anti-virus packages are installed on protected stations and get connected to Dr.Web Server. Each station is included in one or several groups registered on this Dr.Web Server (for more, see p. System and User Groups). Stations and Dr.Web Server communicate through the protocol used in the local network (TCP/IP of 4 or 6 version).

Installation

Anti-virus package can be installed on a workstation by one of the following ways:

1. Locally. Local installation is performed directly on a user's computer or mobile device. Installation may be implemented either by administrator or by user.
2. Remotely. Remote installation is performed from the Control Center through via LAN. Installation is implemented by an anti-virus network administrator. Therefore, no user involvement is required.

Detailed description of anti-virus packages installation procedures on workstations you can find in the **Installation Manual**.

Management

When connection with Dr.Web Server is established, administrator is able to use the following functions implemented by anti-virus package on a station:

- Centralized configuration of Anti-virus on workstations via the Control Center.

  At this, administrator can either deny or grant user's permissions to change Anti-virus settings on stations on one's own.
- Configure the schedule for anti-virus scans and other tasks to execute on a station.
- Get scan statistics and other information on anti-virus components operation and on station states.
- Start and stop anti-virus scans and etc.

Update

Dr.Web Server downloads updates and distributes them to connected stations. Thus, optimal threats protection is implemented, maintained and adjusted automatically regardless of workstation users' computer skills.

In case an anti-virus station is disconnected from the anti-virus network, Anti-virus on station uses the local copy of the settings and the anti-virus protection on a workstation retains its functionality (up to the expiry of the user's license), but the software is not updated. If a station is allowed to use the *mobile mode*, after connection with Dr.Web Server is lost, the virus databases can be updated directly from the GUS.

The principle of operation of stations in mobile mode is described in the Updating Dr.Web Agents in Mobile Mode section.

5.3. Dr.Web Security Control Center

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

For correct functioning of Dr.Web Security Control Center under Windows Internet Explorer browser, you must add Dr.Web Security Control Center address to the list of trusted sites in the web browser settings: **Tools** → **Internet Options** → **Security** → **Trusted Sites**.

For correct functioning of Dr.Web Security Control Center under Chrome browser, you should turn on cookies.

Connecting to Dr.Web Server

From any computer with network access to Dr.Web Server, Dr.Web Security 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 an IP address or domain name of a computer on which Dr.Web Server is installed.

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

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

Lost password can be restored, see Restoring Administrator Password.

If you connect through HTTPS protocol (secure SSL connection), the browser requests you to approve the Dr.Web Server certificate. Warnings and indications of distrust to the certificate may display, because the certificate is unknown to your browser. You need to approve the certificate to connect to Dr.Web Security Control Center. Otherwise, connection will be failed.

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

Dr.Web Security Control Center Interface

Dr.Web Security Control Center window (see figure 5-1) is divided in *main menu header* and *working area*.

Main menu

The main menu consists of the following items:

- Administration section,
- Anti-virus network section,
- Search panel,
- the name of the current administrator logged into Dr.Web Security Control Center. Also, the interserver connections menu may be available,
- Events section,
- Preferences section,
- Help section,
- **Log out** to close the current Dr.Web Security Control Center session.

Working Area

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

- the control menu is always located in the left part of the working area,
- depending on the selected item, one or two additional panels are displayed. In the latter case, the rightmost panel contains the settings of elements from the central panel.

The interface language must be set individually for each administrator account (see p. Creating and Deleting Administrative Accounts and Groups).

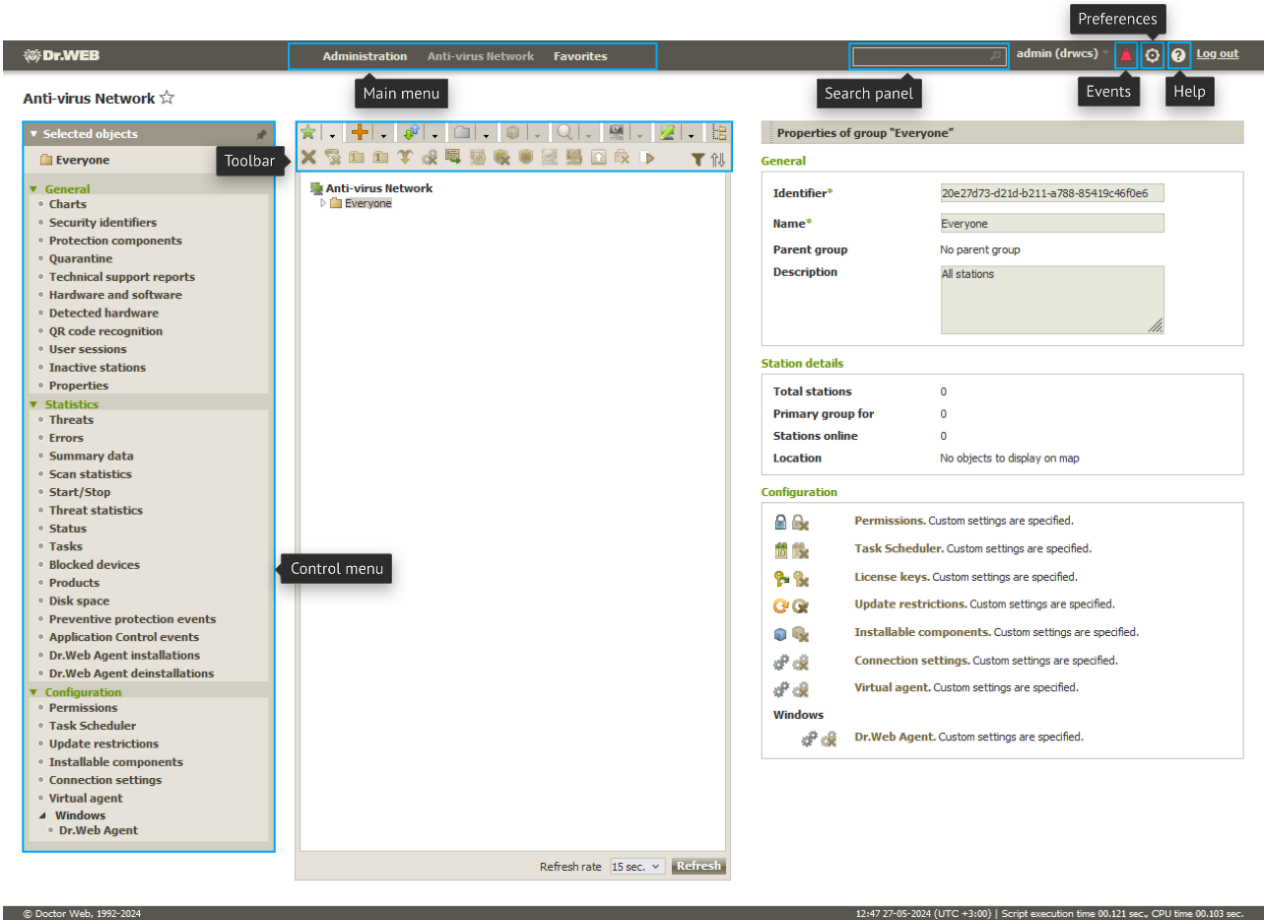


Figure 5-1. Dr.Web Security Control Center window. Click an element tag to open the corresponding section

Control Menu

To view and edit the information in the opened window, use the control menu resided in the left part of the window.

The control menu can be minimized. At this, only section names of the menu are displayed. On mouse over the correspondent section, available menu options of this section will be displayed.

To manage the control menu displaying, you the following icons in the upper right corner:

- **Unpin menu** – disable pinning and display the menu in the minimized view.
- **Pin menu** – pin maximized menu position.

Interserver Connections Menu

Information on multiserver anti-virus networking and neighbor configuration can be found in the Peculiarities of a Network with Several Dr.Web Servers section.

If interserver connections between Dr.Web Servers are configured, the following features are added to administrator login area in the main menu.

- Name of current Dr.Web Server is shown next to administrator login.
- Clicking on administrator login opens drop-down list with connected neighbor Dr.Web Servers. If a neighbor name is not specified, its identifier will be shown instead.

  Clicking on neighbor can have two possible outcomes:
  - The Control Center of a neighbor Dr.Web Server will open, if IP address of the Control Center was specified as a part of connection configuration.
    The action is similar to clicking the → button on the toolbar when managing neighbors.
  - If the Control Center address of this neighbor Dr.Web Server is not set, neighbor setup section will open for you to specify the IP address.

5.3.1. Administration

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

Control Menu

To view and edit the information in the opened window, use the control menu resided in the left part of the window.

The control menu contains the following items:

1. **Administration**

   - **Dr.Web Server**—opens the panel which shows basic information about Dr.Web Server and lets you restart or shutdown it via the and buttons in the top right part of the panel. Also if Dr.Web Server has updates downloaded, from this section you can access the Dr.Web Server Updates section with the Dr.Web Server version list to update and back up. To restore the integrity of Dr.Web Server and roll back to the state of current revision click the **Restore Server** button.
   - **Encryption keys**—allows to export (save locally) public and primary encryption keys and also the Dr.Web Server certificate.

2. **Licenses**

   - License Manager—allows to manage the license key files.
   - License usage report—contains information on licenses usage, including neighbor Dr.Web Servers.

3. **Logs**

   - Real time log—allows to view the list of events and changes on the Dr.Web Server operation and displayed in real time (at the moment of an event appearance).
   - Audit log—allows to view the list of events and changes carried via the control subsystems of Dr.Web Enterprise Security Suite.
   - **Tasks execution log**—contains the list of Dr.Web Server tasks with completion marks and comments.
   - Dr.Web Server log—contains the list of events on the Dr.Web Server operation.
   - Log of repository updates—contains the list of updates from GUS, that includes detailed information on updated products revisions.
   - Message Log—contains all text messages that were sent by administrator to stations of the anti-virus network.
   - **Log of abnormally terminated connections**—contains all cases of abnormally terminated connections of Dr.Web Server with clients: stations, the Dr.Web Agent installers, neighbor Dr.Web Servers, Proxy Servers.

4. **Configuration**

   - Administrators—opens the panel for managing anti-virus network administrator accounts.
   - Authentication—opens the panel to manage authentication methods of Dr.Web Security Control Center administrators (see Authentication of Administrators).
   - Dr.Web Server configuration—opens the panel with main settings of Dr.Web Server.
   - Dr.Web Server remote access—contains settings for connecting Server remote diagnostics utility.
   - Dr.Web SNMP Agent Configuration—opens the panel to configure parameters for connecting to Dr.Web SNMP agent.
   - Dr.Web Server Task Scheduler—opens the panel with the Dr.Web Server task scheduler settings.
   - Web server configuration—opens the panel with general settings of the Web server.
   - User hooks—opens the panel with User hooks settings.

5. **Notifications**

   - Web console notifications—allows to view and manage administrator notifications which are received via the **Web console** method.
   - Unsent notifications—allows to track and manage administrative notifications failed to be sent according to the settings of the **Notification Configuration** section.
   - Notifications configuration—allows to configure administrative notifications on anti-virus network events.

- Message Templates—the templates list of arbitrary text messages sent by administrator to stations of the anti-virus network.

6. **Repository**

- Repository state—allows to check repository state: date of last update of repository components and their state. And also, update repository from GUS.
- Delayed updates—contains the list of products that are temporary disabled for updating in the **Detailed repository configuration** section.
- General repository configuration—opens the window to configure settings of connection to the GUS and repository updates for all products.
- Detailed repository configuration—allows to setup revisions configuration for each repository product separately.
- Repository content—allows to view and manage current repository content as files and folders of repository folder.
- **Known hashes of threats**—allows to search in bulletins with known hashes of threats. To search in the hash table fields, click .
  The section is available only if the usage of bulletins of known threat hashes is licensed. You can check the license in the information on a license key that can be found in the License Manager section, the **Allowed lists of hash bulletins** parameter (the license in at least one of the license keys used by Dr.Web Server is sufficient).

7. **Installations**

- Network Scanner—allows to specify a list of networks, search for installed anti-virus software in networks to determine protection status of computers, and install anti-virus software.
- **Network installation**—allows to simplify installation of the Dr.Web Agent software on certain workstations (see **Installation Manual**, Installing Dr.Web Agent Software via Dr.Web Security Control Center).

8. **Application Control**

- Trusted applications—the lists of applications the launch of which is always allowed on stations with Application Control component (the selection of allowed lists is performed in the settings of the profile assigned to stations).
- Application catalog—the list of applications installed on stations.

9. **Additional features**

- Database management—allows direct maintenance of the Dr.Web Server database.
- Dr.Web Server statistics—contains statistics of this Dr.Web Server operating.
- **SQL console**—allows to execute SQL queries to the database which Dr.Web Server uses.

- **Lua console**—allows to execute Lua scripts both typed in the console directly or loaded from a file.

Together with the access to the Lua console, administrator gets the access to all file system within the Dr.Web Server folder and some system commands on a computer with Dr.Web Server installed.

To forbid the access to the Lua console, disable the **Use additional features** permission for the correspondent administrator (see Administrators and Administrative groups).

- Backups—allows to view and save backups composition of the Dr.Web Server critical data.
- Utilities—opens the section with additional utilities for interaction with Dr.Web Enterprise Security Suite.

5.3.2. Anti-Virus Network

Select the **Anti-virus network** item in the main menu of Dr.Web Security Control Center.

Control Menu

To view and edit the information in the window that opens, use the control menu found in the left part of the window.

The control menu contains the following components:

1. **General**
   - Charts
   - Security identifiers
   - Protection components
   - Quarantine
   - Hardware and software
   - **Detected devices**
   - **User sessions**
   - **Inactive stations**
   - Properties
   - Group membership rules (when user groups are selected)
   - Dr.Web Proxy Server (when Dr.Web Proxy Servers or their group are selected)
2. Statistics
3. **Configuration**
   - Dr.Web Proxy Server (when a Dr.Web Proxy Server or the **Proxies** group and its subgroups are selected)

- Permissions
- Task Scheduler
- Installable components
- Connection parameters
- Virtual environments
- Update Restrictions
- List of anti-virus components for the operating system of the selected station or operating systems when a group is selected.

A detailed description of the settings of anti-virus components which are configured via the Control Center is given in the **Administrator Manuals** on managing stations for the corresponding operating systems.

Hierarchical list of the anti-virus network

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

You can perform the following using the hierarchical list elements:

- Left-click the name of a group or station to display the control menu of the corresponding element (in the left part of the window) as well as brief information on the station on the property pane (in the right part of the window).
- Left-click the icon of a group to open or hide the contents of the group.
- Left-click the icon of a station to open the properties sheet of this station.

To select multiple elements of the hierarchical list, press and hold CTRL or SHIFT during selection.

The appearance of an icon depends on the type and status of this element (see table 5-1).

Table 5-1. Icons of elements in the hierarchical list

Icon	Description
Groups. General icons	
	Groups always shown in the hierarchical list.
	Groups are not displayed in the hierarchical list if:

Icon	Description
	• the **Setup group visibility** → **Hide if empty** option is set and the groups do not contain any stations at the moment, • the **Setup group visibility** → **Hide** option is set and the **Show hidden groups** flag in the **Settings of tree view** section is cleared at the moment.
	The membership rules icon is displayed next to the main icon of the user groups that have rules for automatic station placement in the group. To display the icon, select the **Settings of tree view** → **Show membership rules icon** option on the toolbar.
Workstations. Main icons	
	Available workstation with installed anti-virus software.
	Available workstation with installed anti-virus software. Severity of the station state is **Medium**. To determine the required administrator actions, please clarify the situation on this station in the Status section. To display the icon, select the **Settings of tree view** → **Show station states severity** option on the toolbar.
	Available workstation with installed anti-virus software. Severity of the station state is **Maximal** or **High**. To determine the required administrator actions, please clarify the situation on this station in the Status section. To display the icon, select the **Settings of tree view** → **Show station states severity** option on the toolbar.
	Station is unavailable.
	Anti-virus software on the station is uninstalled.
	Access of the station to Dr.Web Server is blocked.
	Station state during remote network installation of Dr.Web Agent. Station is in this state from the moment of successful Dr.Web Agent installation on the station until the moment of its first connection to Dr.Web Server.
Dr.Web Proxy Servers. Main icons	
	Proxy Server is not connected to your Dr.Web Server.
	Proxy Server is connected to your Dr.Web Server, but it does not use the specified settings.
	Proxy Server is connected to your Dr.Web Server, and it uses the specified settings.
Scanning Servers. Main icons	
	Available Scanning Server.

Icon	Description
	Available Scanning Server. Severity of the state is **Medium**. To determine the required administrator actions, please clarify the situation on this Scanning Server in the Status section. To display the icon, select the **Settings of tree view** → **Show station states severity** option on the toolbar.
	Available Scanning Server. Severity of the state is **Maximal** or **High**. To determine the required administrator actions, please clarify the situation on this Scanning Server in the Status section. To display the icon, select the **Settings of tree view** → **Show station states severity** option on the toolbar.
	Scanning Server is unavailable.
Additional icons for groups, stations, Proxy Servers, and Scanning Servers	
	The personal settings icon is displayed over the main icons of stations, groups, Proxy Servers, and Scanning Servers with personal settings. To display the icon, select the **Settings of tree view** → **Show personal settings icon** option on the toolbar. E.g., if personal settings are specified for an online workstation with anti-virus software installed, its icon looks like this:  .
Policies	
	Policy or policy version with settings of anti-virus components on stations. To display the icon, select the **Settings of tree view** → **Show policy icon** option on the toolbar.
Profiles	
	Profile for storing Application Control settings, active mode.
	Profile for storing Application Control settings, test mode.
	Disabled profile for storing Application Control settings.
	Profile for storing Application Control settings when a specified group of trusted applications is missing in the Dr.Web Server repository.

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

Toolbar

The toolbar of the hierarchical list contains the following elements:

General—manage the general parameters of the hierarchical list. Select the corresponding item in the drop-down list:

Remove selected objects—remove items from the hierarchical list. Select the items in the list and click **Remove selected objects**.

Remove membership rules—remove rules for automatic inclusion of stations to groups.

Set this group as primary—set the selected group as primary for all workstations in it.

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

Merge stations—join workstations under a single account in the hierarchical list. Can be used if a workstation was registered under several accounts.

Remove personal settings—remove individual settings of the selected objects. The settings of the parent group will be used instead. If a group is selected, all workstations within the group will also have their settings removed.

Send message to stations—send a message with an arbitrary content to users of workstations.

Reboot station—restart a station remotely. You can determine whether the station needs a reboot, e.g. after updating/changing the anti-virus components, in the Status section for this station.

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

Install Dr.Web Agent—open the Network Scanner to install Dr.Web Agent on stations with uninstalled Dr.Web Agent. This item is enabled only if stations with uninstalled Dr.Web Agent are selected in the anti-virus network tree.

Install Dr.Web Agent using Network Scanner—open the Network Scanner to install Dr.Web Agent on selected stations (installation with selected IDs). This item is enabled only if new station accounts are selected in the anti-virus network tree.

Restore deleted stations—restore previously deleted stations. This option is active only if stations from the **Deleted** subgroup of the **Status** group are selected.

Mail installation files—send the installation files for stations selected in the list to the email addresses specified in the parameters of this section.

Unassign the profile from the objects—delete a profile from the list of profiles assigned to the selected objects. The option is active when selecting objects with an assigned profile (displayed in the tree as the nested objects of this profile).

Create a technical support report—create a technical support report with system information on a station or group of stations.

Add a network object—add a new element to the anti-virus network. Click the corresponding item in the drop-down menu:

- **Create station**—add a new station (see the **Installation Manual**, Installing Dr.Web Agent via the Personal Installation Package).
- Create group—add a new group.
- Create neighbor—add a neighbor Dr.Web Server connection.
- Create policy—add a new policy to set station settings.
- **Create Proxy Server**—add a new account for connecting the Proxy Server (see the **Installation Manual**, Creating Dr.Web Proxy Server Account).
- Create profile—add a new profile to store the settings of anti-virus components on stations.

Data and configuration:

- **Save data in CSV file**—write the general data about the selected anti-virus network stations to a CSV file.
- **Save data in HTML file**—write the general data about the selected anti-virus network stations to an HTML file.
- **Save data in XML file**—write the general data about the selected anti-virus network stations to an XML file.
- **Save data in PDF file**—write the general data about the selected anti-virus network stations to a PDF file.

> The options from the **Data and configuration** section listed above export information only on the selected stations and stations included into the selected groups.

- **Export configuration**—save the configuration of the selected anti-virus network objects to a file. You will be prompted to select the configuration sections to save.
- **Import configuration**—load the configuration of the selected anti-virus network objects from a file. You will be prompted to select the file to load the configuration from and the configuration sections to be loaded.
- **Export statistics**—save the anti-virus component statistics for the selected anti-virus network objects to a file. You will be prompted to select the statistics sections to save and the export format.
- **Propagate configuration**—propagate the configuration of the selected objects to other anti-virus network objects. You will be prompted to select the objects to propagate configurations to and the configuration sections to be propagated.
- **Assign policy**—assign the selected policy to a group or individual stations. You will be prompted to select the objects to assign the policy to.
- Assign profile—assign the settings profile selected in the anti-virus network tree to objects: stations, users, and groups. You will be prompted to select the objects to assign the profile to.

Setup group visibility—change the appearance of groups in the list. Select one of the following in the drop-down list (the icon of the group will change, see table 5-1):

Hide—the group will not be displayed in the hierarchical list.

Hide if empty—the group will not be displayed if it is empty (does not contain any workstations).

Show—the group will always be displayed in the hierarchical list.

Components management—manage the components on a workstation. Select the necessary action in the drop-down menu:

Recover failed components—force to recover the state of the components operating with errors. Recovery uses the product revision that is currently installed on the station.

Interrupt running components—stop all running anti-virus components on the station. You can stop and start anti-virus components separately in the Protection Components section.

Scan—scan stations in one of the modes selected in the drop-down menu:

Express scan. The following objects are scanned by Dr.Web Agent Scanner in this mode:

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

Full scan. In this mode all hard disks and removable disks (including the boot sectors) will be fully scanned by Dr.Web Agent Scanner.

Custom scan. In this mode you will be able to choose which files and folders to scan with Dr.Web Agent Scanner.

Unapproved stations—manage the list of newbies—stations whose registration is not approved yet (see the New Stations Approval Policy section for more details). This option is active only if stations of the **Newbies** subgroup of the **Status** group are selected. When the registration is approved, the stations will be automatically removed from the predefined **Newbies** group. To manage the registration of stations, select one of the following options from the drop-down list:

Approve selected stations and set a primary group—confirm station access to Dr.Web Server and set a primary group from the given list.

Cancel action specified to execute on connection—cancel the action on an unapproved station which was specified to be executed at the moment the station connects to Dr.Web Server.

Reject selected stations—forbid station access to Dr.Web Server.

Block settings—change the parameters of station access to Dr.Web Server. Select the action in the drop-down list:

Lockout period—set a time slot when the station access to Dr.Web Server is forbidden.

> If a **Lockout period** is set for a user group or policy, the specified parameter is saved only in the settings of stations located in this group or to which the policy is extended, but not in the settings of the group or policy itself.

Settings of tree view—adjust the appearance of the anti-virus network tree. To enable this parameter, set the corresponding flags in the drop-down menu:

- for groups:
  - **All groups membership**—duplicate displaying of a station in the list if the station is a member of multiple groups at the same time (only for groups under the white folder icon, see table 5-1). If the flag is set, the station will be shown in all member groups. If the flag is cleared, the station will be shown only once in the list.
  - **Show hidden groups**—show all groups included in the anti-virus network. If you clear the flag, all empty groups (not containing any stations) will be hidden. It may be helpful to remove the extra data, for example, when there are a lot of empty groups.
  - **Hide empty groups and stations that have never connected to Dr.Web Server**—hide empty groups, stations that have never connected to Dr.Web Server and groups containing only such stations.
- for the Dr.Web Server clients (stations, Dr.Web Proxy Servers, and neighbor Dr.Web Servers):
  - **Show clients identifiers**—show the unique identifiers of clients.
  - **Show clients names**—show the names of clients if they are given.

> You cannot disable the display of client identifiers and names at the same time. Either the **Show clients identifiers** or the **Show clients names parameter** will be always selected.

  - **Show clients addresses**—show the IP addresses of Dr.Web Server clients.
  - **Show station servers**—show the names or addresses of Dr.Web Servers to which stations are connected. Relevant to stations within a Dr.Web Server cluster.
  - **Show policy icon**—show the policy icon next to the icon of the station to which the policy is assigned.
  - **Show station states severity**—show the severity status of active stations. Color differentiation will be used for stations depending on their status (see table 5-1). If the option is disabled, the general icon will be displayed for station statuses with the and icons.
  - **Show blocked stations**—show stations whose access to Dr.Web Server is blocked.

- for all elements:
  - **Show personal settings icon**—show a marker which indicates whether individual settings are present on the icons of groups and the Dr.Web Server clients: stations, Dr.Web Proxy Servers, and neighbor Dr.Web Servers.
  - **Show descriptions**—show descriptions of groups and the Dr.Web Server clients: stations, Dr.Web Proxy Servers, and neighbor Dr.Web Servers (the descriptions are set in the properties of an element).
  - **Show the number of clients**—show the number of the Dr.Web Server clients: stations, Dr.Web Proxy Servers, and neighbor Dr.Web Servers, for all the anti-virus network groups that include these clients.
  - **Show membership rules icon**—show a marker on the icons of stations which were added to groups automatically according to membership rules and on the icons of groups to which stations were added automatically.

Filtering settings—filter the displayed elements of the anti-virus network tree by searching by specified parameters. To specify search criteria, set the corresponding flags next to the relevant criteria in the drop-down list. Enter the search string in the **Search** field. Click **Apply** to start searching by the specified parameters.

The search criteria are the same as those described in the Search Panel section, except for the **Configuration** additional item. The criterion allows you to search by certain parameter values of the anti-virus components installed on stations. When you select this criterion, the search panel opens with the following settings:

- **Component**—in the drop-down list, select the name of the anti-virus component whose settings will be searched. Use the search function to make the component selection from the list easier: start entering the name into the component field, the system will automatically suggest items containing the entered symbols.
- **Parameter**—in the drop-down list, select the name of the parameter whose values will be searched. Parameters with a complex structure of permissible values are not available for the search.
- **Value**—set the value of the parameter selected above. Depending on the permissible values of a specific parameter, you will be offered either a drop-down list with the permissible values or an entry field to specify the values manually via the keyboard.

To reset the search parameters, click the **Default** button.

Settings of clients sorting—change the parameter used for sorting and the sorting order of the Dr.Web Server clients in the anti-virus network tree: stations, Dr.Web Proxy Servers, and neighbor Dr.Web Servers.

- To select the sorting parameter, set one of the following flags (only one parameter can be selected):
  - **Identifier**—sort by unique identifiers of the clients.
  - **Name**—sort by names of the clients.
  - **Address**—sort by network addresses of the clients. Clients without a network address will be displayed in random order without sorting.

- **Created on**—sort by date of creation of the client account on Dr.Web Server.
- **Last connected on**—sort by date of the latest connection of the clients to Dr.Web Server.

- To select the sorting order, set the one of the following flags:
  - **Sort ascending**.
  - **Sort descending**.

The **Settings of tree view** and **Settings of clients sorting** sections are interdependent:

- If you select a sorting parameter in the **Settings of clients sorting** section, this parameter is automatically displayed in the **Settings of tree view** section if it was previously disabled.
- If you disable a parameter in the **Settings of tree view** section that was selected for sorting in the **Settings of clients sorting** section, the sorting by this parameter will be automatically switched to sorting by client name. If display of station names is disabled, then the sorting parameter is switched to station identifier (bothe the name and the identifier cannot be disabled at the same time).

Property pane

The property pane shows the properties and settings of workstations.

To display the property pane

1. Select the name of a station or a group in the hierarchical list.
2. A pane with the properties of the selected workstation or group opens in the right pane of Dr.Web Security Control Center. A detailed description of these settings is given in the Editing Groups and Station Properties sections.

If you select **Anti-virus network** in the hierarchical list, the property pane will display aggregated information about groups and stations of the anti-virus network and the number of available licenses.

5.3.3. Favorites

The control Center allows you to save bookmarks on interface pages into the favorites list for the convenience of the administrating. For example, to jump quickly to the most frequently visited pages of the Control Center.

Manage Favorites List

1. In the main menu of the Control Center, select **Favorites**.

2. The list of Control Center pages that have been added to bookmarks will be opened.
3. Click **Edit**.
4. In the list of favorite pages, you can:
   - Open the page that has been included into the favorites list. To do this, click the bookmark that corresponds to this page in the favorites list.
   - Change the sort order of bookmarks. To do this, click  to the left from the bookmark and move the bookmark above or below in the list.
   - Remove bookmarks from the favorites list. To do this, select the bookmark you want to remove, or all bookmarks. Click **Delete**, then **Save**.

Add a Bookmark to the Favorites

1. Open the Control Center page that you want to add to the favorites.
2. Next to the page name under the control menu, click ☆.
3. It opens the **Add a bookmark** window. In the **Name** field, the page name is added automatically in the following format: <*Main menu item*> > <*Control menu item*>. You can edit the bookmark name, if necessary.
4. The following actions are available:
   - To save a page in the favorites list, click **Add**. The icon next to a page name will be changed to ★.
   - To close the window without changing the list of favorite pages, click **Cancel**.

Edit and Remove a Bookmark from the Favorites

1. Open the Control Center page that you want to edit or remove from the favorites.
2. Next to the page name under the control menu, click ★.
3. It opens the **Edit the bookmark** window. The following actions are available:
   - To edit a bookmark, change its name in the **Name** field. Click **Refresh** to apply changes.
   - To remove a page from the favorites list, click **Delete**. The icon next to a page name will be changed to ☆.

5.3.4. Search Panel

The *search panel* locates at the top right part of Dr.Web Security Control Center and used to simplify searching for elements. The panel may find both groups and separate stations according to specified parameters.

For an extended parameter search, use the Filtering settings item on the **Anti-Virus Network** toolbar.

To find a workstation or group of workstations

1. Select the search criterion in the drop-down list of the search panel:
   - **Station**—to search for stations by name.
   - **Group**—to search for groups by name.
   - **Station ID**—to search for stations by unique identifiers.
   - **Group ID**—to search for groups by unique identifiers.
   - **User name**—to search for stations by user name on the station.
   - **IP address**—to search for stations by IP address.
   - **MAC address**—to search for stations by MAC address.
   - **Hardware**—to search for stations by the name or vendor of the hardware installed on the station.
   - **Software**—to search for stations by the name of the software installed on the station.
   - **Description**—to search for stations and groups by description.

   To start searching by component parameters, click **Search**.
2. Enter a parameter value to search. You can specify:
   - a specific string for full match with search value,
   - a mask for search string: the * symbol is allowed.
3. Press ENTER to start the search. The anti-virus tree will open.
4. The search results contain a hierarchical list of elements according the search parameters.
   - If you searched for a workstation, occurrence of the workstation in groups will be displayed.
   - If no elements are found, the message **Nothing found** will be displayed in the empty hierarchical list.

5.3.5. Events

To notify administrator on events requiring attention, the section displayed under the **Events** icon on the main menu is provided.

The icon may take the following states:

—no new notifications on events in the network.

—new notifications on minor events.

—new notifications on major events requiring administrator intervention.

The following actions are available for the events list:

1. The icon click opens the drop-down list of anti-virus network events. At this, the icon automatically changes to .

2. The click on notification string on event opens the Control Center section that responsible for corresponding functions.
3. The stub of every notification in the events list is marked with a color corresponding to the severity of the events (same as the icon). When opening a section that responsible for the notification functions, the notifications is considered as read and the stub changes color into gray.

Table 5-2. The list of available notifications on events in anti-virus network

Event	Severity	Control Center section	Description
Notifications on newbies	minor	**Anti-virus Network** The **Newbies** group opens in the hierarchical tree of anti-virus network	New stations connected to Dr.Web Server and waiting for approval of an access by administrator. It is possible if the **Approve access manually** value is set for the **Newbies registration mode** option in the Dr.Web Server configuration.
Unread news	minor	**Support → News**	Unread news of Doctor Web company are available.
New notifications	minor	**Administration → Web console notifications**	New administrator notifications which are received via the Web console method are available.
Critical notifications	major		
Dr.Web Server updates are available	major	**Administration → Dr.Web Server**	Dr.Web Server update is downloaded into repository and available for installation.
Dr.Web Server configuration has been changed. Dr.Web Server restart required.	major	**Administration → Dr.Web Server configuration**	Settings of the Dr.Web Server configuration file has been changed after the Dr.Web Server start. To take new settings, Dr.Web Server must be restarted.
Web server configuration has been changed. Dr.Web Server restart required.	major	**Administration → Web Server configuration**	Settings of the Web server configuration file has been changed after the Dr.Web Server start. To take new settings, Dr.Web Server must be restarted.

5.3.6. Preferences

To open the section of Control Center preferences, click **Preferences** in the main menu.

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

The control menu located in the left pane of the window, consists of the following items:

- My account.
- Interface.
- Subscription.

My Account

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

General

Values of fields marked with the * character must be specified.

You can edit the following settings, if necessary:

- **Login***—administrator account login to access Dr.Web Security Control Center.
- **First name**, **Middle name** and **Last name** of the administrator.
- **Email address** associated with the account.
- **Interface language** used by the administrator.

Interface texts for the selected language will be updated automatically after saving administrator settings. Also, flags for the necessary language will be set automatically in the **Administration → General repository configuration → Dr.Web Server → Dr.Web Security Control Center languages** and **Administration → General repository configuration → Dr.Web Server → Documentation** sections.

- **Date format**, which is used by this administrator during editing settings that contain dates. The following formats are available:
  - European: `DD-MM-YYYY HH:MM:SS`
  - American: `MM/DD/YYYY HH:MM:SS`
- **Time zone**—date and time of events in the interface will be displayed in accordance with the selected time zone.
- Account **Description**.
- To change the password, click **New password** at the toolbar.

The following parameters are read only:

- **Identifier** of the administrator account.
- **Authentication type** used for this account (see Authentication of Administrators):

  - **Internal**—based on the credentials in the Dr.Web Server database.
  - **External**—via external systems.
- Dates when the account was created and last modified.
- **Last address**. Displays the network address of the last connection under this account.

Permissions

Description of administrative rights and its editing see in the Editing Administrative Accounts and Groups section.

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

Interface

Tree Settings

Parameters of this section let you adjust the appearance of the list, and they are similar to the settings, located in the **Settings of tree view** option of the toolbar of the **Anti-virus network** item of the main menu:

- for groups:
  - **All groups membership**—duplicate displaying of a station in the list if a stations is a member of several groups simultaneously (only for groups under the white folder icon, see table 5-1). If the flag is set, the station will be shown in all member groups. If the flag is cleared, the station will be shown only once in the list.
  - **Show hidden groups**—show all groups included in the anti-virus network. If you clear the flag, all empty groups (not containing stations) will be hidden. It may be convenient to remove extra data, for example, when there are many empty groups.
  - **Show only groups with activated stations**—hide empty groups, stations that have never connected to Dr.Web Server, and groups containing only such stations.
- for the Dr.Web Server clients (stations, Proxy Servers and neighbor Dr.Web Servers):
  - **Show clients identifiers**—show clients unique identifiers.
  - **Show clients names**—show clients names, if such are given.

You cannot disable displaying both identifiers and names of stations at the same time. One of the **Show clients identifiers** and **Show clients names** parameters will be always selected.

  - **Show clients addresses**—show clients IP-addresses.
  - **Show station servers**—show names or addresses of Dr.Web Servers to which stations are connected. Relevant to the stations within Dr.Web Servers cluster.

- **Show station states severity**—show severity of active stations status. At this, the color differentiation will be used for stations depending on their status (see table 5-1). If the option is disabled, for station statuses with the and icons, the common icon will be displayed.
- **Show policy icon**—show the policy icon next to the icon of the station to which the policy is assigned.
- **Show blocked stations**—show stations whose access to Dr.Web Server is blocked.

- for all elements:
  - **Show personal settings icon**—show the marker which shows whether individual settings are present on the icons of groups and the Dr.Web Server clients: stations, Proxy Servers and neighbor Dr.Web Servers.
  - **Show descriptions**—show descriptions of groups and the Dr.Web Server clients: stations, Proxy Servers and neighbor Dr.Web Servers (the descriptions are set in the properties of an element).
  - **Show the number of clients**—show the number of the Dr.Web Server clients: stations, Proxy Servers and neighbor Dr.Web Servers for all the groups of an anti-virus network into which these clients are included.
  - **Show membership rules icon**—show the marker on stations icons which are added to groups automatically according to the membership rules, also on groups icons stations of which are added automatically.

Settings of clients sorting

Parameters of this section let you to change the parameter that is used for sorting and the sorting order of the Dr.Web Server clients: stations, Proxy Servers and neighbor Dr.Web Servers in the anti-virus tree, and they are similar to the settings, located in the **Settings of clients sorting** option of the toolbar of the **Anti-virus network** item of the main menu:

- To select the parameter to use for sorting, set the one of the following flags (only one parameter can be selected):
  - **Identifier**—sort by unique identifiers of clients.
  - **Name**—sort by names of clients.
  - **Address**—sort by network addresses of clients. Clients without network address will be displayed in random order without sorting.
  - **Created on**—sort by date of creation of a client account on Dr.Web Server.
  - **Last connected on**—sort by date of last connection of clients to Dr.Web Server.
- To select the sorting order, set the one of the following flags:
  - **Sort ascending**.
  - **Sort descending**.

Time Interval

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

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

  When you open the page for the first time, statistics will be displayed for this time interval. You can change the time interval at statistics pages directly, if necessary.
- Set the **Save last interval for statistics data** flag, to save the interval, specified last time at statistics sections.

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

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

Authorization

In the **Allowed inactivity** drop down list, select time period after which the user session of Control Center in a web browser is automatically terminated.

PDF Export

In this section you can specify text settings for statistic data export to the PDF format:

- In the **Report font** drop down list, select a font, which is used when exporting report to PDF format.
- In the **Report font size** field, specify the font size of general text of statistic tables, which is used when exporting report to PDF format.

Reports

In this section you can specify view settings for statistic data in the Reports section of the Control Center:

- In the **Number of lines per page** field, specify the maximal number of lines on one report page for paginal view of statistic.
- In the **Number of characters after long lines trim** field, set the maximum number of characters to remain visible after trimming long lines in log and notification tables.
- Set the **Show charts** flag to show charts on statistic report pages. If the flag is cleared, chart viewing is disabled.

Subscription

In this section you can manage the subscription to the Doctor Web company news. Set the flags to receive news of the following categories:

- **Updates**—news about Dr.Web product updates.
- **Promotions**—news about promotional events of Doctor Web company.
- **Virus alerts**—monthly reviews of malware activity and news about the most prominent threats and attacks.
- **Products**—news about Dr.Web products.
- **Dr.Web AV-Desk**—news about the Dr.Web AV-Desk service.
- **Corporate news**—news about Doctor Web company events.

Set the **Automatic subscription to new sections** flag to add new sections on the **News** page of the Control Center automatically.

5.3.7. Help

To get help on Dr.Web Enterprise Security Suite, click **Help** in the main menu. A context menu will open with the following options:

- **Documentation**—opens a page of administrator documentation that corresponds with the currently opened section of the Control Center. If the current section of the Control Center does not have a correspondent documentation page, the **Documentation** option will not be displayed in the context menu of the icon.
- **Support**—opens the **Support** page of the Control Center (see below).

Support

The **Support** page contains the following elements:

1. Links to support resources
   - **Forum**—opens official Doctor Web forums.
   - **News**—opens Doctor Web news page.
   - **Contact technical support service**—opens Doctor Web technical support page.
   - **Send a suspicious file**—opens a web form for sending a potential threat to the Doctor Web Virus Laboratory.
   - **Doctor Web wikipedia**—go to the knowledge base containing information about Doctor Web products (in Russian).
   - **Report false alarm in Office Control**—opens a web form for sending a message about false alarm or detection failure in Office Control module.

2. The **Documentation** section. Every document here is available in HTML and also PDF, as long as you set the flag next to your current interface language and check the box to update PDF documentation in **General repository configuration** → **Dr.Web Server** → Documentation. Click the required document name to open it in HTML. You can open the same document in PDF by clicking in the **Download** column. For the sake of convenience, the documentation is divided into several subsections:

   - **Dr.Web Enterprise Security Suite installation and use (administrator documentation)**

   Manuals in this subsection provide in-depth representation of how the Dr.Web Enterprise Security Suite service works. Materials grouped here let you understand the procedure of deploying and setting up the complex anti-virus protection and aspects of its components' interaction with third-party software. You can also review the latest updates available in the Dr.Web Enterprise Security Suite version you have installed at the moment.

   - **Managing stations protected by Dr.Web Enterprise Security Suite (administrator documentation)**

   These manuals contain information about configuration and centralized administration of different Doctor Web products, when they are included in the Dr.Web Enterprise Security Suite anti-virus network.

   - **User Documentation**

   These materials contain detailed information about installation and configuration of different Doctor Web products, as well as recommendations on their use and troubleshooting that users may need.

   A document downloaded via Dr.Web Mobile Control Center to an Android device is automatically saved to the Downloads folder.

   If the Dr.Web Server uses HTTPS with a self-signed certificate, make sure that you have installed this Dr.Web Server certificate on your Android device before downloading the documentation.

5.4. Dr.Web Security Control Center Components

5.4.1. Network Scanner

Network Scanner Functions

- Scan (browse) the network for workstations.
- Detect Dr.Web Agents on stations.
- Install Dr.Web Agent on the detected stations as instructed by the administrator. Dr.Web Agent installation is described in detail in the **Installation Manual**, Installing Dr.Web Agent Software via Dr.Web Security Control Center.

Network Scanner Operation Principal

Network scanner supports the following search modes:

1. Search in Active Directory
2. Search via NetBIOS
3. Search via ICMP
4. Search via TCP
5. Additional mode: Dr.Web Agent detect.

Procedure when all modes are enabled

1. First three modes are run in parallel. Repeated inquiring of already inquired stations is not performed.
2. After ICMP search is complete, the TCP search is launched for stations that have not responded. If ICMP search is disabled, TCP search is launched immediately in parallel with first two modes.

   ICMP search is implemented by sending ping requests that can be blocked because of network policies (e.g. by firewall settings).

   For example:

   If in Windows OS (Vista or later) network settings, the **Public location** options is set, OS will block all ping requests.

3. For stations found by search via the first four modes, the Dr.Web Agent detect search is launched.

   Network Scanner can detect Dr.Web Agents only of version 4.44 and later but cannot interact with Dr.Web Agents of earlier versions.

   Dr.Web Agent installed on a protected stations process respective calls of Network Scanner received at a certain port. By default, port `udp/2193` is used. Correspondingly, the default port is offered to call by the Scanner. Network Scanner decides whether Dr.Web Agent is on a station or not basing on the assumption of the possibility to exchange information (request-response) via the specified port.

   If the station is forbidden (for example, by a firewall) to accept packages at `udp/2193`, Dr.Web Agent will not be detected and consequently Network Scanner considers that there is no Dr.Web Agent installed on the station.

Network Scanner Launch

To scan the network

1. Open the Network Scanner window: select the **Administration** item in the main menu of Dr.Web Security Control Center and in the opened window, select the **Network Scanner** item in the control menu. The Network Scanner window will be opened.
2. Set the **Enable ICMP search** flag to search for stations via ICMP protocol in range of specified IP addresses.
3. Set the **Enable TCP search** flag to search for stations via TCP protocol in range of specified IP addresses.

   Specify the settings for this mode:

   - **Quick scan**. In the quick network scan mode, only most common ports on stations are checked: 445, 139, 22, 80.
   - **Extended scan**. In the extended network scan mode, a set of frequently used ports are checked. The ports are scanned in the specified order: 445, 139, 135, 1025, 1027, 3389, 22, 80, 443, 25, 21, 7, 19, 53, 110, 115, 123, 220, 464, 465, 515, 873, 990, 993, 995, 1194, 1433, 1434, 2049, 3306, 3690, 4899, 5222, 5269, 5432, 6000, 6001, 6002, 6003, 6004, 6005, 6006, 6007, 6446, 9101, 9102, 9103, 10050, 10051, 8080, 8081, 98, 2193, 8090, 8091, 24554, 60177, 60179.
   - **IPv4 addresses**—the list of IPv4 addresses:
     - single addresses: `10.4.0.10`
     - range of addresses with a hyphen: `172.16.0.1-172.16.0.123`
     - range of addresses with a network prefix: `192.168.0.0/24`

     If you set several addresses, use ";" or "," as a separator.
   - **IPv6 addresses**—the list of IPv6 addresses:
     - single addresses: `fe80::9109:1808:8e44:735b%3`
     - range of addresses with a hyphen: `[FC00::0001]-[FC00::ffff]`
     - with a network prefix: `[::ffff:10.0.0.1]/7`

     If you set several addresses, use ";" or "," as a separator.
4. Set the flag **Enable search by NetBIOS** to search for stations via NetBIOS protocol.

   Specify the settings for this mode:

   - **Domains**—domains list in which stations are searched. Use comma to divide several domains.
   - Set the flag **Extended scan** to use extended scan using data from network browsers.
5. Set the flag **Enable search in Active Directory** to search for stations in the Active Directory domain.

To be able to search stations in the Active Directory domain via the Network Scanner, the web browser in which the Control Center is opened, must be launched in the name of the domain user with permissions to search objects in the Active Directory domain.

Specify the settings for this mode:

- **Active Directory controller**—Active Directory controller, e.g. `dc.example.com`.
- **Login**—Active Directory user login.
- **Password**—Active Directory user password.

For Dr.Web Servers under Windows OS, settings of Active Directory search are not obligatory. Information of a user on whose behalf the Dr.Web Server process is run (usually, it is `LocalSystem`) is used as a default registration information.

For Dr.Web Servers under Unix-like OS, the settings must be obligatory specified.

- In the **Connection security** drop-down list, select the type of encrypted data exchange:
  - **Use data encryption**—switching to a secure encrypted LDAP connection is performed using the `STARTTLS` command. By default, a connection is established via TCP or UDP protocol using port 389.
  - **Use SSL**—establish a new secure LDAPS connection. By default, a connection is established via TCP protocol using port 636.
  - **No**—do not use encryption. Data exchange will be performed over an unprotected LDAP connection via TCP protocol using port 389.

6. In the General parameters section, specify common settings for all search modes:
   - **Time-out (sec.)**—maximum time in seconds to wait a response from a station.
   - **Number of requests to one station**—maximum number of requests to one station waiting for the answer.
   - **Number of simultaneous requests**—maximum number of stations for simultaneous requests.
   - Set the **Show station names** flag to display either IP address or DNS name of found stations. If a station is not registered at DNS server, only its IP address displays.
   - Set the **Detect installed Agent** flag to detect installed Dr.Web Agent on a station. If the option is disabled, the status for all found stations indicates that the state of anti-virus software on the station is unknown.

If the **Detect installed Agent** option is disabled, all found stations will have the  state, i.e. the state of anti-virus software on a station is unknown.

   - **Port**—UDP protocol port number to call the Dr.Web Agent during the search. The range is 1-65535. The 2193 port is used by default.
7. Click **Scan** to launch the network scanning.

8. The list of computers demonstrating where Dr.Web Agent is installed will be loaded into this window.

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

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.
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 software detection was not perform.

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

5.5. The Interaction Scheme of an Anti-Virus Network Components

The Figure 5-2 describes a general scheme of an anti-virus network built with Dr.Web Enterprise Security Suite.

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

In this example the anti-virus network is implemented within a local network, but for the installation and operation of Dr.Web Enterprise Security Suite and anti-virus packages the computers need not be connected within any local network, internet connection is enough.

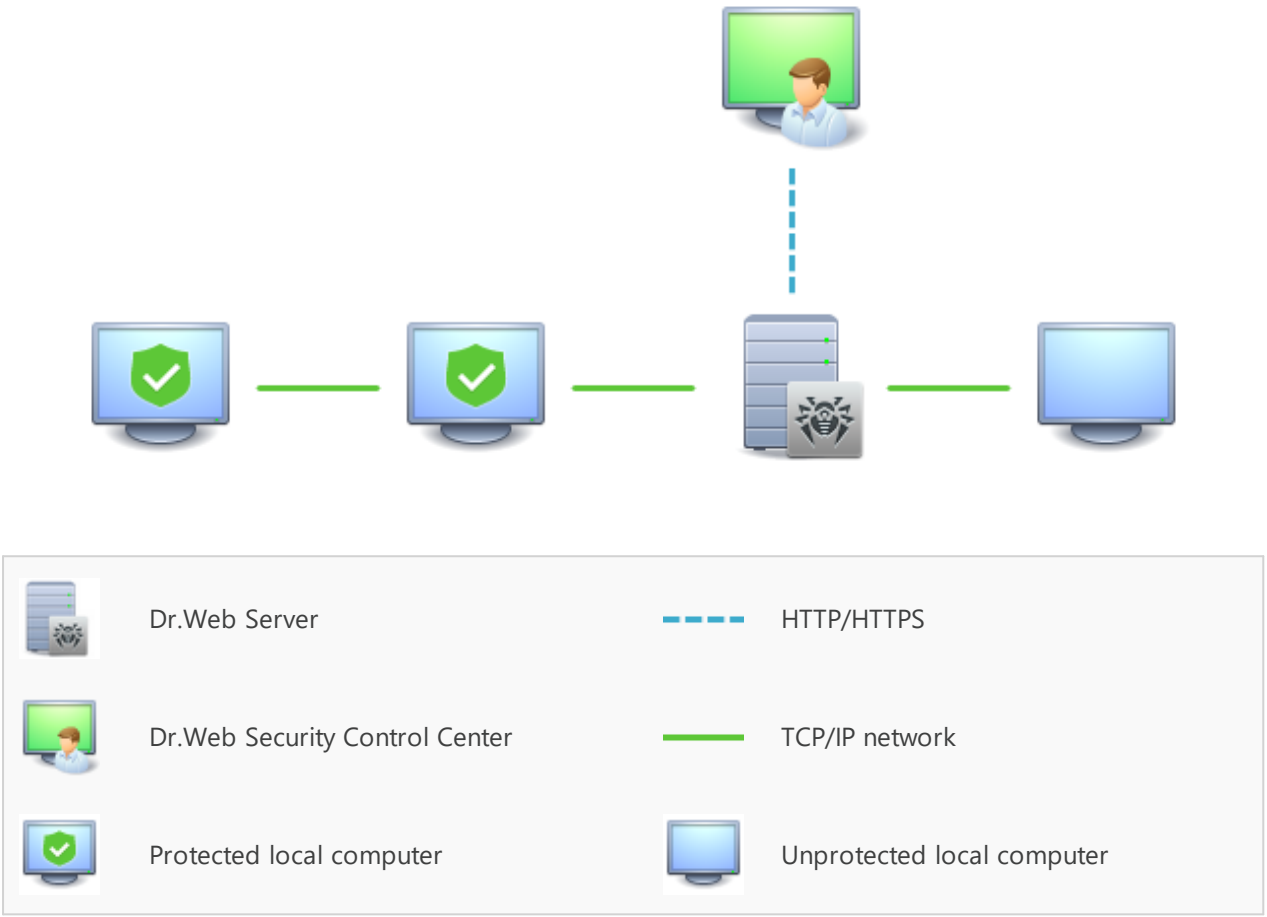


Figure 5-2. The physical structure of the anti-virus network

When Dr.Web Server is launched, the following sequence of commands is performed:

1. Dr.Web Server files are loaded from the `bin` folder.
2. Dr.Web Server Task Scheduler is loaded.
3. The content of the update folder is loaded, notification system is initialized. The Dr.Web Server database integrity is checked.
4. Dr.Web Server Task Scheduler tasks are performed.
5. Dr.Web Server is waiting for information from Dr.Web Agents and commands from Dr.Web Security Control Center.
6. The whole stream of instructions, data and statistics in the anti-virus network always goes through Dr.Web Server.

Dr.Web Security Control Center exchange information only with Dr.Web Servers. Based on Dr.Web Security Control Center commands, Dr.Web Servers transfer instructions to Dr.Web Agents and change the configuration of workstations.

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

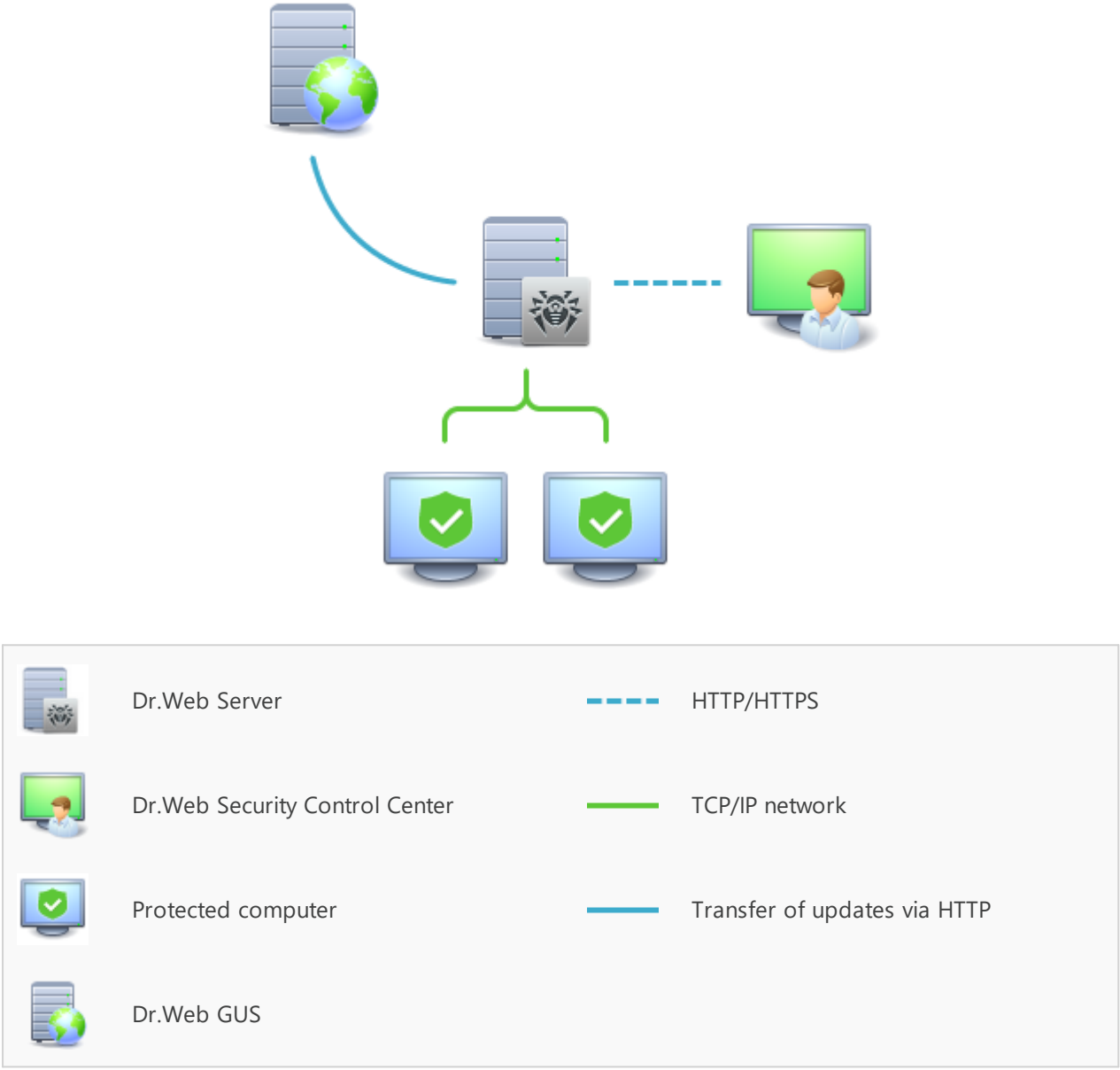


Figure 5-3. The logical structure of the anti-virus network

Between Dr.Web Server and workstations (a thin continuous line in the Figure 5-3) transferring the following information:

- Dr.Web Agents requests for the centralized schedule and the centralized schedule of workstations,
- settings of the Dr.Web Agent and the anti-virus package,
- requests for scheduled tasks to be performed (scanning, updating of virus databases, etc.),
- files of anti-virus packages—when the Dr.Web Agent receives a task to install them,
- software and virus database updates—when an updating task is performed,
- Dr.Web Agent messages on the configuration of the workstation,

- statistics on the operation of Dr.Web Agents and anti-virus packages for adding to the centralized log,
- messages on events related to threats and other events which should be logged.

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

Traffic between Dr.Web Server and Dr.Web Agent can be encrypted. This allows to avoid disclosure of data transferred via the described channel as well as to avoid substitution of software downloaded on workstations. By default traffic encryption is enabled. For more detailes, please read p. Traffic Encryption and Compression.

From the update web server to Dr.Web Server (a thick continuous line in the Figure 5-3) files necessary for replication of centralized installation and update folders as well as overhead information on this process are sent via HTTP. The integrity of the information (Dr.Web Enterprise Security Suite files and anti-virus packages) is provided through the checksums: a file corrupted at sending or replaced will not be received by Dr.Web Server.

Between Dr.Web Server and Dr.Web Security Control Center (a dashed line in Figure 5-3) data about the configuration of Dr.Web Server (including information about the network layout) and workstations settings are passed. This information is visualized on Dr.Web Security Control Center, and in case a user (an anti-virus network administrator) changes any settings, the information about the changes is transferred to Dr.Web Server.

Connection between Dr.Web Security Control Center and a certain Dr.Web Server is established only after an anti-virus network administrator is authenticated by his login name and password on the given Dr.Web Server.

Chapter 6: Anti-Virus Network Administrators

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

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

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

6.1. Authentication of Administrators

To connect to Dr.Web Server, administrator can authenticate by the following ways:

- With storing administrative account information in the Dr.Web Server DB.
- Using the common LDAP/AD settings that allow to connect to LDAP and Active Directory servers.
- Via the RADIUS protocol.
- Via PAM (for Dr.Web Servers running Unix-like OSs).
- Via Active Directory (for Dr.Web Servers running Windows OS).

When updating Dr.Web Server from a previous version, authentication via the LDAP protocol may also be available if it was enabled in the previous version.

After disabling LDAP authentication the corresponding section will be excluded from the Control Center settings.

The section is not provided during the initial installation of Dr.Web Server.

Authentication methods are used sequentially according to the following rules:

1. Authentication of administrator from the Dr.Web Server DB is always tried first.
2. The order of usage of authentication methods via the external systems depends on the order of their following in the settings, specified in the Control Center.
3. Authentication methods via the external systems are disabled by default.

To swap the usage of authentication methods

1. Select **Administration** in the main menu of the Control Center.
2. Select **Authentication** in the control menu.
3. In the opened window, list of authentications types is represented in the order of use. To change this order, drag and drop authentication methods in the list and place them in the necessary order of use the authentication.
4. To apply changes, you must restart Dr.Web Server.

Administrative login must be unique.

Administrators are not allowed to connect via external authentication systems if an administrator with the same login already exists at Dr.Web Server.

After each saving of changes in the **Authentication** section, the backup copy of the previous version of the configuration file with administrators authentication parameters is saved automatically. Only 10 last copies are stored.

Files are placed in the same folder as the configuration file itself and named according to the following format:

<file_name>_<creation_time>

where *<file_name>* depends on authentication system: `auth-ads.conf`, `auth-ldap.conf`, `auth-radius.conf`, `auth-pam.conf`.

You can use created backup copies particularly to restore the configuration file if the Control Center interface is not available.

6.1.1. Authentication of Administrators from the Dr.Web Server DB

Authentication method with storing administrative account information in the Dr.Web Server DB is used by default.

To open administrative accounts control section

1. Select **Administration** in the main menu of the Control Center.
2. Select **Administrators** in the control menu. The list of all administrators registered in the DB will be opened.

See the Administrators and Administrative groups section for details.

6.1.2. LDAP/AD Authentication

To enable LDAP/AD authentication

1. Select **Administration** in the main menu of the Control Center.
2. Select **Authentication** in the control menu.
3. In the opened window, select **LDAP/AD authentication** section.
4. Set the **Use LDAP/AD authentication** flag.
5. Click **Save**.
6. Restart Dr.Web Server to apply changes.

You can configure authentication using LDAP protocol at any LDAP server. Also you can use this mechanism to configure Dr.Web Server under Unix-like OS for authentication in Active Directory on a domain controller.

If an LDAP server other than MS Active Directory is used, it is recommended to configure the rules for translating user names to DN in the `auth-ldap-rfc4515.conf` configuration file in accordance with RFC4515 using the `<user-dn-extension-enabled/>`, `<user-dn/>`, `<user-dn-expr/>` parameters.

If the authorized user does not have search rights on the LDAP server, then in the `<bind dn/>` parameter you can configure the DN and password of the LDAP server user with read rights, on whose behalf the search for the authorized user data will be performed on the LDAP server.

The description of these parameters is given in the **Appendices** document, B3. LDAP/AD Authentication section.

For the convenience of a user, the section provides the ability to switch between simplified or extended versions of authentication settings via LDAP/AD.

Settings of LDAP/AD authentication are stored in the `auth-ldap-rfc4515.conf` configuration file.

Configuration files with typical settings are also provided: `auth-ldap-rfc4515-check-group.conf`, `auth-ldap-rfc4515-check-group-novar.conf`, `auth-ldap-rfc4515-simple-login.conf`.

General xml attributes are described in the **Appendices** document, in the B3. LDAP/AD Authentication section.

Specifics of configuration in the presence of a domain forest (root and child domains)

If you want to authenticate not only the root Active Directory domain, but also its child domains, the access group in the root domain must include users from all child domains. The type of this access group in Active Directory must be **Universal**.

The **Global Catalog** option must be enabled in **NTDS Settings** for the root domain (if this option is enabled, port 3268 will be listened to). In the authentication settings in the Dr.Web Server Control Center, only the root domain and the Global Catalog port number (3268 by default) should be specified. In the configuration file for this case, the host attribute value will be the following: `host='example.srv:3268'`.

In order to avoid entering the full name with the domain when authenticating under an account from a child domain, the `<bind dn/>` tag should be configured, see the description of the tag in the **Appendices** document, B3. LDAP/AD Authentication.

6.1.3. RADIUS Authentication

To use the RADIUS authentication protocol, you must install a server that implements this protocol, e.g., freeradius (for details, see https://www.freeradius.org/).

Before you start configuring RADIUS authentication, make sure that the `dictionary.drweb` file located in the `etc` folder of Dr.Web Server is copied to the `/usr/share/freeradius` directory. The dictionary stores the list of RADIUS attributes of Doctor Web company (VSA—Vendor-Specific Attributes).

Use the command line to change the access permissions of the `dictionary.drweb` file located in the `/usr/share/freeradius` directory. Command example to change the access permissions:

```
chmod 644 /usr/share/freeradius/dictionary.drweb
```

Add the following line to the end of the `/etc/raddb/dictionary` file:

```
$INCLUDE/usr/share/freeradius/dictionary.drweb
```

Add the following lines to the beginning of the `/etc/raddb` file:

```
<Login> Cleartext-Password := "<password>"

DrWeb-ES-Adm-Flag = 1
```

After you complete these steps, enable RADIUS authentication via the Control Center.

To enable RADIUS authentication

1. Select **Administration** in the main menu of the Control Center.
2. Select **Authentication** in the control menu.
3. In the opened window, select **RADIUS authentication** section.
4. Set the **Use RADIUS authentication** flag.
5. Click **Save**.
6. Restart Dr.Web Server to apply changes.

In the Control Center you can specify the following parameters for the RADIUS server communication:

- **Server**, **Port**, **Password**—parameters for connection to the RADIUS server: IP address/DNS name, port number, password (secret) correspondingly.
- **Time-out**—time for waiting the response from the RADIUS server, in seconds.
- **Retries number**—maximum number of retries to connect the RADIUS server.

Also, you can setup additional RADIUS parameters via the `auth-radius.conf` configuration file located in the `etc` folder of Dr.Web Server.

Besides parameters that are specified via the Control Center, in the configuration file you can specify the NAS identifier value. This identifier according to the RFC 2865, can be used instead of IP address/DNS name as a client's identifier for connection to the RADIUS server. In the configuration file it is stored in the following form:

```
<!-- NAS identifier, optional, default - hostname -->
<nas-id value="drwcs"/>
```

6.1.4. PAM Authentication

To enable PAM authentication

1. Select **Administration** in the main menu of the Control Center.
2. Select **Authentication** in the control menu.
3. In the opened window, select **PAM authentication** section.
4. Set the **Use PAM authentication** flag.
5. Click **Save**.
6. Restart Dr.Web Server to apply changes.

PAM authentication under Unix-like OS is performed by using pluggable authentication modules.

To configure PAM authentication parameters, you can use one of the following ways:

- Configure authentication methods via the Control Center: in the **Administration** → **Authentication** → **PAM authentication** section.

- The `auth-pam.xml` configuration file located in the `etc` folder of Dr.Web Server. Configuration file example is:

```
...
<!-- Enable this authorization module -->
  <enabled value="no" />
<!-- This authorization module number in the stack -->
  <order value="50" />
<!-- PAM service name>" -->
  <service name="drwcs" />
<!-- PAM data to be queried: PAM stack must return INT zero/non-zero -->
  <admin-flag mandatory="no" name="DrWeb_Esuite_Admin" />
...
```

Description of PAM authentication parameters which are configured at Dr.Web Enterprise Security Suite side

Control Center items	auth-pam.xml file items			Description
	Tag	Attribute	Available values	
Use PAM authentication flag	<enabled>	value	yes | no	Flag that defines whether the PAM authentication method is used.
Use *Drag and Drop*	<order>	value	positive integer, coordinated with other methods values	Serial number of PAM authentication if several authentication methods are used.
Service name field	<service>	name	-	Service name which is used to create PAM context. PAM can read politics for this service from the `/etc/pam.d/`<*service name*> or from the `/etc/pam.conf`, if the file does not exist. If the parameter is not set (no <service> tag in the configuration file), the `drwcs` name is used by default.
Control flag is mandatory flag	<admin-flag>	mandatory	yes | no	Parameter defines whether the control flag identifying a user as an administrator is mandatory. By default is `yes`.
Control flag name field	<admin-flag>	name	-	Key string according to which PAM modules read the flag.

Control Center items	auth-pam.xml file items			Description
	Tag	Attribute	Available values	
				By default is `DrWeb_Esuite_Admin`.

When configuring operating of PAM authentication modules, use parameters which are set at Dr.Web Enterprise Security Suite side, and consider default values which are used if parameters are not specified.

6.1.5. Active Directory Authentication

Before enabling Active Directory authentication for any account, make sure that this account is not a member of the **Protected Users** group. Since the Dr.Web Server is a service, an attempt to authenticate an account that is added to the **Protected Users** group will fail. Please visit Microsoft official website for details.

To enable Active Directory authentication

1. Select **Administration** in the main menu of the Control Center.
2. Select **Authentication** in the control menu.
3. In the opened window, select **Microsoft Active Directory** section.
4. Set the **Use Microsoft Active Directory authentication** flag.
5. Click **Save**.
6. Restart Dr.Web Server to apply changes.

For Active Directory authentication, only enabling of using this authentication method is configured in Control Center.

You must edit Active Directory administrators' settings manually at the Active Directory server.

When automatically creating an administrator with the Active Directory authentication enabled, the administrator account is automatically placed to the Newbies group and requires manual placement to the required group.

It is possible to automatically place an administrator account from the Newbies group to a required one (based on Active Directory group membership) via a user hook; see **Appendices**, M1. Administrators.

To edit Active Directory administrators

The following operation must be carried out from a computer with Active Directory Service snap-in.

1. To enable editing of administrator parameters, do the following:
   a) Modify the Active Directory scheme with the `drweb-modify-ad-schema-<package_version>-<build>-<OS_version>.exe` utility (it is included into Dr.Web Server distribution kit).
   Modification of Active Directory scheme may take some time. Depending on the domain configuration, it may take up to 5 minutes and more to synchronize and apply the modified scheme.

If the Active Directory scheme has been modified earlier via this utility for the 6 version of Dr.Web Server, it is no need to perform modification repeatedly via the utility from the 13 version of Dr.Web Server.

   b) Register Active Directory Schema snap-in, execute the `regsvr32 schmmgmt.dll` command with the administrative privileges, then run `mmc` and add the **Active Directory Schema** snap-in.
   c) Using the Active Directory Schema snap-in, add the auxiliary **DrWebEnterpriseUser** class and the additional **DrWebAdmin** attribute to the **User** and (if necessary) **Group** classes.

If the scheme modification and application process has not finished, the **DrWebEnterpriseUser** class may be not found. In this case, wait for a few minutes and retry to add the class as described in **c)** step.

   d) With the administrative privileges run the `drweb-aduac-<package_version>-<build>-<OS_version>.msi` file (included in the Dr.Web Enterprise Security Suite 13.0 distribution kit) and wait until the installation finishes.
2. Visual editing of attributes is available from the **Active Directory Users and Computers** control panel → **Users** section → in the **Administrator Properties** window for editing settings of selected user → on the **Dr.Web Authentication** tab.
3. The following parameter is available for editing (**yes**, **no** or **not set** values can be set for the attribute):

   User is administrator indicates that the user is full-rights administrator.

Algorithms of operating principles and attributes handling during authentication are described in the **Appendices** document, in the B1. Active Directory Authentication section.

To work with an Active Directory account, log in to the Dr.Web Server Control Center under credentials of Active Directory user who had the appropriate **Dr.Web Authentication** attribute set. The user account will appear in the **Newbies** directory of the **Administration** → **Administrators** section.

6.1.6. LDAP Authentication

This section is available for configuration via the Control Center only at update of Dr.Web Server from the previous version. After disabling this authentication type, its section will be excluded from the Control Center settings.

At the first Dr.Web Server installation, this section is not available.

To enable LDAP authentication

1. Select **Administration** in the main menu of the Control Center.
2. Select **Authentication** in the control menu.
3. In the opened window, select **LDAP authentication** section.
4. Set the **Use LDAP authentication** flag.
5. Click **Save**.
6. Restart Dr.Web Server to apply changes.

You can configure authentication using LDAP protocol at any LDAP server. Also you can use this mechanism to configure Dr.Web Server under Unix-like OS for authentication in Active Directory on a domain controller.

Settings of LDAP authentication are stored in the `auth-ldap.conf` configuration file.

General xml attributes are described in the **Appendices** document, in the B2. LDAP Authentication section.

Unlike to Active Directory, this mechanism can be configures to any LDAP scheme. By default the Dr.Web Server attributes are used as they were defined for Active Directory.

LDAP authentication process can be presented as the following:

1. LDAP server address is specified via the Control Center or xml configuration file.
2. For the specified user name, the following actions are performed:
   - Translation of name to the DN (Distinguished Name) using DOS-like masks (with * symbol), if rules are specified.
   - Translation of name to the DN using regular expressions, if rules are specified.
   - Custom script for translation of name to the DN is used, if it is specified in settings.

- If matches in translation rules are not found, specified name is used as it is.

> Format of user names specifying is not predefined and not fixed—it can be any as it is accepted in the company, i.e. forced modification of LDAP scheme is not demanded. Translation according given scheme is performed using rules of translation of names to LDAP DN.

3. After translation, like for the Active Directory, attempt of the user registration at the specified LDAP server using determined DN and specified password is performed.
4. After this, like for the Active Directory, LDAP object attributes are read for the determined DN. Attributes and their possible values can be redefined in the configuration file.
5. If undefined values of administrator attributes are found, and inheriting is specified (in the configuration file), the search of needed attributes in the user groups is the same as in the Active Directory.

6.2. Administrators and Administrative groups

To open administrative accounts control section

1. Select **Administration** in the main menu of the Control Center.
2. Select **Administrators** in the control menu. The list of all administrators registered in the DB will be opened.

> The **Administrators** section is available for all Control Center administrators. Full hierarchical tree of administrators is available only for **Administrators** group members who have the **View properties and configuration of administrative groups** permission. The rest of administrators will only see their respective groups with subgroups and accounts.

On the toolbar of the **Administrators** section, the following options are available:

Create account
Create group
Remove selected objects
Change password
Propagate administrator permissions

6.2.1. Hierarchy of Administrators

Hierarchical view of administrators is a tree which represents a structure of administrative groups and administrators accounts. Administrative groups and their members (administrators accounts) both can be nodes of such tree. Each administrator can be a member of only one group. Nesting level of groups in a tree is not limited.

Predefined groups

After installing Dr.Web Server two groups are automatically created:

- **Administrators**. The group initially contains only **admin** user with a full set of privileges. The **admin** user is automatically created during Dr.Web Server installation (see below).
- **Newbies**. The group is initially empty. Administrators with external type of authentication, such as LDAP, Active Directory or RADIUS, will be automatically moved to this group.

  Administrators of the **Newbies** group have read-only access by default.

Predefined administrators

After installing Dr.Web Server the following administrative account is automatically created:

Parameter	Value
Account name	**admin**
Password	Password is set during Dr.Web Server installation (step 9 of installation procedure).
Privileges	Full set of privileges.
Account editing	Administrator privileges cannot be edited. Administrative account cannot be deleted.

Hierarchical Lists Displaying

- In the hierarchical list of anti-virus network: administrator sees only those user groups, which are granted in the **View groups of stations properties** permission. All system groups are also displayed in the anti-virus network tree, but only stations from the specified user groups list are available inside.
- In the hierarchical list of administrators: administrator from the **Newbies** group sees only a tree, the root node of which is a group of this administrator, i.e. sees administrators from the own group and its subgroups. Administrator from the **Administrators** group sees all administrators not depending on their groups.

6.2.2. Administrators Permissions

All administrators activity in the Control Center is limited by the set of permissions, which can be defined either for specific account or for a group of administrators.

Administrative permissions system includes the following opportunities of permissions management:

- **Granting permissions**

  Granting permissions performed during creation of administrative account or administrative group. When administrator or administrative account is created, it inherits permissions from the parent group it is added to. Changing permissions is not allowed during creation.

- **Inheriting permissions**

  By default permissions of administrators and administrative groups are inherited from a parent group, but inheritance can be disabled.

  - If inheritance is disabled, administrator uses independence set of personal permissions witch is set directly for the account. At his, permissions of the parent group are not considered.
  - Inheriting account or group permissions does not reassign them with parent permissions but calculates new set of permissions from permissions of all parent groups in the branch of hierarchy. The resulting set of permissions for an object depends on own permissions and parent groups permissions can be found in the Permissions Merge section.

- **Changing permissions**

  Changing permissions is not allowed for administrators accounts or administrative groups during creation. Permissions can be changed only for already created accounts and groups and can be done in the properties section of an account or a group. You can only reduce permissions at editing own settings. You cannot edit permissions for the **admin** predefined administrator and **Administrators** and **Newbies** predefined groups.

  The procedure is described in the Editing Permissions section.

Editing Permissions

To edit permissions of an administrator or a group of administrators

1. Select the **Administration** item in the main menu of the Control Center and in the opened windows, select the **Administrators** item in the control menu.
2. Select the account you want to edit from the list of administrators. The properties section will be opened for editing.
3. In the **Permissions** subsection, you can edit the list of actions that are allowed for the selected administrator or administrative group.
4. To manage the permissions inheritance from the parent group for the selected object, use the switch:

    **Inheritance enabled**

    **Inheritance disabled**
5. The general settings are set in the permissions table:

a) In the first column, permission names are given. A column name depends on the specific section that unifies permissions by types.

Brief description of administrative permissions and Control Center sections depended on a certain permissions, is given in the **Appendices** document, B4. Depended Permissions Sections.

b) The **Permissions** column contains the settings for corresponding permissions from the first column.

Managing objects	Settings list in the Permissions column	How to setup the permission
Permission is set for all objects		
Permission does not implicate dividing on groups by managing objects.	One of the following permission types may be given: • **Personal**—personal settings are assigned for this object. • **Inherited**—settings are inherited from the parent group.	Set/clear the **Grant** flag in the corresponding permission line.
Permission is set for the list of objects (stations, administrators or groups)		
• *All granted*—permission is granted for all managing objects. • *All forbidden*—permission is forbidden for all managing objects. • *Granted for some objects*. At this, the list of objects to grant the permission must be set. For all other objects, the permission is considered forbidden. • *Forbidden for some objects*. At this, the list of objects to forbid the permission must be set. For all other objects, the permission is considered granted.	If settings are merged, the following permission types are given at the same time: • **Personal**—personal settings specified for this object. • **Result**—the result of merging of an object personal permission and a parent group permission. If settings are inherited, only the permission type **Inherited** is given.	Click the objects list (even it is **All**). Either the anti-virus network tree or administrator groups tree or tariffs tree opens depending on the editing permission. Select necessary objects in the tree. Use CTRL and SHIFT to select several objects. If necessary, set the **For all permissions of the section**, to apply these settings for all permissions given in the same section as the edited permission. Click the button: • **Grant** to allow the permission for selected objects. • **Forbid** to forbid the permission for selected obkects.

For the same permission assigned on the list of objects, cannot be set the lists of forbidden and allowed objects at the same time. These concepts are mutually exclusive.

c) The **Inheritance** column reflects the state of the permission relatively a parent group:

- **Inherited from a group**—the inheritance from the specified parent group is enabled, personal permissions are not set.
- **Personal settings**—the inheritance from the specified parent group is disabled, personal permissions are set.
- **Merged with the group**—the inheritance from the specified parent group is enabled, personal permissions are set. Result permission of an object is calculated by merging of parents group permissions and personal permissions (see the Merging Permissions). In this case, personal permissions of an object can be removed. To do this, click  in the **Inheritance** column. After personal permissions been removed, the **Inheritance from a group** will be set.

Merging Permissions

Calculation of result permissions of an object (administrator or administrative group) when inheritance is enabled, depends on paren groups permissions and permissions of an object itself. The table below contains the calculation principal of an object permission result:

Parent group permission	Examining child permission	Result permission
All granted	Granted for some objects	Granted for objects of a child
Granted for some objects	Granted for some objects	The list of allowed objects are merged
Granted for some objects	All granted	All granted
A parent and a child have forbidding permissions and one of them forbids all		All forbidden
Forbidden for some objects	Forbidden for some objects	The list of forbidden objects are merged
All forbidden	All granted	All granted
Forbidden for some objects	All granted	Forbidden of objects of a parent
Forbidden for some objects	Granted for some objects	Allowed objects are subtracted from forbidden objects. If the forbidden objects list is not empty, in the result, the left objects are forbidden. Otherwise, in the result, all objects of a child are allowed
Granted for some objects	All forbidden	All forbidden
All granted	Forbidden for some objects	Forbidden of objects of a child
Granted for some objects	Forbidden for some objects	Forbidden objects are subtracted from the allowed objects. If the allowed

Parent group permission	Examining child permission	Result permission
		objects list is empty, in the result, all is forbidden. Otherwise, in the result all left objects are allowed.

6.3. Management of Administrative Accounts and Administrative Groups

6.3.1. Creating and Deleting Administrative Accounts and Groups

The administrative login name must be unique.

Administrators are not allowed to connect via external authentication systems if an administrator with the same login already exists at this Dr.Web Server.

Adding Administrators

To create an administrative account, the administrator must have the **Create administrators, administrative groups** permission.

To add a new administrative account

1. Select the **Administration** item in the main menu of the Control Center; in the window that opens, select the **Administrators** item in the control menu.
2. Click the  **Create account** icon in the toolbar. A window for setting up an account will open.
3. In the **General** section, specify the following parameters:
   - In the **Login** field, specify the administrator account login for accessing Dr.Web Security Control Center. You may use lowercase characters (a-z), uppercase characters (A-Z), digits (0-9), symbols "_" and ".".
   - In the **Password** and **Confirm Password** fields, set the password for accessing Dr.Web Server and Dr.Web Security Control Center.

You cannot use non-Latin characters in the administrator's password.

The password fields are active only for administrators using internal authentication.

The values of these fields specified in the Control Center for administrators using external authentication are irrelevant.

- In the **First name**, **Middle name**, and **Last name** fields, specify the administrator's personal data.
- Specify the **Email address**. Otherwise, the password reset option will be unavailable.
- In the **Interface language** drop-down list, select the language which will be used by the administrator (web browser language or English is specified by default).

If you select an interface language whose texts are not currently being updated, you will be prompted to enable the update for this language. To do this, follow the link to the **Administration → General repository configuration → Dr.Web Server → Dr.Web Security Control Center languages** section, set the flag for the necessary language and click **Save**. At the next repository update, the interface texts for the selected language will be updated. You can also launch the update manually in the **Repository state** section.

- In the **Date format** drop-down list, select the date format which will be used by this administrator when editing settings that contain dates. The following formats are available:
  - European: `DD-MM-YYYY HH:MM:SS`
  - American: `MM/DD/YYYY HH:MM:SS`
- In the **Description** field, you can set an optional description of the account.

Values of fields marked with the * character must be specified.

4. In the **Groups** subsection, you can specify the parental administrative group. The list contains groups to which an administrator can be assigned. A flag is set next to the group to which the new administrator will be assigned. Newly created administrators are placed in the parent group of the current administrator by default. To change the group, set the flag next to the group you need.

   Each administrator may be a member of one group only.

   The administrator inherits permissions from the parental group (see Administrators Permissions).
5. After you set all the necessary parameters, click **Save** to create the new administrative account.

To provide the newly created administrator with the latest information about anti-virus network events, it is recommended that you configure the notification settings immediately after creating the new account by following the instructions from the Notification

Configuration section. Make sure to enable the **Statistic report** notification to allow the administrator to create scheduled statistical reports.

Adding Administrative Groups

To create administrative groups, the administrator must have the **Create administrators, administrative groups** permission.

To add a new administrative group

1. Select the **Administration** item in the main menu of Dr.Web Security Control Center, then select the **Administrators** item in the control menu of the windows that opens.
2. Click the **Create group** icon in the toolbar. A window for setting up a new group will open.
3. In the **General** section, specify the following parameters:
   - In the **Group field**, specify the name of the administrative group. You may use lowercase characters (a-z), uppercase characters (A-Z), digits (0-9), symbols "_" and ".".
   - In the **Description** field, you can set optional description of the group.
4. In the **Groups** subsection, you can specify the parental administrative group. The list contains groups which can be assigned as a parental group. A flag is set next to the group to which the new administrative group will be assigned. Newly created groups are placed in the parent group of the current administrator by default. To change the group, set the flag next to the group you need.

   Only one parent group may be assigned.

   The administrative group inherits permissions from its parental group (see Administrators Permissions).
5. After you set all the necessary parameters, click **Save** to create the new administrative group.

Deleting Administrators and Administrative Groups

To delete administrative accounts and administrative groups, the administrator must have the **Create administrators, administrative groups** and **Edit properties and configuration of administrative groups** permissions correspondingly.

To delete an administrative account or group

1. Select the **Administration** item in the main menu of Dr.Web Security Control Center and then the **Administrators** item in the control menu.

2. In the hierarchical list of administrators, select the administrative account or administrative group you want to delete.
3. Click the **Delete selected objects** icon in the toolbar.

   If the administrator to be deleted is the author of tasks from the Dr.Web Server Task Scheduler, assign their tasks to another administrator in the right part of the window before you delete the account. Then click **Delete**.
4. Confirm the action.

6.3.2. Restoring Administrator Password

You can restore lost administrator password in one of the following ways:

1. Reset the password on the Dr.Web Security Control Center login page.
2. Set a new password from the command line when launching Dr.Web Server.

To reset the password on the Dr.Web Security Control Center login page

1. Open the login page (`http://<Dr.Web_Server_address>:9080` or `https://<Dr.Web_Server_address>:9081`).
2. Click **Reset password**.
3. In the opened window, fill in the **Login** and **Email address** fields using credentials of the administrator whose password you would like to restore.

   The email address you enter must match the address specified in the administrator account preferences.
4. Click **Send link**. An email with embedded link to reset the password will be sent to the specified email address.

   The email will be sent only if you configured the SMTP server beforehand (see Email for details).
5. Follow the specified link and set a new password on the opened page. If you did not receive the email, please try again.

To change the password when launching Dr.Web Server from the command line:

Launch Dr.Web Server from the command line while including the necessary parameter, administrator login and a new password.

- for **Windows** OS:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" modexecdb set-admin-password <login> <new_password>
```

- for **Linux** OS:

```
/etc/init.d/drwcsd modexecdb set-admin-password <login> <new_password>
```

- for **FreeBSD**:

```
/usr/local/etc/rc.d/drwcsd modexecdb set-admin-password <login>
<new_password>
```

6.3.3. Editing Administrative Accounts and Groups

To edit accounts of administrators and administrative groups, you need to have the **Edit administrative accounts** and **Edit properties and configuration of administrative groups** permissions.

To edit own administrative account, you need to have the **Edit own settings** permission.

Fields marked with the * sign must be specified.

To edit an administrative account

1. Select the account you want to edit from the list of administrators. The properties section will be opened for editing.
2. The **Main** subsection contains properties that were set during account creation. Also, please note:
   a) To change the password for the administrative account, click the **Change password** icon on the toolbar.

   An administrator with corresponding permissions can change passwords of all other administrators.

   Login for administrative account cannot contain national characters.

   b) The following properties of the administrator account are read-only:
      - Account creation date and its properties last change date,
      - **Status**—displays network address of the last connection under the current account.
3. In the **Groups** subsection, you can change an administrative group. The list contains groups to which an administrator can be assigned. The flag is set next to the current parent group of administrator. To change assigned group, set the flag next to the required group.

   It is mandatory to assign a parent group to the administrator. Each administrator can be included only to the one group at a time. Permissions of administrator are inherited from the parent group.

See also the Editing membership subsection.

4. In the **Permissions** subsection, you can edit the list of actions that are allowed for the selected administrator.

   Details on editing permissions are described in the Editing permissions subsection.

5. Click **Save** to apply changes.

To edit an administrative group

1. Select the group you want to edit from the list of the administrators. Click the group name to open its properties section for editing.
2. The **Main** subsection contains properties that were set during group creation.
3. In the **Groups** subsection you can change the parent administrative group. The list contains groups which can be assigned as a parental group. The flag is set next to the current parent group. To change assigned group, set the flag next to the required group.

   It is mandatory to assign a parent group to the administrative group. The group inherits permissions from its parent group.

   See also the Editing membership subsection.

4. In the **Permissions** subsection, you can edit the list of actions that are allowed for the selected administrative group.

   Details on editing permissions are described in the Editing permissions subsection.

5. Click **Save** to apply changes.

To assign a parent group for an administrator or an administrative group, use one of the following ways:

- Change administrator settings or group settings as described above.
- Drag and drop administrator or administrative group from the hierarchical tree to the group you want to assign as a parent group.

To propagate permissions of an administrator or group on another administrator or group

1. In the list of administrators, select one object permissions of which you want to propagate. It can be either administrator or administrative group.
2. On the toolbar, click **Propagate administrator permissions**.
3. In the opened window, select objects to assign permissions. Please note the following features:
   - You can select one or several objects to assign permissions. It can be either administrators or administrative groups.
   - Permissions are saved for selected objects as a personal. Inheritance with a parent group became broken.

- You cannot assign permissions to default objects (the **Administrators**, **Newbies** groups, the **admin** administrator).
- You can propagate permissions only on objects allowed in the **Edit administrators accounts** and **Edit properties and configuration of administrative groups** permissions.
- If the propagation causes assignment of permissions that exceed the own permissions of administrator who perform the operation, the error about insufficient permissions to perform the operation is returned.

4. Click **Propagate**.

Chapter 7: Integrated Workstations Management

For the integrated management of stations and their settings, the following tools are provided:

- Groups.

  Station can be included into unlimited number of groups. Obligatory into predefined groups according to a station state and optionally into user groups. But only one of these groups is primary.

- Policies.

  Only one policy or none of policies can be assigned to a station.

- Profiles.

  Profiles are used to specify the settings of the Application Control component. Profiles can be assigned to stations and groups of stations and also individual users.

  To control the launch of applications on stations, at least one active profile must be assigned to the station or to the station user.

Station Settings Types

- **Inherited settings.**

  When creating a new station, its settings are always inherited from a policy or a primary group. Detailed information is given in the Inheriting Stations Configuration section.

- **Personal settings.**

  During a station operation, inheritance can be broken and personal settings are set.

  To set the personal settings for a station, edit corresponding settings section.

  If the personal settings are specified for a station, then settings of assigned policy or personal group settings and their changing will not have any affect on station settings.

  You can restore the inheritance from a policy or a primary group. To do this, click the **Remove personal settings** button on the toolbar of the Control Center, in the corresponding settings section or in a station properties section.

  In each settings section of workstation configuration elements, the information that settings of this section are set personally or inherited from a corresponding object is displayed.

  A part of the settings sections can be set personally and a part be inherited from a policy or a primary group if the policy is not specified.

You can set different configurations for different groups and stations, by editing corresponding settings.

7.1. Inheriting Stations Configuration

When creating a new station or a group, their settings are always inherited:

- A new group inherits settings from its parent group into which it is directly included. If it has no parent group (created group is a root group in hierarchical tree), its settings are inherited from the **Everyone** group.
- A new station inherits settings from a policy that had been assigned during the station creating. If a policy has not been assigned, station settings are inherited from one of the groups to which the station is included. That group is called a *primary group*.

During further operation, inheritance can be broken and personal settings are set for the station.

For the Application Control component, settings inheritance principle differs from the typical. For more details, see Settings Inheritance for the Application Control component.

Priority of applying settings for a station:

1. If a station has personal settings, the personal settings will be used. At this, a policy can be assigned to a station. If personal settings of specific section are set, the inheritance for this section is broken.
2. If a station has no personal settings, applied policy settings are used.
3. If a station has no personal settings and no policy applied, a station uses settings of its primary group.

Personal settings are set	Policy is assigned	Used settings
+	+	Personal settings
+	–	Personal settings
–	+	Policy settings
–	–	Primary group settings

None of policies can be assigned to a station but a stations always has a primary group.

Inheritance of Station Settings from Policies

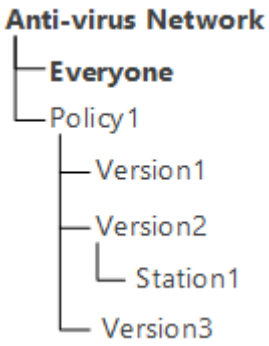
If a policy is assigned to a station, the inheritance of station settings from policies settings is set.

If the settings of the policy are modified, these changes are inherited by all stations for which this policy is assigned, unless the personal settings have been set to stations. When creating a station, you can specify what policy will be assigned to a station. A policy can be replaced in any time during operation. If no policy is assigned, settings will be inherited from a primary group.

Policies have no hierarchical structure of inheritance. When policy is created, its settings are copied as a personal settings from the specified object (the **Default policy** by default). Only one policy version is the current and its settings are the settings of the policy itself. Only the current version can be assigned to stations.

Example

The structure of hierarchical list is the following:



For the `Station1` station the `Policy1` policy is assigned. The `Version2` policy version is the current for the `Policy1` policy. Settings of the `Version2` version are the same as the `Policy1` policy settings which are personal.

Inheritance of Station Settings from Groups

If the policy is not set for a station, the settings of a station get inherited from the settings of a primary or group.

If the settings of a primary group are modified, these changes are inherited by all stations included into the group, unless the personal settings have been set to stations. When creating a station, you can specify what group will be set as primary. By default the primary group is **Everyone**. A primary group can be replaced in any time during operation.

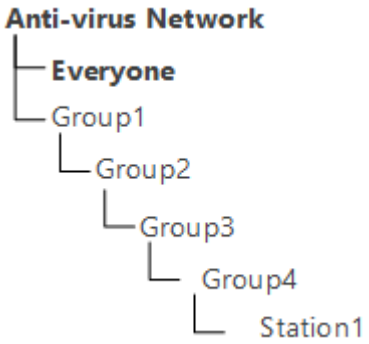
If **Everyone** is not a primary group, and a different primary group that is a root group in hierarchical tree, has no personal settings, the settings of the **Everyone** group are inherited by a new station.

It is possible to create nested groups.

In nested groups, If a station has no personal settings, the inheritance of the configuration elements is performed according to the structure of nested groups. The search is performed upwards through the hierarchical tree, starting from the station primary group, its parent group and so on till the root element of the tree. If no personal settings are found, then configuration elements of the **Everyone** group are inherited.

Example

The structure of hierarchical list is the following:



The `Group4` is the primary group for the `Station1`. To determine which settings to inherit for the `Station1`, the search is carried out in the following order: `Station1 → Group4 → Group3 → Group2 → Group1 → Everyone`.

By default the network structure is displayed in such a way as to show a station in all the groups it is included into. If you want stations to be displayed in the network catalog in their primary groups only, on the toolbar of the Control Center in **Settings of tree view**, clear the **All groups membership** flag.

Inheritance of Application Control Settings

Settings of Application Control profiles can be assigned not only to stations and groups of stations, but also to individual users and groups of users.

Priority of applying settings:

1. If user settings are specified, they have the highest priority.
2. If user settings are not specified, the group of users have the priority.
3. If neither user settings nor group of users settings are specified, the inheritance is implemented according to the priority of applying settings for a station.

7.2. Groups

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

Grouping of stations may be used for the following purposes:

- Group operations over all stations, included to these groups.

  As for separate group so and for several selected groups, you can launch, view and stop scan tasks on stations, included to this group. In the same way, you can view statistics (including detected threats, start/stop, scan and installation errors and etc) and summary statistic for all workstations of the group or several groups.
- Settings the single parameters for stations via the group, to which these stations are included (see p. Chapter 7: Integrated Workstations Management).
- Order (structure) the list of workstations.

It is possible to create nested groups.

7.2.1. System and User Groups

System Groups

Dr.Web Enterprise Security Suite has an initial set of pre-installed system groups. These groups are created during the installation of Dr.Web Server and may not be deleted. Still the administrator may disable their display, if necessary.

Each system group except **Everyone** contains a set of feature-packed subgroups.

After Dr.Web Server has been installed, until no station connected, the list of system groups displays the **Everyone** group only. To display all system groups, use the **Show hidden groups** option in the **Settings of tree view** section of the toolbar.

Everyone

Group contains all stations known to Dr.Web Server. The **Everyone** group has default settings of all groups and stations.

Active Directory

Group contains users and user groups registered in the Active Directory domain. This group appears in the anti-virus network tree after executing the **Synchronization with Active Directory** task from the Dr.Web Server schedule.

Configured

Group contains stations which have personal settings specified.

Neighbors

The **Neighbors** group contains all Dr.Web Servers connected to this Dr.Web Server and designed to manage connections between Dr.Web Servers in a multi-server anti-virus network (for more details, see Peculiarities of a Network with Several Dr.Web Servers).

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

The **Neighbors** group contains subgroups displaying the state of neighbor Dr.Web Servers connected to this Dr.Web Server:

- **All neighbors** group contains all neighbor Dr.Web Servers connected to this Dr.Web Server.
- **Children** group contains subordinate Dr.Web Servers.
- **Offline** group contains currently offline Dr.Web Servers.
- **Online** group contains currently online Dr.Web Servers.
- **Parents** group contains main Dr.Web Servers.
- **Peers** group contains peer Dr.Web Servers.

Operating system

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

- **Android** family groups. This family includes a set of groups, that correspond to specific version of Android OS for mobile devices.
- **macOS** family groups. This family includes a set of groups, that correspond to specific version of macOS operating system.
- **UNIX** family groups. This family includes a set of groups, that correspond to OS of Unix-like systems, for example, Linux, FreeBSD, etc.
- **Windows** family groups. This family includes a set of groups, that correspond to specific version of Windows operating system.
- **Unknown OS** category. It includes stations working under an OS that is unknown to Dr.Web Server.

Policies

Group contains policies for configuring stations.

The **Policies** group is displayed in the anti-virus tree only if using policies is allowed in the Dr.Web Server configuration.

Profiles

Group contains profiles with settings of the Application Control component for stations under Windows OS. See Profiles.

Proxies

Group contains Dr.Web Proxy Servers for connecting Dr.Web Agents and neighbor Dr.Web Servers.

Status

The **Status** group contains subgroups reflect the current status of the station, that is if it is connected to Dr.Web Server or not at the moment. These groups are completely virtual, may not have any settings or be primary groups.

- **Deinstalled** group. Once Dr.Web Agent software has been deinstalled from a station, the station is transferred to the **Deinstalled** group.
- **Deleted** group contains stations, which were deleted by an administrator from Dr.Web Server. Such stations can be restored (see p. Removing and Restoring Stations).
- **New** group contains new stations, which have been created by administrator via Dr.Web Security Control Center, but Dr.Web Agent is not installed yet.
- **Newbies** group contains all stations not registered at Dr.Web Server at the moment. When the registration is approved, stations will be removed from this group automatically (see the New Stations Approval Policy section for more details).
- **Offline** group contains all workstations not connected at the moment.
- **Online** group contains all workstations connected at the moment (reacting to the Dr.Web Server requests).

Transport

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

- **TCP/IP** group contains workstations connected at the moment through the TCP/IP protocol.
- **TCP/IP Version 6** group contains workstations connected at the moment through the TCP/IP version 6 protocol.

Ungrouped

Group contains stations, which are not included in any of user groups.

User Groups

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

In the table 7-1, all possible groups and group types are given for your reference, along with the specific parameters supported (+) or not supported (–) by the groups.

The following parameters are considered:

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

Table 7-1. Groups and supported parameters

Group/group type	Parameter			
	Automatic membership	Membership administration	Primary group	Possibility to have own settings
Everyone	+	–	+	+
Configured	+	–	–	–
Operating system	+	–	+	+
Status	+	–	–	–
Transport	+	–	–	–
Ungrouped	+	–	–	–
User groups	–	+	+	+

Under *group administrator* account, the user group which he manages will be the root of the hierarchical tree, even if it has the parent group. At this, all nested groups of managing group are available.

7.2.2. Group Management

7.2.2.1. Creating and Deleting Groups

To create a new group

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. Select **Add a network object** on the toolbar and **Create group** in the submenu.

   A window for creating a group will be opened.
3. The **Identifier** field is filled automatically. You can edit it during creation, if necessary. The identifier should not contain spaces. In the sequel, a group identifier cannot be changed.
4. Specify a group name in the **Name** field.
5. For nested groups, in the **Parent group** field, select from the drop-down list a parental group to inherit configuration from it if personal settings are not specified. For a root group (without a parent), leave this field blank to add the group to the root of the hierarchical tree. In this case settings are inherited from the **Everyone** group.
6. Specify optional comment in the **Description** field.
7. Click **Save**.

The groups you create are initially empty. Procedure of including workstations to groups is described in the Including Stations into Groups section.

To delete existing group

1. Select the user group in the hierarchical list of the Control Center.
2. Click **General** → **Remove selected objects** on the toolbar.

> You cannot delete pre-installed groups.

7.2.2.2. Editing Groups

To edit group properties

1. Select the **Anti-virus network** item in the main menu of the Control Center, then select the group in the hierarchical list of the opened window.
2. Open the group properties section by one of the following ways:
   a) Click the name of the group in the hierarchical list of anti-virus network. A panel with properties of the group will be automatically opened in the right part of Dr.Web Security Control Center.

b) Click **Properties** in the control menu. A window with the group properties will be opened.

3. The window with the group properties contains the **General** and **Configuration** sections, which contain editable parameters of the selected group. These sections and their parameters are described below.

If you open group properties in the right part of the Control Center (see step **2.a)**), the **Station details** section with general information about stations in this group becomes available as well.

4. Edit group properties.
5. Click **Save** to save all changes.

General

In the **General** section, the following information is given for any selected group:

- **ID**—group unique identifier. Is read-only.
- **Name**—group name. You can change the group name, if necessary. For pre-installed groups, the **Name** field is read-only.
- **Parent group**—parent group in which this group is included and from which group configuration is inherited, if the personal settings are not specified. If a parent group is not specified, settings are inherited from the **Everyone** group.
- **Description**—optional filed with group description.

If a user group is selected, the following items are also available:

- **Profile**—Application Control profile assigned to this group.
- **Installation package**—links for downloading Dr.Web Agent installation packages for this group.

  The availability of installation package links for different operating systems depends on whether the corresponding installers are present in the Dr.Web Server repository.
- **Configuration file**—link for downloading the file with Dr.Web Server connection settings for stations running Linux, Android and macOS operating systems that are included in this group.

Station details

In the **Station details** section, the following information is presented:

- **Total stations**—total number of stations which are included into this group.
- **Primary group for**—number of stations for which this group is primary.
- **Stations online**—number of stations in this group which are currently online.
- **Location**—information on the location of stations in this group. **Show on map**—link to an OpenStreetMap with placemarks corresponding to the coordinates of stations in the group

specified in the **Latitude** and **Longitude** fields in the station properties. The link is available if at least one station in the group has its **Latitude** and **Longitude** fields filled in.

Configuration

For more details on inheriting settings by stations from primary groups, see the Chapter 7: Integrated Workstations Management section.

In the **Configuration** section, the following groups parameters are presented:

Icon	Settings	Description section
	Permissions for workstations, which inherit this setting from a group if it is primary. Setting permissions of groups is similar to setting permissions of separate workstations.	Permissions of Station Users
	Centralized task schedule for workstations, which inherit this setting from a group if it is primary. Setting schedule of group is similar to setting centralized schedule of separate workstations.	Scheduled Tasks of a Station
	License key file for workstations, which inherit this setting from a group if it is primary.	License Keys
	Restrictions for anti-virus software updating for workstations, which inherit this setting from a group if it is primary.	Update Restrictions for Workstations
	List of installable components for workstations, which inherit this setting from a group if it is a primary group. Editing the component list of a group is similar to setting the component list of a station.	Installable Components of the Anti-Virus Package
	Configuring automatic placing the stations into the group. Available for user groups only.	Configuring Automatic Group Membership
	Settings of the anti-virus components. Setting the anti-virus package components of group is similar to setting the anti-virus package components of separate workstations.	Management of Anti-virus Components

Groups with personal settings in the **Configuration** section, also contain the number of nested groups with broken inheritance and own personal settings, if such are present. Click this option to open the window displaying the list of groups with their names and identifiers given.

7.2.3. Including Stations into Groups

Setting a Primary Group

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

To set primary group for station

1. In the main menu, select **Anti-virus network**, then click the name of a workstation in the hierarchical list.
2. The station properties panel opens. Also, you can open the stations properties section by selecting **Properties** in the control menu. In the opened window, go the **Groups** section.
3. If you want to reassign the other primary group, click an icon of necessary group in the **Membership** list. The **1** sign displays on the icon.
4. Click **Save**.

To set primary group for several stations

1. In the main menu, select **Anti-virus network**. In the hierarchical list of the opened window, click the name of workstations (you can select groups of workstations either, in such case, the action spreads on all stations in the group) for which you want to set a primary group. To select several workstations and groups, press and hold CTRL or SHIFT during mouse selection.
2. On the toolbar, click **General** → **Set a primary group for stations**. This opens the window listing the groups which can be set as primary for the selected workstations.
3. Click the name of a group to set it as primary.

You can also make a group primary for all workstations included into it. To do this, select the necessary group in the hierarchical list, and click **General** → **Set this group as primary** on the toolbar.

Including into User Groups

Dr.Web Enterprise Security Suite provides the following ways how to place stations into user groups:

1. Place stations into groups manually.
2. Use automatic group membership.

7.2.3.1. Including Stations into Groups Manually

There are several ways how to add a workstation to a user group manually:

1. Change the station settings.
2. Drag and drop a station in the hierarchical list.

To edit the list of groups a station is included in via the station settings

1. In the main menu, select **Anti-virus network**, then click the name of the workstation in the hierarchical list.
2. The station properties panel opens. You can also open the station properties section by selecting **Properties** in the control menu.
3. In the **Properties of station** panel, navigate to the **Groups** section.

   Click **Edit** in the **Membership** list. The window that opens displays all the groups the workstation is already included in and can be included in.
4. To add the workstation to a group, set the flag next to this group.
5. To remove the workstation from a group, clear the flag next to this group.

   You cannot remove stations from pre-installed groups.
6. To save your changes, click **Apply** in the editor window and then click **Save** in the station properties panel.

In the **Properties** section, you can also set a group as the primary one for the station (for more details, see Inheriting Stations Configuration).

To edit the list of groups a station is included in via the hierarchical list

1. In the main menu, select **Anti-virus network** and unfold the hierarchical list of groups and stations.
2. To copy a station to the user group, press CTRL and drag and drop a station to the corresponding group.

   To move a station from one user group to another, drag and drop a station to the corresponding group.

   When dragging a station from pre-installed group in both cases station is added in the user group and is not removed from pre-installed group.

7.2.3.2. Configuring Automatic Group Membership

Dr.Web Enterprise Security Suite allows you to configure the rules of automatic inclusion of stations into user groups.

Automatic placement of stations in a group

To specify the rules for automatic inclusion of stations in a group

1. Select **Anti-virus Network** in the main menu of the Control Center.
2. From the hierarchical list of the anti-virus network, select a user group for which you want to specify membership rules.
3. Open the membership rules editing section in one of the following ways:
   - In the group properties pane on the right side, click **Group membership rules** in the **Configuration** section.
   - In the control menu, in the **General** section, select **Group membership rules**.
   - In the control menu, in the **General** section, select **Properties**, open the **Configuration** tab and click **Group membership rules**.
4. If no group membership rules have been specified before, click **Add the rule**.
5. If needed, select the **Set group as primary** check box to automatically assign the group for which the rule is created as the primary group for all stations that will be moved to this group according to this rule.
6. Select one of the options that determine how the rules will be applied:
   - **Apply rules after saving**—apply these rules immediately after clicking the **Save** button to all stations registered on this Dr.Web Server. If there are a large number of stations connected to Dr.Web Server, performing this action may take some time. Rules for regrouping stations are applied to all already registered stations immediately after the action is set and will be applied further to all stations, including those registered with Dr.Web Server for the first time, at the time of their connection.
   - **Apply rules on stations connect**—apply these rules to stations at the moment of their connection to Dr.Web Server. Rules for regrouping stations are applied to all already registered stations at the moment of their next connection to Dr.Web Server and will be applied to all stations registered with Dr.Web Server for the first time at the time of their first connection.
7. Membership rules are grouped into blocks. Specify the following settings for each block of rules:
   a) Select one of the options that determine how the rules are combined inside this block: **Matches all conditions**, **Matches any of conditions**, **Does not match any of conditions**.
   b) From the condition drop-down lists, select a station parameter that will be checked for compliance with the conditions and the principle of compliance with this condition. If the

station parameter implies it, specify the condition string in the input field to the right of the drop-down lists.

Stations can be combined into groups based on the following conditions:

- **Dr.Web Server ID** of the Dr.Web Server the station connects to (a set of characters contained in the ID or a regular expression);
- **Station ID** (a set of characters contained in the ID or a regular expression);
- **IP address** (a set of characters contained in the IP address, the subnet it is part of, or a regular expression);

Grouping stations based on the **IP address** condition does not work correctly if DNS names are written in the workstation address fields in the Control Center instead of IP addresses (the **Replace IP addresses** flag is set in the **Administration → Dr.Web Server configuration** section on the **General** tab). If you want to group stations by their addresses, there are two ways of resolving the conflict between these settings:

- clear the **Replace IP addresses** flag on the **General** tab in the **Administration → Dr.Web Server configuration** section;
- when selecting the **IP address** parameter, instead of specifying characters contained in the IP addresses of stations, specify characters contained in their DNS names, or an appropriate regular expression. Specifying the subnet is not allowed in this case.

- **LDAP DN from Active Directory** (a set of characters contained in the LDAP DN or a regular expression);

If you select the **LDAP DN from Active Directory** parameter, perform the following:

1. Enable the **Synchronization with Active Directory** task in the Dr.Web Server schedule (**Administration → Dr.Web Server Task Scheduler**).
2. In the membership rules, specify the required DN as a condition string for the **LDAP DN from Active Directory** parameter, for example:
   `OU=OrgUnit,DC=Department,DC=domain,DC=com`

- **Station name** (a set of characters contained in the name or a regular expression);
- **Newbie** (stations are added to the group based on whether or not they have the newbie status);
- **Operating system build** (a set of characters contained in the build number or a regular expression);
- **Operating system** installed on the station (Windows, UNIX, macOS, Android, etc.; the Unknown value is also available);
- **Description** (a set of characters contained in the description or a regular expression);
- **Station platform** (the version of the OS installed on the station);
- **Connection protocol** (TCP IP, TCP IPv6, UNIX);
- **Station type** (Full agent, Virtual agent, Scanning server).

You may use regular expressions only for the **matches regular expression** option. All other options search for the exact match of the entered string.

Regular expressions are briefly described in the **Appendices** document, section Appendix I. Regular Expressions Used in Dr.Web Enterprise Security Suite.

To add another condition to this block of rules, click  to the right of the condition string.

c) To add a new block of rules, click  to the right of the block. Specify the principle of combining this block of conditions with other blocks:

- **AND**—conditions of the blocks must be fulfilled simultaneously,
- **OR**—conditions of at least one of the blocks must be fulfilled.

If several blocks are joined by **AND** and **OR** operators, **AND** takes the priority. For instance, if your sequence of blocks looks like [1] **AND** [2] **OR** [3] **AND** [4], stations will be placed in the group according to this representation: ([1] **AND** [2]) **OR** ([3] **AND** [4]).

8. If you would like to check whether a certain station meets the conditions specified in the group membership rules first, click **Check station**. Select the station in the hierarchical list and click **Check**. The window then displays a message about whether the station meets the group membership requirements.
9. To save and apply the changes, click **Save**.

When automatic membership rules are specified for a user group, the  icon is displayed next to the icon of this group in the hierarchical list, if the **Show membership rule icon** check box is set in the  **Settings of tree view** list on the toolbar.

Automatic removal of stations from groups

If a station was automatically included in a user group according to the membership rules, manually removing the station from this groups makes no sense, because the station will be automatically returned to this group the next time it connects to Dr.Web Server. To exclude an automatically station (stations) from the group, you can use one of the following methods:

- Change the station parameters in such a way that they no longer meet the group membership conditions. The station will be excluded from the group once it connects to Dr.Web Server.
- Add an additional rule or block of rules with the **AND** operator and specify conditions that are met by all stations in the group but the station in question. The station will be excluded from the group in accordance with the selected rule application option (see step 6).
- Add an additional block of rules with the **AND** operator, select the **Does not match any of conditions** combination principle and create a rule to be uniquely matched by the station in question. The station will be excluded from the group in accordance with the selected rule application option (see step 6).

To remove rules for automatic inclusion of stations in a group

1. Select **Anti-virus Network** in the main menu of the Control Center.
2. From the hierarchical list of the anti-virus network, select a user group for which you want to remove membership rules.
3. Perform one of the following actions:
   - On the toolbar, click **Remove membership rules**.
   - In the group properties pane on the right side, click **Remove membership rules** in the **Configuration** section.
   - In the control menu, select **Properties** in the **General** section, open the **Configuration** tab and click **Remove membership rules**.

After group membership rules are removed, all stations included in the group will be automatically removed. If this group was set by the administrator as the primary group for any of these stations, the **Everyone** group will be set as the primary group for these stations after they are removed from the group.

7.2.4. Comparison of Stations and Groups

You can compare stations and groups by general parameters.

To compare several objects of the anti-virus network

1. In the main menu, select **Anti-virus network**, then select the objects you want to compare in the hierarchical list. Use CTRL and SHIFT for this. The following variants are possible:
   - selection of several stations—to compare selected stations;
   - selection of several groups—to compare selected groups and all nested groups;
   - selection of several stations and groups—to compare all stations: selected directly in the hierarchical list and included in all groups and their nested groups.
2. In the control menu, click **Comparison**.
3. The comparison table for selected objects will be opened.
   - Comparative parameters for groups:
     - **Stations**—total number of stations which are included into this group.
     - **Stations online**—number of online stations.
     - **Primary group for**—number of stations for which this group is parental.
     - **Personal configuration**—list of components with personal settings, not inherited from the parental group.
   - Comparative parameters for stations:
     - **Created on**—date and time when the stations were created.
     - **Primary group** for the stations.

- **Personal configuration**—list of components with personal settings, not inherited from the primary group.
- **Installed components**—list of anti-virus components installed on the stations.

7.2.5. Propagation of Settings to Other Groups/Stations

Configuration settings of anti-virus programs, schedules and user permissions and other settings of a group or a workstation can be copied (propagated) to other group or several groups and workstations.

To propagate settings

1. Click **Propagate these settings to another object** in the one of the following locations:
   in the editor of anti-virus component configuration,
   in the schedule editor,
   in the update restrictions window,
   in the installable components window,
   in the window for stations user permissions setup.
   A window of the anti-virus network hierarchical list will be opened.
2. Select necessary groups and stations to which you want to propagate the settings.
3. To enable changes in the configuration of these groups, click **Save**.

7.3. Policies

Policy is a set of all existing station settings: permissions, task schedule, license keys, update restrictions, the list of installed components, configuration of anti-virus components.

Policy can be assigned to stations only.

To allow using policies to configure stations

1. Select the **Administration** item in the main menu of the Control Center; in the opened window, select the **Dr.Web Server configuration** item of the control menu.
2. On the **General** tab:
   a) Set the **Use policies** flag.
   b) In the **Policy versions number** field, specify the number of versions that can be created for each policy, in addition to the current version. If this value is exceeded during the creation of a new policy version, the oldest policy version will be deleted.
3. Click **Save** and restart Dr.Web Server.

4. After you allow the use of policies, the **Default policy** predefined policy is created. You cannot delete this policy, but you can edit it and assign it to stations.

To manage policies and their settings, administrator must have the **View policies properties and configuration** and **Edit policies properties and configuration** permissions.

If the permissions are not assigned, policies are displayed in the anti-virus network tree and in the License manager but viewing their content and managing them are not provided.

7.3.1. Policy Management

Creating Policy

To create a new policy

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. Select **Add a network object** on the toolbar and **Create policy** in the submenu.

   A window for creating a policy will be opened.
3. The **Identifier** field is filled automatically. You can edit it during creation, if necessary. The identifier should not contain spaces. In the sequel, a policy identifier cannot be changed.
4. Specify a policy name in the **Name** field.
5. When creating a policy, its settings are copied from the **Default policy** by default. To change the object from which the settings will be copied, click the **Select another object** link. In the opened window, select the object from the given list. It can be a group, a station, other policy or a policy version. You can select only one object. Click **Save**. The selected object will be displayed in the policy creation window.
6. Click **Save** to create policy with the specified settings.
7. When creating a policy, a policy version that corresponds to the date of a policy adding is created automatically.

Policy Versions

Policy can have several versions but not more than specified in the settings of the Dr.Web Server configuration. Policy version name corresponds to the time of its creation.

To create a new policy version

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. You can access the policy configuration via the hierarchical list of the anti-virus network. Edit the configuration of the policy for which you want to create a new version. You can do it

manually or using the import/propagation of the configuration from other object of the anti-virus network (station, group, policy).

3. When saving the changes, a new policy version will be created automatically on a base of specified settings of the policy. Created version will be assigned as a current.

Only one version of a policy is the current and can be assigned to stations.

Configuration of a policy version is read-only.

To change the current version of a policy

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. In the hierarchical list, select a policy current version of which you want to change.
3. On the opened properties pane of a policy, in the **General** section, select the necessary version in the **Current version** drop-down list.
4. Click **Save**.

Removing Policy

You can remove policies either whole or by versions.

To remove policy or policy version

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. Select a policy or a policy version in the hierarchical list.
3. Click **General** → **Remove selected objects** on the toolbar.

When removing a policy, please note the following features:

- When removing the last version of a policy, the policy is also removed.
- If you remove a current policy version, the latest version (with the last date) become a current.
- To all stations to which the removed policy version was assigned, the current version of this policy will be assigned.

7.3.2. Assigning Policy to Stations

Only one policy can be assigned to a station.

Only the policy to which the license key is specified, can be assigned to stations.

To assign or change a station policy

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. In the hierarchical list, select a station to which you want to assign or change policy.
3. On the opened properties pane of a station, in the **Groups** section, in the **Policy** list, set the flag next to the policy you want to assign.

   If a policy was already assigned earlier, its flag will be automatically cleared because only one policy can be assigned to a station.

   Also, you can clear all the flags from all policies. In this case, the settings of a station will get their previous state that was before policy assigning.
4. Click **Save**.

7.4. Profiles

Profiles define the Application Control settings, which specify whether applications, modules, script interpreters, drivers and MSI packages on stations will be launched or blocked.

Profiles are created by the administrator and are assigned to policies, stations and users, as well as groups of stations or users. Profiles define the Application Control operation mode.

Profiles are configured via the anti-virus network tree:

- All profiles are located in the preinstalled **Profiles** group.
- Objects with assigned profile are placed nested under this profile in the anti-virus network tree.

To configure Application Control

1. Create a new profile.
2. Configure settings of the created profile.
3. Assign the created profile to necessary objects.

It is recommended that profiles are configured in test mode.

Possible operation modes for profiles:

- **Disabled**—profile is not active, profile settings are not applied.
- **Active**—profile is active, settings are applied for objects on which the profile is propagated.

- **Test** *global*—profile is active but operates in global test mode. This test mode imitates operation of Application Control with full activity logging (see Application Control Events), but no application is getting blocked.
- **Test** *for rules*—profile is active and both functional analysis settings and rules are propagated to objects. However the rules switched to test mode have no impact on applications being blocked. Results of their imitated actions are kept in the activity log (see Application Control Events). The test mode can be enabled or disabled in allow and deny rule settings.

  The table below illustrates which options are responsible for specific profile operation mode.

Mode / Option	Disabled	Active	Test *global*	Test *for rules*
General → Enable profile	–	+	+	+
General → Switch profile to global test mode	inactive	–	+	–
<Mode> → *<Rule>* → **Enable rule**	inactive	+/–	+/–	+
<Mode> → *<Rule>* → **Switch rule to test mode**	inactive	–	+/–	+

Conventions

+	option shall be enabled
–	option shall be disabled
+/–	option does not matter
inactive	option is not editable

7.4.1. Creating and Assigning Profiles

To create a new profile

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. On the toolbar of the opened window, select **Add a network object** → **Create profile**.
3. On the opened pane, specify **Profile name**. If necessary, you can change it further in the General section of the settings.
4. Click **Save**.
5. New profile will be created and placed to the **Profiles** group.

To assign profile to an object

1. Select the **Anti-virus network** item in the main menu of the Control Center.

2. In the hierarchical list of the opened window, select profile you want to assign.
3. On the toolbar, click **Data and configuration** → **Assign profile**.

   In the opened window, select the object to propagate settings:

   - On the **Active Directory** tab, the lists are given that are similar to the list in the anti-virus network tree which is updated according to the **Synchronization with Active Directory** task from the Dr.Web Server schedule. These lists are identical in composition of users, but different by the type of objects for which the profile will be assigned:
     - In the **Active Directory stations** list, you can select stations registered in the Active Directory domain.
     - In the **Active Directory users** list, you can select users and groups of users registered in the Active Directory domain.

     The same objects should not be selected in different lists.

   - On the **Anti-virus network** tab, you can select the following objects:
     - Station groups. In this case, settings will be propagated on accounts of all users of stations included into these groups.
     - Separate stations in groups. In this case, settings will be propagated on accounts of all users of the selected stations.
     - Policies in the **Policies** group. In this case, settings will be propagated on accounts of all users of the stations the selected policy is assigned to.
   - On the **Local users** tab, you can select a user group or individual users at stations. In this case, settings will be propagated only on accounts of the selected users.

   For more details on priorities when assigning profiles, see Inheriting Stations Configuration.
4. Click **Save**. All selected objects will be added to the list to which the configured profile propagated (displayed in the tree as nested objects of this profile).

To unassign profile from an object

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. In the hierarchical list of the opened window, open the objects list of the profile and select the object from which you want to unassign the profile.
3. On the toolbar, click **General** → **Unassign the profile from the objects**.

7.4.2. Configuring Profiles

To edit profile settings

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. Open the profile properties section by one of the following ways:

a) Click the name of the profile in the hierarchical list of anti-virus network. A panel with properties of the profile will be automatically opened in the right part of the Control Center.

b) Click the icon of the profile in the hierarchical list of anti-virus network or select the profile, when click **Properties** in the control menu. A window with the profile properties will be opened.

3. On the **General** tab, you can specify principles of the profile operation:
   - In the **Profile name** field, you can change the profile name.
   - Set the **Enable profile** flag to start using this profile.
     - Setting the **Switch profile to global test mode** flag will enable activity logging only, as with enabled settings. You can use this mode to debug profile operation.
   - On the Functional Analysis section, specify the set of predefined rules by which applications will be allowed or prohibited to launch.
4. To apply the settings specified in the **General** section, click **Save** in the profile properties.
5. The **Allow mode** section contains the general summary on the mode settings: the number of created allow rules and trusted applications groups that are assigned on this profile. To enable or disable the mode, and also configure the rules and trusted applications, click the Allow Mode link to open the corresponding section.
6. The **Deny mode** section contains the general summary on the mode settings: the number of created deny rules. To enable or disable the mode, and also configure the rules, click the Deny Mode link to open the corresponding section.

Please note the following features of the Application Control profile operation:

- If no criteria are enabled in the **Functional analysis criteria** section, the profile itself will be disabled.
- If none of the criteria in the **Functional analysis criteria** section has an additional settings specified and allow and deny modes are disabled, such configuration will not be saved.
- If neither allow rules nor trusted applications are specified, allow mode will be disabled.
- If no deny rules are specified, the deny mode will be disabled.

7.4.2.1. Functional Analysis

Functional analysis specifies the set of predefined conditions by which applications are allowed or prohibited to be launched in accordance with the functions performed.

Functional analysis is configured in the **General** → **Functional analysis criteria** section of the profile preferences.

If no criteria are enabled in the **Functional analysis criteria** section, the profile itself will be disabled.

If none of the criteria in the **Functional analysis criteria** section has an additional settings specified and allow and deny modes are disabled, the profile itself will be disabled.

To configure functional analysis

1. In the **Functional analysis criteria** section, set the flags for categories you want to use:
   - **Application launch**,
   - **Modules load and execution**,
   - **Launch of script interpreters**,
   - **Drivers loading**,
   - **MSI packages installation**,
   - **Executable files integrity**.

   If you configure a profile for the first time, then at enabling each of criterion, its permissive categories in additional settings are automatically enabled.

   This feature is used as a security measure if, after applying settings of allow or deny modes, the objects of the operating system necessary for the operation of the station are blocked.

   Further, if necessary, you can disable these permissive categories in additional settings.

2. To specify the additional settings for the selected criterion, click **Edit** next to the corresponding criterion. The window with the settings list will be opened.

   Functional analysis additional settings can be either permitting or prohibiting the launch of applications.

   Set the flags for those settings that must be followed.
3. If you enable any of criterion but do not specify its additional settings, then the launch will be controlled for all objects under this criterion in accordance with the settings of allow or deny modes.

   For example:

   - If the **Launch of script interpreters** criterion is set but its additional settings are not set, then the launch of all script interpreters will be controlled in accordance with the settings of allow or deny modes.
   - If the **Launch of script interpreters** criterion is set and its additional setting **Prevent running of scripts from removable media** is set, then only running of scripts from removable media will be forbidden.
4. If you specify additional settings, but do not enable the use of the criterion itself, neither the additional settings nor the criterion itself will be used.
5. To save the additional settings, click **Save** in the window with the additional settings list.
6. To save the settings of the functional analysis, click **Save** in the window with profile settings.

7.4.2.2. Allow Mode

Allow mode means that on all monitored stations, only applications from the **Trusted applications** list and\or applications that comply with the allow rules are allowed to run. All other applications are blocked based on functional analysis criteria.

Allow Mode can be enabled even if only allow rules are enabled. In this case, it works as a complement for functional analysis allowing launching of certain applications from the denied list. For example, if launching applications from network and shared resources is prohibited in functional analysis criteria, but, at the same time, running specific application is allowed in allow rules, than this application will be launched while other applications are still blocked.

Allow rules and trusted applications can be configured under the **Allow mode** tab in profile properties.

To use allow mode

1. Set the **Use allow mode** flag on the **Allow mode** tab.
2. Specify the settings in at least one of its sections:
   - Allow rules.
   - Trusted applications.
3. Click **Save**.

If neither allow rules nor trusted applications are specified, allow mode will be disabled.

Allow Rules

Allow rules are configured in the **Allow mode** → **Allow rules** section of the profile properties.

To create a new allow rule

1. In the **Allow rules** section, click ➕ **Create rule** on the toolbar.
2. In **Adding rule** windows, specify **Rule name** and click **Save**.
3. In the rule list, select created rule and specify its settings on the opened properties pane:
   a) Set the **Enable rule** flag to start using this rule.
   b) If you want to check the rule operation, set the **Switch rule to test mode** flag. Applications will not be controlled at stations, but the activity log will be written as for enabled settings. Application launch and block results based on a rule in test mode will be displayed in the Application Control Events section.
   If the **Switch rule to test mode** flag is cleared, the rule operates in active mode and launches applications at stations by specified rule settings (see also modes of profiles operation).

c) In the **Allow the launch of applications on the following criteria** section, select options according to which the applications launch at stations will be allowed. In the **File name** field, specify a file or a directory.
Environment variables and wildcards are allowed. You can do the following:

- Specify file or folder.
  - To add an existing folder or file, enter the full path to the file or folder in the input field.
  - To add a file with a particular name, enter the name and the extension in the input field. If the value of the parameter is not a path, it is treated as a file with the specified name in any directory.
    - `C:\folder\file.exe`—adds the `file.exe` file stored in `C:\folder`.
    - `C:\folder`—adds all files located in `C:\folder` and its subfolders.
    - `file.exe`—adds all files with the name `file` and the `.exe` extension located in all folders.
    - `file`—adds all files with the name `file` located in all folders without regard for the extension.
- Use a mask which denotes the common part of object names, at that:
  - The asterisk (*) character replaces any, possibly empty, sequence of characters.
  - The question mark (?) replaces any character (one).
    - `C:\Program Files\folder\*.exe` —adds applications with the `.exe` extension in the `C:\Program Files\folder` folder, including those in its subfolders.
    - `C:\Program Files\*\*.exe` —adds applications with the `.exe` extension in subfolders of any nesting level of the `C:\Program Files` folder.
    - `example.exe`—adds all applications with the name `example` and the `.exe` extension located in all folders.
    - `example*`—adds all types of applications with the name starting with `example` located in all folders.
    - `example.*`—adds all applications with the name `example` in all folders without regard for the extension.
- You can add an application by the name of a variable if the name and a value of this variable are specified in the environment variable settings.

  `%EXAMPLE_PATH%\example.exe` – adds an application by the name of a system variable. A name of a system variable and its value can be specified in the operating system settings (for Windows OS: **Control Panel** → **System** → **Advanced system settings** → **Advanced** → **Environment variables** → **System variables**).

  A name of a variable in an example: `EXAMPLE_PATH`.

  A value of a variable in an example: `C:\Program Files\folder`.

Also you can create allow rules from the Application Control Events and Application Catalog sections basing on the data received from stations. At this, application parameters in the

rule settings will be filled automatically according to the selected application.

4. Click **Save**.

To create a duplicate of allow rule

1. In the **Allow rules** section, in the rules table, select the rule you want to duplicate for this profile.
2. Click **Duplicate rule** on the toolbar.
3. The new rule will appear in the rules table; its settings will be completely copied from the rule selected at step 1. The number **1** is added to the rule name.

To delete a deny rule

1. In the **Allow rules** section, in the rules table, select the rule you want to remove from this profile.
2. Click **Delete rule** on the toolbar.

Trusted Applications

To use trusted applications, perform one of the following actions:

- If trusted applications will be collected at your Dr.Web Server (see also Trusted Applications Repository), enable collecting of trusted applications in the **Administration** → **Application Control** → **Trusted applications** section of the Control Center.
- If trusted applications will be received on your Dr.Web Server via interserver connection from the neighbor Dr.Web Server, specify corresponding settings in the repositories of Dr.Web Servers sending and receiving the **Trusted applications** product.

Trusted applications of a certain profile are configured in the **Allow mode** → **Trusted applications** section of the profile preferences.

The section table contains the list of all trusted applications groups assigned to this profile.

Trusted applications group (or applications white list) is a list of applications collected by the specified conditions from the selected station or station group. This applications will be allowed to run on stations of the anti-virus network for which this profile is assigned when operating in the allow mode.

If your Dr.Web Server receives trusted applications via interserver connection from the neighbor Dr.Web Server (see Trusted Applications Repository), the table of groups may contain records with the icon **Trusted applications group is missing in Dr.Web Server repository**. These records are made for application groups that were added from the previous revision of the **Trusted application** product; after that a new revision was

received, in which this group is not included. While the applications on corresponding stations may still remain functional, in order to prevent disruption of profile operation, it is recommended that such groups are removed from the profile settings.

To add trusted applications group to a profile

1. In the **Trusted applications** section, click **Add trusted applications group to the profile** on the toolbar.
2. The opened window contains all available groups of trusted applications.

   When configuring allow mode, trusted applications groups are selected from the list of groups available in the repository for the **Trusted applications** product.

3. Set the flags next to the groups you want to add to the profile.
4. Click **Save**.

To remove trusted applications group from a profile

1. In the **Trusted applications** section table, set the flags for the groups you want to remove from the profile.
2. Click **Remove trusted applications group from the profile** on the toolbar.
3. Applications of this group will be removed from the list of allowed to run at stations for which this profile is assigned.

   When removing from a profile, the trusted applications group itself is not deleted. The group is still available in repository and can be added both to this profile and to other profiles.

7.4.2.3. Deny Mode

Deny mode means that on all monitored stations, only applications that comply with the deny rules are prohibited to run. All other applications are allowed.

Deny rules can be configured under the **Deny mode** tab in profile properties.

To use deny mode

1. Set the **Use deny mode** flag on the **Deny mode**tab.
2. Create deny rules as given below.
3. Click **Save**.

If no deny rules are specified, the deny mode will be disabled.

To create a new deny rule

1. In the **Deny rules** section, click **Create rule** on the toolbar.
2. In **Adding rule** windows, specify **Rule name** and click **Save**.
3. In the rule list, select created rule and specify its settings on the opened properties pane:
   a) Set the **Enable rule** flag to start using this rule.
   b) If you want to check the rule operation, set the **Switch rule to test mode** flag. Applications will not be controlled at stations, but the activity log will be written as for enabled settings. Application launch and block results based on a rule in test mode will be displayed in the Application Control Events section.
   If the **Switch rule to test mode** flag is cleared, the rule operates in active mode and blocks applications at stations by specified rule settings (see also modes of profiles operation).
   c) In the **Prohibit the launch of applications on the following criteria** section, select options according to which the applications launch at stations will be prohibited.

In the **File name** field, specify a file or a directory. Environment variables and wildcards are allowed. If the value of the parameter is not a path, it is treated as a file with the specified name in any directory. Detailed description is given in the Allow Mode section.

Also you can create deny rules from the Application Control Events and Application Catalog sections basing on the data received from stations. At this, application parameters in the rule settings will be filled automatically according to the selected application.

4. Click **Save**.

To create a duplicate of deny rule

1. In the **Deny rules** section, in the rules table, select the rule you want to duplicate for this profile.
2. Click **Duplicate rule** on the toolbar.
3. The new rule will appear in the rules table; its settings will be completely copied from the rule selected at step 1. The number **1** is added to the rule name.

To delete a deny rule

1. In the **Deny rules** section, in the rules table, select the rule you want to remove from this profile.
2. Click **Delete rule** on the toolbar.

Chapter 8: Administration of Workstations

Anti-virus networks operated by Dr.Web Enterprise Security Suite provide for centralized configuring of anti-virus packages on workstations and allows:

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

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

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

8.1. Management of Workstation Accounts

8.1.1. New Stations Approval Policy

Procedure of stations adding via the Control Center is described in the **Installation Manual**, Creation of a New Station Account.

Possibility of managing authorization of stations at Dr.Web Server depends on the following parameters:

1. If during Dr.Web Agent installation, the **Manual authorization on server** flag is cleared, mode of stations access to Dr.Web Server is defined according to settings specified at Dr.Web Server (used by default), see below.
2. If during the Dr.Web Agent installation, the **Manual authorization on server** flag is set and **Identifier** and **Password** parameters are specified, when connecting to Dr.Web Server, station will be authorized automatically regardless of the Dr.Web Server settings (is used by default when installing Dr.Web Agent via the `drweb_es_<OS>_<station>.exe` installation package—see **Installation Manual**, Installation Files).

Setting the type of the Dr.Web Agent authorization during its installation is described in the **User Manual**.

To change the access mode of stations to Dr.Web Server

1. Open the Dr.Web Server configuration: select the **Administration** item in the main menu, then click **Dr.Web Server configuration** in the control menu.

2. On the **General** tab, in the **Newbies registration** drop-down list select the necessary option:
   - **Approve access manually** (the mode is specified by default unless changed at the Dr.Web Servers installation).
   - **Always deny access**.
   - **Allow access automatically**.

Manual Access Approving

In the **Approve access manually** mode, new stations are placed to the **Newbies** subgroup of the **Status** group until administrator submits them.

To change the access mode of unapproved stations

1. Select the **Anti-virus Network** item in the main menu of Dr.Web Security Control Center. In the anti-virus network tree, select stations in the **Status** → **Newbies** group.

   The **Status** → **Newbies** group is available in the anti-virus tree only if the following conditions are met:

   1. In the **Administration** → **Dr.Web Server configuration** → **General** section, the **Newbies registration** option is set to the **Approve access manually** value.
   2. The **Approve newbies** permission is allowed for the administrator.

2. To specify an access to Dr.Web Server, in the **Unapproved stations** section of the toolbar, set the action to apply for selected stations:

   Approve selected stations and set a primary group—approve access for selected stations and set the primary group from the offered list.

   Cancel action specified to execute on connection—cancel an action under unapproved station which was specified for executing when station will connect to Dr.Web Server.

   Reject selected stations—deny access to Dr.Web Server for selected stations.

Access Denying

In the **Always deny access** mode, Dr.Web Server denies access for requests from new stations. The administrator should manually create an account for new stations and set access password for them.

Automatic Access Approving

In the **Allow access automatically** mode, all stations that request an access to Dr.Web Server will be approved automatically without requesting the administrator. The group which is set in the **Primary group** drop down list of the **Dr.Web Server configuration** section, on **General** tab, is set as a primary.

8.1.2. Removing and Restoring Stations

Removing Stations

To remove a workstation account

1. Select the **Anti-virus network** item in the main menu.
2. In the hierarchical list of the opened window, click the name of one or several stations you want to delete.
3. On the toolbar, click **General** → **Remove selected objects**.
4. You will be prompt to remove the station. Click **OK**.

After a station is removed from the hierarchical list, it is added to the deleted stations table. You can restore the removed station via Dr.Web Security Control Center.

Restoring Stations

To restore a workstation account

1. Select the **Anti-virus network** item in the main menu, in the opened window in the hierarchical list select deleted station or several stations you want to restore.

   All deleted stations are located in the **Deleted** subgroup of the **Status** group.

2. On the toolbar, select **General** → **Restore deleted stations**.
3. The section for station restoring will be opened. You can specify the following station parameters, which will be set during restoring:
   - **Primary group**—select the primary group, in which the station will be added. By default the primary group which was set before station deletion is selected.

     If you restore several stations simultaneously, the **Former primary group** is selected by default. It means that for each selected station its own primary group, in which station was resides before deletion, will be specified. If the definite group is selected, for all restoring stations the same specified group will be set.

   - In the **Membership** section, you can change the list of groups in which the station will be included. By default, the list of groups in which the station has been included before deletion is set. To include the station in a user groups, set the flags for this groups.
4. To restore the station with specified parameters, click **Restore.**

8.1.3. Merging Stations

As a result of some database operations or reinstallation of the anti-virus software on workstations, several station accounts with the same name may appear on the anti-virus network list, yet only one of them will actually correspond to the respective workstation. The configuration previously set for the station and its statistics may also remain with the out-of-date station accounts. To remove duplicate station accounts and restore the configuration and statistics of the station, use the station merge operation.

To remove out-of-date accounts of a station and restore its configuration and statistics

1. Using the CTRL key, select all the accounts associated with the same station.
2. In the toolbar, select **General** → **Merge stations**.
3. In the column, select the main station (the station account that will remain on the anti-virus network list). The other station accounts will be deleted, and their statistics will be ascribed to the selected station.
4. In the column, select the station whose settings will be used for the selected main station. The settings of the **Configuration** section in the station properties, the primary group, and the Application Control profile settings are taken from the selected station.
5. Click **Save**.

To prevent a new station account from being automatically created when reinstalling software, use the personal installation package available for download in the **Properties** section of the station.

8.2. General Workstation Settings

8.2.1. Station Properties

To view and edit the properties of a workstation

1. Select the **Anti-virus network** item in the main menu of the Control Center, then select the station in the hierarchical list of the opened window.
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. Station properties pane contains the following groups of settings: **General**, **Configuration**, **Groups**, **Security**, **Location**. These settings are described below.

4. To save changes in the settings, click **Save**.

To remove personal settings of a workstation

1. Select the **Anti-virus network** item in the main menu of the Control Center, then select a station in the hierarchical list of the opened window and click **General** → **Remove personal settings** on the toolbar. A list of settings for this station will be opened. Personal settings will be marked with flags.
2. For the personal settings you want to remove, leave the flags set. For the settings you want to leave personal, clear the flags. Click **Delete**. For the settings marked by the flags, the inheritance from the primary group will be restored.

8.2.1.1. General

The **General** section contains the following read-only fields:

- **Station identifier**—unique identifier of the station. It is set when the station account is created and cannot be changed later on.
- **Name**—station name. It is specified when the station account is created and is automatically replaced with the computer name after the Dr.Web Agent connects.
- **Created on**—date when the station account was created on Dr.Web Server.
- **Security identifier**—SID (security identifier) of the Windows OS user account. The field is filled in automatically after a station under Windows OS connects to Dr.Web Server.
- **LDAP DN**—distinguished name of a station under Windows OS. Relevant for stations included in a ADS/LDAP domain. The field is filled in automatically after the station connects to Dr.Web Server.
- **MAC address**—MAC address of the station. The field is filled in automatically after the station connects to Dr.Web Server.
- **First Dr.Web Agent download**—date when the Dr.Web Agent installation package was first downloaded using the link from the **Installation package** item (see below).
- **Last connected on**—date of last connection of this station to Dr.Web Server.
- **Network address**—network address of the station.
- **Operating system build**—build number of the Windows OS build installed on the station.

You can also set or change the values of the following fields:

- In the **Password** field, specify a password to authorise the station on Dr.Web Server (enter the same password in the **Confirm Password** field). If you change the password, repeat this action in the Dr.Web Agent connection settings on the station to permit Dr.Web Agent connection to Dr.Web Server.
- In the **Start of lockout period** and **End of lockout period** fields, set the period (date of the first and last day) during which the workstation will be blocked on Dr.Web Server. These parameters allow you to temporarily block access to Dr.Web Server for a station. If you

specify only the **Start of lockout period** value, the station will be blocked permanently starting from the specified date.

- In the **Description** field, you can add any additional information about the station.

> Values of fields marked with the * character must be specified.

The following links are also available in this section:

- In the **Installation package** item—link for downloading the Dr.Web Agent installation package for this station.

  After a new station is created, before its operating system is set, the item contains links for downloading installation files for all operating systems supported by Dr.Web Enterprise Security Suite.
- In the **Configuration file** item—link for downloading the file with Dr.Web Server connection settings for stations under Android, macOS, and Linux.

8.2.1.2. Configuration

In the **Configuration** section, you can change station configuration that includes the following:

Icon	Settings	Description section
	Permissions for the workstation users	Permissions of Station Users
	Centralized schedule to run tasks on workstation	Scheduled Tasks of a Station
	License keys file for workstation	License Keys
	Restrictions on propagation of anti-virus software updates	Update Restrictions for Workstations
	List of installable components	Installable Components of the Anti-Virus Package
	Settings of anti-virus components for the station.	Management of Anti-virus Components

Dr.Web Security Control Center also provides you with option for deleting personal settings of a workstation. These settings are located on the right of the corresponding options for components configuration options. When you delete personal settings of a workstation, it inherits settings from the primary group.

> When you change settings of SpIDer Gate and/or Office Control, please consider that settings of these components are interconnected, so if personal settings of one of them are

removed via  **Remove personal settings**, it also removes settings of second component (settings inheritance from the parent group is set).

8.2.1.3. Groups

In the **Groups** section, you can set the list of groups into which the workstation is included. The **Membership** list displays the groups which include the workstation and to which you can include it.

To manage the membership of a workstation

1. To add a station to the user group, set the flag for this group in the **Membership** list.
2. To remove a workstation from the group, clear the flag for this group in the **Membership** list.

   You cannot remove stations from pre-installed groups.

3. If you want to reassign the other primary group, click the icon of necessary group in the Membership list. The **1** sign displays on the icon.

8.2.1.4. Security

In the **Security** section, restrictions for network addresses from which Dr.Web Agents installed on the station will be able to access Dr.Web Server are set.

To configure access restrictions

1. Set the **Use this ACL** flag to specify lists of allowed or denied addresses. If the flag is cleared, all connections are allowed.
2. To allow the access from a specific TCP address, include it into the **TCP: Allowed** or **TCPv6: Allowed** list.
3. To deny specific TCP address, include it into the **TCP: Denied** or **TCPv6: Denied** list.
4. The addresses not included into any of the lists are allowed or denied depending on whether the **Denial priority** flag is set. If the flag is set, the **Denied** list has a higher priority than the **Allowed** list. Addresses not included in any of the lists or included into both of them are denied. Allowed only addresses that are included in the **Allowed** list and not included in the **Denied** list.

To edit the address list

1. Specify network address in the corresponding field in the following format: <*IP address*>/[<*network prefix*>].
2. To add a new field, click the  button in the corresponding section.
3. To delete a field, click  next to the deleting address.
4. Click **Save** to apply settings.

Lists for TCPv6 addresses will be available, if the IPv6 interface is installed on the computer.

Examples of prefix usage:

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

   Containing 254 addresses.

   Host addresses look like: `195.136.12.*`
2. Prefix 8 stands for a network with a network mask: `255.0.0.0`

   Containing up to 16777214 addresses (256*256*256-2).

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

8.2.1.5. Dr.Web Proxy Server

In the **Dr.Web Proxy Server** section, you can configure the settings of Dr.Web Proxy Server installed on this station.

Detailed information on how to install Dr.Web Proxy Server and connect it to Dr.Web Server is given in the **Installation Manual**, Installing Dr.Web Proxy Server.

If Dr.Web Proxy Server is installed on the station:

1. The **Identifier** and **Name** fields contain the identifier and the name of the Dr.Web Proxy Server account created in the Control Center. Both the Identifier and the Name cannot be changed after the account is created.
2. In the **Password** and **Confirm Password** fields, you can change the password of the Dr.Web Proxy Server account created in the Control Center. The password is used to connect Dr.Web Proxy Server to Dr.Web Server. If the password has been changed in the Control Center, please make sure that the password in the connection settings at Dr.Web Proxy Server matches with the changed password in the Control Center. If the passwords are different, Dr.Web Proxy Server will not be able to connect to Dr.Web Server for remote configuring via the Control Center.

The Dr.Web Proxy Server password is stored in the `drwcsd-proxy.auth` file which is located as follows:

- Windows: `%ProgramData%\Doctor Web\drwcs\etc`
- Linux: `/var/opt/drwcs/etc`
- FreeBSD: `/var/drwcs/etc`

After changing the password of the Dr.Web Proxy Server account, you must restart the service.

3. The **Membership** section defines the group in which Dr.Web Proxy Server is included. To change the group, set the flag next to the necessary group in the given list.

   Dr.Web Proxy Server can be included in one group only.

   You can select the pre-installed **Proxies** group and its subgroups only.

4. You can uninstall Dr.Web Proxy Server connected with Dr.Web Agent on the edited station. To do this, click **Delete Dr.Web Proxy Server**.

   After you click **Save**, Dr.Web Proxy Server will be uninstalled from the station. The Dr.Web Proxy Server account will be deleted from Dr.Web Server.

If Dr.Web Proxy Server is not installed on the station:

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

Remote installation of Dr.Web Proxy Server is possible only if the selected station is running Windows.

2. After you click **Save**, the Dr.Web Proxy Server account will be created in the Control Center. After the settings are transmitted to the station, Dr.Web Proxy Server will be installed on this station in the background mode. Dr.Web Agent on the selected station will be connected to Dr.Web Server through the installed Dr.Web Proxy Server only. The use of Dr.Web Proxy Server will be transparent to the user.

8.2.1.6. Location

In the **Location** section, you can specify additional information about the physical location of the workstation.

Also on this tab you can view the station location on a geographical map.

To view the station location on a map

1. In the **Latitude** and **Longitude** fields, specify the station geographical coordinates in the Decimal Degrees format.

2. Click **Save** to save the changes.
3. On the **Location** tab, the **Show on map** link will become available. The link opens an OpenStreetMap with a mark at the specified coordinates.

> For stations under Android OS, you can configure automatic location detection.
>
> Detailed information on usage and configuring this feature you can find in the **Appendices** document, in the Automatic Location of Stations under Android OS section.

8.2.2. Protection Components

Components

To view the list of anti-virus package components installed on a workstation and start or stop components operation

1. Select the **Anti-virus network** item in the Control Center main menu, then click the name of a station or a group in the hierarchical list of the opened window.
2. In the opened control menu in the **General** section, select the **Protection components** item.
3. This opens a window with information on components installed on protected stations.

> Compound of installed components list depends on:
>
> - Components enabled in the license key file.
> - Workstation OS.
> - Settings specified by administrator of anti-virus network at Dr.Web Server. Administrator is able to change the list of anti-virus package components either before Dr.Web Agent (see Installable Components of the Anti-Virus Package) installation or at any time after its installation.

4. If necessary, you can change the state of components operation directly from the Control Center. For this, set the flags for those components operation status of which you want to change and click corresponding button on the toolbar:
   - —stop the selected component operation on stations.
   - —start the selected components on stations.

> When interrupting the components operation, running scans will be terminated, Scanner stopped and running monitors paused.
>
> ---
>
> Also you can stop the components operation depending on their launch type as it is described in Interrupting Running Components.

5. If necessary, you can export data on components operation state into a file. For this, click the one of the following buttons on the toolbar:

    **Save data in CSV file**,

    **Save data in HTML file**,

    **Save data in XML file**,

    **Save data in PDF file**.

Virus Databases

To view the list of virus databases installed on a workstation

1. Select the **Anti-virus network** item in Dr.Web Security Control Center main menu, then click the name of a workstation in the hierarchical list of the opened window.
2. In the opened control menu in the **Statistics** section, select the **Virus databases** item.
3. This opens a window with information on installed virus databases: the name of the file containing a particular database; virus database version; the database creation date; the total number of threat records in the database.

If the **Virus databases** item is hidden, to view the item, select **Administration** in the main menu, and then select **Dr.Web Server configuration** in the control menu of the window. On the **Statistics** tab, set **Station statuses** and **Virus database statuses** flags, then restart Dr.Web Server.

The **Virus databases** item is available only if a single station is selected.

8.2.3. Hardware and Software on Stations under Windows OS

Dr.Web Enterprise Security Suite allows to accumulate and view information on hardware and software installed on protected stations under Windows OS.

To collect information on hardware and software of the stations

1. Enable statistics collecting on Dr.Web Server:
   a) Select the **Administration** item in the main menu of the Control Center.
   b) Select the **Dr.Web Server configuration** item in the control menu.
   c) In the Dr.Web Server settings, open the **Statistics** tab and set the **Hardware and software** flag if it is cleared.
   d) To apply the changes, click **Save** and restart Dr.Web Server.
2. Allow collecting statistics on stations:
   a) Select the **Anti-virus Network** item in the main menu of the Control Center.

b) In the hierarchical list of anti-virus network, select a station or a group of stations for which you want to allow statistics collecting. When selecting a group of stations, please note the settings inheriting: if the stations of selected group have personal settings, when changing the group settings will not change the station settings.

c) In the control menu, in the **Configuration** → **Windows** section, select **Dr.Web Agent**.

d) In the Dr.Web Agent settings, on the **General** tab, set the **Collect information about stations** flag if it is cleared. If you did not enable statistics collection in the Dr.Web Server configuration earlier, this setting will be unavailable. If necessary, edit the **Period of collecting information about stations (min.)** parameter value.

e) To apply the changes, click **Save**. The settings will be transmitted to the stations.

To view hardware and software on one or several stations

1. Select the **Anti-virus Network** item in the main menu of the Control Center.
2. In the hierarchical list of anti-virus network, select a station or a group of stations.
3. In the control menu, in the **General** section, select the **Hardware and software** item.
4. The table contains the following tabs with information about the hardware and software of the selected stations:
   - **Hardware**—the list of hardware mounted on the stations.
   - **Software**—the list of program applications installed on the stations.
   - **Windows updates**—the list of Windows OS updates packages installed on the stations.
5. The **Station** column on each tab, contains the name of a station for which the information id given.
6. To edit the data view in the table
   - Using the icon, select the columns to display in the table.
   - Using the icon, specify the arbitrary string to search by all sections of the table.
7. If necessary, you can export data on hardware and software on station into a file. For this, click the one of the following buttons on the toolbar:

   Save data in CSV file,

   Save data in HTML file,

   Save data in XML file,

   Save data in PDF file.

8.3. Management of Workstation Configuration

8.3.1. Permissions of Station Users

To edit users permissions via Dr.Web Security Control Center for administrating the anti-virus package

1. In the main menu, select **Anti-virus network**, then click the name of a workstation in the hierarchical list of the opened window. In the opened control menu, select **Permissions**. Permissions configuration window opens.
2. You can edit permissions on tabs that correspond to the workstation operating system. To change (allow or deny) any of permissions, set or clear the flag for this permission.
3. To edit permissions for stations under Windows, macOS, Android and Linux operating systems, use the following tabs:
   - **Components**—change permissions for components management. By default, a user is authorized to launch each component, but prohibited to edit components configuration or stop the operation of components.
   - **General**—change permissions for Dr.Web Agent and its functions management:

Permissions section flag	Flag actions	Result on the station if the flag is cleared
Stations under Windows OS		
Change Dr.Web Agent configuration	Set the flag to allow users on the station to change Dr.Web Agent settings.	In the Dr.Web Agent settings, in the **Main** section, the settings of the following options are not available: • **Notifications**: all settings are not available. • **Server**: the Dr.Web Server connection settings, the **Synchronize system time with the server time** flag and the **Use Mobile mode when there is no connection with the server** option are not available. • **Self-Protection**: the **Block changing of system date and time**, **Block user activity emulation** options are not available. • **Advanced**: in the **Log** section settings, the **Dr.Web Update**, **Dr.Web Services**, **Create memory dumps at scan errors** options are not available.
Disable self-protection	Set the flag to allow users on the station to disable self-	In the Dr.Web Agent settings, in the **Main** → **Self-Protection** the **Enable self-protection**

Permissions section flag	Flag actions	Result on the station if the flag is cleared
	protection.	option and the **Enable hardware virtualization** option are not available.
Uninstall Dr.Web Agent	Set the flag to allow users on the station to uninstall Dr.Web Agent.	Disables uninstalling of Dr.Web Agent on the station either via the installer or via standard Windows OS services. In this case, Dr.Web Agent can be uninstalled only via the **General** → **Uninstall Dr.Web Agent** option on the toolbar of Dr.Web Security Control Center.
Stations under macOS		
Run in mobile mode	Set the flag to allow users on the station to switch to mobile mode and use Dr.Web Global Update System for updating, if there is no connection with Dr.Web Server.	The **Updates** section in the application main window is blocked.
Stations under Linux-based OS		
Run in mobile mode	Set the flag to allow users on the station to switch to mobile mode and use Dr.Web Global Update System for updating, if there is no connection with Dr.Web Server.	For the console mode of the application: the `drweb-ctl update` command for updating the virus databases from the GUS is not available.
Stations under Android OS		
Run in mobile mode	Set the flag to allow users of mobile devices to switch to mobile mode and use Dr.Web Global Update System for updating, if there is no connection with Dr.Web Server.	The **Updates** section on the application main screen is blocked.

After disabling an option that changes Dr.Web Agent settings, the value which has been set at the last time before disabling, will be used.

Actions following the corresponding menu items are described in **User Manuals** for Dr.Web products for corresponding operating system.

4. To use the same settings for another object, click **Propagate these settings to another object**.
5. To export settings to a file, click **Export settings from this section to the file**.
6. To import settings from a file, click **Import settings to this section from the file**.
7. To save permissions changes, click **Save**.

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

8.3.2. Scheduled Tasks of a Station

Dr.Web Enterprise Security Suite provides the *centralized task schedule* which is set by the anti-virus network administrator and complies with all the rules of configuration inheritance.

Task schedule—a list of actions performed automatically at a preset time on workstations. Schedules are mostly used to scan stations for threats at a time most convenient for users, without having to launch the scanning manually. Dr.Web Agent also allows to perform certain other types of tasks as described below.

To edit centralized schedule of regular tasks execution for certain stations and groups, use Dr.Web Security Control Center.

Users at station are not allowed to view and edit scheduled tasks of centralized schedule.

By default, the schedule contains the **Daily scan** task, which performs a daily remote scan of a station.

Results of tasks execution according to the centralized schedule are not stored into statistic data of Dr.Web Agent but sent to Dr.Web Server and stored in the Dr.Web Server statistic data.

To edit centralized schedule

1. Select the **Anti-virus network** item in the main menu of the Control Center, in the hierarchical list of the opened window, select a group or workstation. In the opened control menu, select **Task Scheduler**. The list with the tasks of the station will be opened.

The majority of tools in this section are unavailable as long as the station or the group you selected keeps the inheritance of settings from a parent group. The following toolbar elements let you change the inheritance settings related to the task schedule:

Inherit settings from policy or primary group—remove personal task schedule settings and set inheritance of settings in this section from a parent group.

Copy settings from policy or primary group and set them as personal—copy task schedule settings from a parent group and assign them to selected stations. That will break the inheritance, and all further changes in the task schedule will be considered personal.

2. To manage schedule, use the corresponding elements from the toolbar:
   a) General elements on the toolbar are used to create new tasks and generally manage schedule section.

   Create task—add a new task. This action is described in details below, in the Task Editor section.

   Propagate these settings to another object—copy scheduled tasks into other objects—stations and groups. For details, see Propagation of Settings to Other Groups/Stations.

   Export settings from this section to the file—export schedule to the file of special format.

   Import settings to this section from the file—import schedule from the file of special format.

   Import of the task list for Dr.Web Server into the Task Schedule on workstations and vice versa is not allowed.

   b) To manage existing tasks, set the flags next to the necessary tasks or the common flag in the table header to select all task from the list. As long as the group or the station you selected does not keep the inheritance of task schedule settings from a parent group, the following toolbar elements will be available to manage selected tasks:

Option		Action
Start type	**Synchronous type**	Run all tasks marked below synchronously. The task with the specified periodicity will be placed in the general queue of the Scheduler tasks to be executed sequentially.
	Asynchronous type	Run all tasks marked below asynchronously. The task with the specified periodicity will be executed in parallel with other tasks, out of turn.
Status	**Enable execution**	Activate execution of selected tasks according to their schedule, if they were disabled.
	Disable execution	Disable execution of selected tasks. Tasks remain on the list but will not be executed according to the schedule.

The same option you can specify in the task editor on the **General** tab by setting the **Enable execution** flag.

Option		Action
Severity	**Make critical**	Perform extra launch of the task at next Dr.Web Agent launch, if scheduled execution of this task has been omitted.
	Make noncritical	Execute the task only at scheduled time regardless of whether a task launch has been omitted or not.
The same option you can specify in the task editor on the **General** tab by setting the **Critical task** flag.		
Duplicate settings		Duplicate tasks that are selected in the list of current schedule. When you run the **Duplicate settings** option, new tasks are created with settings similarly to the selected tasks.
Schedule repeatedly		For tasks which executed once: execute task one more time according to the specified time settings (changing execution multiplicity of the task is described below, in the Task Editor section).
Remove these settings		Remove selected task from the schedule.
Execute task		Execute the tasks selected in the list immediately. At this, a task will be launched even if it is disabled for execution on a schedule.
Edit task		Change task parameters. The **Task editor** window described below opens.

If you do not need a schedule inherited from the parent group, disable inheritance for the station, leave at least one task and disable its execution.

1. Select the **Anti-virus network** item in the main menu of the Control Center, then select the station in the hierarchical list of the opened window.
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. Select **Configuration** → **Task Scheduler** in the section with station properties.
4. Click the **Copy settings from policy or primary group and set them as personal** icon and confirm the action.
5. Leave at least one task and disable its execution by clicking on the **Status** icon → **Disable execution**.

Task Editor

In the **Task Editor** you can specify settings to:

1. Create a new task.

   For this click **Create task** on the toolbar.
2. Edit existing task.

   Click the name of one of the tasks on the task list and click **Edit task** on the toolbar.

The window for editing a task opens. Settings for editing of existing task are similar to the settings of creating a new task.

Interface fields marked with the * sign are mandatory.

To edit task settings

1. On the **General** tab in the **General** section, you can set up the following parameters:
   - In the **Name** field, specify the name of the task displayed in the schedule list.
   - Set the **Enable execution** flag, to enable the task execution. If the flag is cleared, the task remains in the list but will not be executed according to the schedule.

     The same action you can perform from the main window of the schedule via the **Status** option on the toolbar.
   - Set the **Critical task** flag to perform extra launch of the task at next Dr.Web Agent launch, if scheduled execution of this task has been omitted (Dr.Web Agent is switched off at the due time). If at launch, the task was omitted several times, it will be executed only once.

     The same action you can perform from the main window of the schedule via the **Severity** option on the toolbar.

     If several scan tasks must be implemented, only one task will be executed—the first one in the queue.

     For example, if **Daily scan** is enabled and a critical remote scan via Dr.Web Agent Scanner is skipped, only **Daily scan** will be executed and the skipped critical task will not be run.
   - If the **Run the task asynchronously** flag is cleared, the task will be placed to the general queue of Scheduler tasks that are executed sequentially. Set the flag to execute this task in parallel out of order.
2. In the **Time** section, specify the task launch parameters:

- In the **Periodicity** drop-down list, set the launch mode of the task and setup the time according to the specified periodicity:

Launch type	Description
Startup	The task will be launched at the Dr.Web Server start up. No additional parameters required to run the task.
N minutes after initial task	In the **Initial task** drop-down list, select the task relatively to which the time of current task execution is set. In the **Minute** field, specify or select from the offered list the number of minutes that should pass after the execution of initial task to start execution of edited task.
Daily	Specify the hour and the minute for the task to be launched at the time specified.
Monthly	Specify the day of the month, the hour and the minute for the task to be launched at the time specified.
Weekly	Select a day of the week, specify the hour and the minute, for the task to be launched at the time specified.
Hourly	Specify a number from 0 to 59 to set the minute of every hour the task will be run.
Every N minutes	The **N** value should be specified to set the time interval for the execution of the task. At **N** equal `60` or more, the task will be run every **N** minutes. At **N** less than `60`, the task will be run every minute of the hour multiple of **N**.

- Set the **Disable after the first execution** flag to execute the task only once at specified time. If the flag is cleared, the task will be executed multiple times according to the specified periodicity.
  To repeat the launch of task already ones executed, use the **Schedule repeatedly** on the toolbar of the schedule section.
- Set the **Run the task by UTC** flag to launch the task relatively the universal time (UTC+0 time zone). If the flag is cleared, the task will be launched by the local time on station.
- Set the **Run task with random delay** flag for the task to be launched with a random delay after the specified start time of the task. In the **Random delay interval** field, specify the maximum task launch delay time. The option may be of use if you want to distribute the resource load in a large anti-virus network or in a network whose virtual stations are located within one hypervisor.

3. On the **Action** tab, in the **Action** drop-down list, select the type of the task and specify task parameters which are needed to perform the task:

Task type	Parameters and description
Write to log file	**String**—the text of the message to be added to the log file.
Run program	Specify the following settings: • The **Path** field—full name (with the path) of the executable file to be launched. • The **Arguments** field—line parameters for the program to be run. • Set the **Wait for the completion of the program** flag to wait for the completion of the program which has been launched by this task. At this, the Dr.Web Agent logging the start of the program, the returned code and the time of the program end. If the **Wait for the completion of the program** flag is cleared, the task become completed right after the launch of the program and the Dr.Web Agent logging only the start of the program.
Dr.Web Agent Scanner. Full scan	Remote anti-virus scanning of stations. Parameters that can be specified for a scan are described in Configuring Remote Scan Parameters.
Dr.Web Agent Scanner. Custom scan	
Dr.Web Agent Scanner. Express scan	

Remote scanning performed by Dr.Web Agent Scanner is available only on stations running Windows OS, macOS, and Unix-like OSs.

4. When all parameters for the task are specified, click **Save** to accept changes of edited parameters, if you editing existing task, or to create a new task with specified parameters if you created a new task.

8.3.3. Installable Components of the Anti-Virus Package

It is not recommended to install SpIDer Gate, SpIDer Mail and Dr.Web Firewall components on servers that implement significant network functions (domain controllers, license distribution servers and etc.) to avoid probable conflicts between network services and internal components of Dr.Web anti-virus.

To change the list of anti-virus package components to be installed

1. Select the **Anti-virus network** item in the main menu, then select a station or a group and select the **Installable Components** item in the opened control menu.
2. Select an option for necessary components in the drop-down list:
   - **Must be installed**—means that a component must be present on the workstation. When a new workstation is created, the component is installed with the anti-virus package. If the

Must be installed option is specified for an existing workstation, the component will be added to the available anti-virus package.

- **May be installed**—means that the component can potentially be installed. The user decides whether the component is required.
- **Cannot be installed**—means that installing the component is not allowed. When a new workstation is created, the component will not be installed with the anti-virus package. If the **Cannot be installed** option is specified for an existing workstation, the component will be removed from the anti-virus package.

Table 8-1 shows whether the component will be installed on the workstation (+) according to the parameters specified by the user and the settings defined by the Dr.Web Server administrator.

Table 8-1.

User parameters	Specified on Dr.Web Server		
	Must	May	Cannot
Install	+	+	
Do not install	+		

3. Click **Save** to save the settings and the set of anti-virus package components on the workstation.

8.3.4. Connection Parameters

On the **Connection Parameters** tab, you can specify parameters determining interaction with Dr.Web Server:

- In the **Certificate** field specify the SSL certificate of Dr.Web Server (`drwcsd-certificate.pem`) which is stored on the station. To select the certificate file, click  .

  Several certificates can be stored on a station at the same time, e.g., during moving from one Dr.Web Server to another. Note that certificates must be unique, i.e. you cannot specify two similar certificates.

  To add one more certificate, click  and select the certificate file.

  To remove existing certificate from the station, click  next to certificate to remove.

  Certificate must be obligatory specified.

- In the **Server** field, you can specify address of Dr.Web Server or Dr.Web Proxy Server (see Dr.Web Proxy Server for details). You may leave this field blank. Then Dr.Web Agent will use the address of Dr.Web Server that is set on the user's local computer (the address of Dr.Web Server from which the installation has been performed).

Either one Dr.Web Server address or several different Dr.Web Servers addresses can be set. To add one more Dr.Web Server address, click  and specify an address in the added field. Format of the Dr.Web Server network addresses is described in the **Appendices** document, in Appendix D. The Specification of Network Addresses.

Dr.Web Server address example:

tcp/10.4.0.18:2193

tcp/10.4.0.19

10.4.0.20

If the **Server** parameter value is set incorrectly/invalid, Dr.Web Agents will disconnect from Dr.Web Server and will not be able to reconnect. In this case you will have to set the Dr.Web Server address on the stations directly.

- In the **Search retries number** field, set the parameter determining the number of attempts to find Dr.Web Server via the connection using the Multicasting mode.
- In the **Search time-out (sec.)** field, set the interval between attempts to find Dr.Web Server in seconds via the connection using the Multicasting mode.
- The **Compression mode** and **Encryption mode** fields determine the compression and encryption settings of network traffic correspondingly (also see p. Traffic Encryption and Compression).
- In the **Network listening parameters** field, specify the UDP port for Dr.Web Security Control Center to search for working Dr.Web Agents in a network. To disable ports listening, enter **NONE**.

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

  By default, the **udp/:2193** is used, which means "all interfaces, port `2193`".

8.3.5. License Keys

You can view and edit the list of license keys of a station or a group by the following ways:

1. Via the License Manager.
2. Via configuration of a licensing object (a station or a group) in the anti-virus network.

To edit the list of license keys via the configuration of licensing object

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. Open the Station Properties or Editing Groups section for the object, license keys of which you want to edit.
3. In the configuration section, click the  **Edit** icon or the **License keys** link.
4. The **License keys** opened window contains the list of object license keys, their current state (inherited or personally specified), and also the list of all keys that are available on this Dr.Web Server. Also, if necessary, you can open the License Manager directly.

5. Actions on the keys list depend on the state of the current license keys of an object:

Action	Current keys are inherited	Current keys are personally specified	No key specified
Add license key	Inheritance will be broken. A new key is added to the list of assigned keys and the key list become personal.	A new key will be added to the list of assigned keys.	Keys will be added to the list of license keys of an object as personal.
Remove license key	Action is not available.	A key will be removed from the list of object keys.	Action is not available.
Set inheritance	Action is not available.	Current keys will be removed from the list of object keys, the inheritance of keys will be set from a primary/parent group.	Action is not available.
Broke inheritance	Inheritance will be broken. The list of keys remains the same but becomes personal.	Action is not available.	Action is not available.

Current keys are inherited

To add a license key

1. In the **License keys** window, in the **All keys** list, select one or several license keys that you want to add.
2. Click  .
3. If the lists of installed components on stations and in the added keys are different, you will be warned and will be asked to edit the result components list.
4. After you specify all necessary changes, click **Save**.
5. Inheritance will be broken. A new key is added to the list of assigned keys and the key list become personal.

To break the inheritance without changing the list of license keys

1. In the **License keys** window, click **Copy settings from the primary group and set them as personal**.
2. Inheritance will be broken. The list of keys will be copied from a primary/parent group and specified for the object as personal.
3. Click **Save**.

Current keys are personally specified

To add a license key

1. In the **License keys** window, in the **All keys** list, select one or several license keys that you want to add.
2. Click  .
3. If the lists of installed components on stations and in the added keys are different, you will be warned and will be asked to edit the result components list.
4. After you specify all necessary changes, click **Save**.
5. A new key will be added to the list of assigned keys.

To remove a license key

1. In the **License keys** window, in the **Object keys** list, click ✖ next to those license keys that you want to remove.

   If all keys are removed, the inheritance of the license keys will be set from a primary/parent group (see also Set the inheritance).

2. Click **Save**.
3. If the lists of installed components on stations and in the remained keys are different, you will be warned and asked to edit the result components list.

To set the inheritance

1. You can set the inheritance by one of the following ways:
   - Open the Station Properties or Editing Groups section for the object, inheritance for which you want to set. In the configuration section, click **Remove key**.
   - In the **License keys** window, in the **Object keys** list, click ✖ next to all assigned license keys. Click **Save**.
2. Current keys will be removed from the list of object keys, the inheritance of keys will be set from a primary/parent group.
3. If the lists of installed components on stations and in the inherited keys are different, you will be warned and will be asked to edit the result components list.

No key specified

This may happen if none of the license keys has been added to Dr.Web Server or license keys have been added to Dr.Web Server but have not been propagated to any of the objects including the **Everyone** group.

To add a license key

1. In the **License keys** window, in the **All keys** list, select one or several license keys that you want to add.
2. Click  .
3. Click **Save**.
4. Keys will be added to the list of license keys of an object as personal.

8.4. Management of Anti-virus Components

Detailed description of anti-virus components settings which are configured via the Control Center, is given in the **Administrator Manual** on managing stations for corresponding operating system.

Components

Depending on the operating system of the station, the following anti-virus components are provided:

Stations under Windows OS

Dr.Web Scanner

Scans the computer at the user's request.

Dr.Web Agent Scanner

Performs remote anti-virus scanning of stations, including scanning for rootkits, from the Control Center at the administrator's request or according to the task schedule.

SpIDer Guard

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

SpIDer Mail

Checks all incoming and outgoing mail messages when using the mail clients.

The spam filter is also available (if the license permits this function).

SpIDer Gate

Checks all calls to websites via the HTTP protocol. Neutralizes malicious software in HTTP traffic (for example, in uploaded and downloaded files) and blocks the access to suspicious or incorrect resources.

Office Control

Controls access to network and local resources, in particular, limits access to websites. Controls the integrity of important files by preventing accidental modification or infection and allows you to limit access to unwanted information for employees.

Firewall

Protects computers from external unauthorized access and prevents leak of vital data via internet. Monitors connection attempts and data transfer via the internet and blocks suspicious connections both on network and application levels.

Quarantine

Isolates malware and suspicious objects in the specific folder.

Self-protection

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

Preventive protection

Includes Behavior Analysis, Exploit Prevention and Ransomware Protection.

Prevents of potential security threats. Controls the access to the operating system critical objects, controls drivers loading, programs autorun and system services operation and also monitors running processes and blocks them if malicious activity is detected.

Application control

Monitors activity of all processes on stations. Allows the anti-virus network administrator to adjust which applications to allow and which ones to prohibit for launching on protected stations.

Stations under Unix-like OS

Dr.Web Scanning Engine

Scanning engine. Provides the anti-virus scanning service (contents of files and 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.

Dr.Web File Checker

The component which scans file system objects and manages quarantined files. It receives scanning tasks from other Dr.Web for UNIX components. Checks file system directories according to a received task, transmits 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

cache that stores information on scanned files to lessen the frequency of repeated file scanning.

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

Dr.Web ICAPD

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

SpIDer Guard for Linux (only within distribution kits for GNU/Linux-based OS)

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

SpIDer Guard for SMB

Monitor of Samba shared file system directories. It operates as a resident mode and monitors file operations (creation, opening, closing, and read or write operations) in directories used by SMB file server Samba. It sends to the files check component contents of new and modified files for the check.

SpIDer Guard for NSS (only within distribution kits for GNU/Linux-based OS)

NSS volumes monitor (Novell Storage Services). It operates as a resident mode and monitors file operations (creation, opening, closing and write operations) on NSS volumes mounted in the specified file system point. It sends to the files check component contents of new and modified files for the check.

SpIDer Gate (only within distribution kits for GNU/Linux-based OS)

The component for monitoring network traffic and URLs. It is designed to check data downloaded from the network to the local host and transmitted from it to the external network for threats. The components also prevents connections with the network hosts, included not only to the unwanted categories of web resources, but also to black lists created by the system administrator.

Dr.Web MailD

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

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

Other components for stations under Unix-like OS, are additional and serve for internal configuration of anti-virus software operation.

Stations under macOS

Dr.Web Scanner

Scans the computer at the user's request.

Dr.Web Agent Scanner

Performs remote anti-virus scanning of stations, including scanning for rootkits, from the Control Center at the administrator's request or according to the task schedule.

SpIDer Guard

The constant file system protection in the real-time mode. Checks all launched processes and also created files on hard drives and opened files on removable media.

SpIDer Gate

Checks all calls to websites via the HTTP protocol. Neutralizes malicious software in HTTP traffic (for example, in uploaded and downloaded files) and blocks the access to suspicious or incorrect resources.

Quarantine

Isolates malware and suspicious objects in the specific folder.

Mobile devices under Android OS

Dr.Web Scanner

Scans the computer at the user's request.

Dr.Web Agent Scanner

Performs remote anti-virus scanning of stations, including scanning for rootkits, from the Control Center at the administrator's request or according to the task schedule.

SpIDer Guard

The constant file system protection in the real-time mode. The check of all files as they are saved in the memory of the device.

Calls and SMS filter

Filtering the incoming phone calls and SMS allows to block the undesired messages and calls, such as advertisements or messages and calls from unknown numbers.

Anti-theft

Detect the device location or lock its functions in case it has been lost or stolen.

Cloud Checker

URL filter allows to protect user of the mobile device from unsolicited internet sites.

Firewall (settings are available on a mobile device only)

Protects the mobile device from external unauthorized access and prevents leak of vital data via internet. Monitors connection attempts and data transfer via the internet and blocks suspicious connections both on network and application levels.

Security Auditor (settings are available on a mobile device only)

Diagnostic and analysis of the security of mobile device and resolving the detected problems and vulnerabilities.

Application filter

Blocks the launch on mobile device those applications that are not included into the list of allowed by administrator.

8.4.1. Interrupting Running Components

When you use this option, running scans are canceled, components are stopped, and running monitors are paused.

To interrupt all running components of a certain type on stations

1. Select **Anti-virus network** in the main menu of the Control Center, then select a group or individual stations in the hierarchical list.
2. On the toolbar, click **Components management**. Select **Interrupt running components** from the drop-down list.
3. Set the flags next to the types of components which you want to interrupt immediately:
   - **Interrupt Dr.Web Agent Scanner launched by Task Scheduler**—to stop an active remote anti-virus scan that was launched according to the centralized schedule.
   - **Interrupt Dr.Web Agent Scanner launched by administrator**—to stop an active remote anti-virus scan that was launched manually by an administrator via the Control Center.
   - **Interrupt Dr.Web Scanner for Windows launched by user**—to stop an active anti-virus scan which was launched by a user on the station.
   - **Interrupt Dr.Web Agent for Windows components: SpIDer Guard, SpIDer Mail, SpIDer Gate, Office Control, Firewall, Self-protection, and Preventive protection**—to pause the corresponding components.

   To select all components to interrupt, set the flag in the header of the **Interrupt running components** panel.
4. Click **Interrupt**.

8.5. Anti-Virus Scanning of Stations

Anti-virus scanning can be launched by the station user or by the administrator from the Control Center:

- **Local scanning by users.** May be initiated by the station user using the GUI of Dr.Web software or via the command line (in Windows, Linux). This type of scanning is performed by the **Dr.Web Scanner** component. While its configuration can be managed by the administrator in the Control Center, it can only be launched locally on the station. The parameters are described in the **Administrator Manuals** on managing stations.
- **Remote scanning by the administrator.** May be initiated from the Control Center by the anti-virus network administrator. Remote scanning may also be done according to a schedule. This type of scanning is performed by the **Dr.Web Agent Scanner** component. The parameters are specified for a specific scan and are not saved and reused in subsequent scans. Instructions on launching a remote scan and configuring its parameters are provided in the next sections.

8.5.1. Launching Remote Scanning of Stations

The anti-virus network administrator can launch an express, full, or custom scan for security threats on stations via the Dr.Web Agent Scanner component. A remote scan can also be initiated according to a task from the workstation Task Scheduler.

Remote scanning is performed in the background without alerting the station user.

Remote scanning is available only on stations that are online when a scan is launched.

To immediately launch a remote anti-virus scan on stations

1. Select **Anti-virus network** in the main menu of the Control Center.
2. Click the name of a station or group in the hierarchical list that opens.
3. In the toolbar, click **Scan**. In the drop-down list, select one of the scan types:

   Express scan. The following objects will be scanned:
   - main memory (RAM),
   - boot sectors of all disks,
   - autorun objects,
   - root directory of the boot sector,
   - root directory of the Windows OS installation disk,
   - system directory of Windows OS,
   - `My documents` folder,
   - temporary folder of the system,

- temporary folder of the user.

Full scan. A full scan of all hard and removable disks (including the boot sectors) will be performed.

Custom scan. This scan type allows you to select which files and folders to scan and specify some additional parameters of the scan.

4. After you select the scan type, a window with scan parameters will open. Change the parameters if necessary (see the Configuring Remote Scan Parameters section).
5. Click **Scan** to start scanning the selected stations.

To schedule a remote scan on stations

1. Select **Anti-virus network** from the main menu of the Control Center. Select a group or station in the hierarchical list. In the control menu, select **Task Scheduler**. The list of tasks for the station will open.
2. Click the **Create task** icon in the toolbar.
3. In the **General** section, set the name of the task and configure its parameters and start time (see Scheduled Tasks of a Station).
4. In the **Actions** section, select one of the options in the drop-down list (a description of the scan types is given above):
   - **Dr.Web Agent Scanner. Express scan**
   - **Dr.Web Agent Scanner. Full scan**
   - **Dr.Web Agent Scanner. Custom scan**
5. Change the scan parameters displayed below if needed (see Configuring Remote Scan Parameters).
6. Click **Save**.

The task for remote scanning via Dr.Web Agent Scanner that you created will appear on the list of tasks and will start according to the specified periodicity and time.

A **Daily scan** task for performing a remote full scan daily at 16:00 (local station time) on stations is present in the Task Scheduler for workstations by default. The task is disabled for execution. You can edit and enable the task if needed (see Scheduled Tasks of a Station).

8.5.2. Configuring Remote Scan Parameters

Configuration of the **Dr.Web Scanner** component, which performs local scanning at the request of station users, is described in the **Administrator Manuals** on managing stations. Dr.Web Scanner settings have no relation to the remote scan parameters.

The parameters of a remote scan performed by the Dr.Web Agent Scanner component are specified immediately before scanning and apply only to the scan being launched.

Whether a section of the remote scan parameters is available (+) or unavailable (–) depends on the selected scan type as shown in the table below.

Sections of remote scan parameters available depending on the scan type

Scan type	Parameter section			
	General	Actions	Limitations	Exclusions
Custom scan	+	+	+	+
Express scan	+	+	+	–
Full scan	+	+	+	–

Depending on the operating system of the stations on which the remote scan is launched, only the parameters supported by the operating system are available.

8.5.2.1. General

Parameters that are not supported when scanning stations running Unix-like OSs and macOS are given in square brackets **[ ]**.

Parameters that are not supported when scanning stations running Android OS are given in brackets **( )**.

In the **General** section, you can configure the following parameters of remote anti-virus scanning performed by Dr.Web Agent Scanner:

- In the drop-down list, select the scope of the scan:
  - **Scan all disks**—scan all available local drives.
  - **Scan specified paths**—scan only the specified paths.

  In the **Paths selected for scan** field, specify paths to be scanned (how to specify paths is detailed in the Exclusions section).
    - To add a new line, click  and specify a path in the new line.
    - To remove a path from the list, click  next to the corresponding line.
- Set the **(Scan boot sectors)** flag for Dr.Web Server-based Scanner to scan boot sectors. Both boot sectors of logical drives and main boot sectors of physical drives are scanned.
- Set the **[(Scan programs that run on startup)]** flag to scan files that are automatically launched at operating system startup.
- See the **[(Scan loading programs and modules)]** flag to scan processes that are run in the RAM.
- Set the **[(Scan for rootkits)]** flag to enable scanning for malware that hides its presence in the system.

- Set the **Scan fixed volumes** flag to scan fixed hard drives (hard disk drives, etc.).
- Set the **Scan removable media** flag to scan all removable storage media such as floppy or CD/DVD disks, flash drives, etc.
- Set the **Use heuristic analysis** flag for Dr.Web Server-based Scanner to scan for unknown threats using the heuristic analyzer. Note that false positives are possible in this mode.
- Set the **Follow symbolic links** flag to follow symbolic links when scanning.
- Set the **[(Interrupt scanning when switching to battery mode)]** flag to stop the anti-virus scan when the user computer switches to battery power.
- Set the **[(Disable network while scanning)]** flag to disable network and internet connections during the scanning process.
- Set the **Archives** flag to search for threats in files within archives.
- Set the **(Email files)** flag to scan mailboxes.
- Set the **Installation packages** flag to scan program installation packages.
- In the **[(Scan priority)]** drop-down list, select the priority of the scan process relative to the computing resources of the operating system.
- In the **[(Load level of computer resources)]** drop-down list, select the maximum allowed load of computer resources to be utilized by Dr.Web Server-based Scanner when scanning. In the absence of other tasks, computer resources are used to the maximum.

The **Load level of computer resources** option has no effect on the actual resource load when performing a scan on a single-processor system with one core.

- In the **[(Processor cores to use (number))]** field, specify the maximum number of processor cores used while scanning. Integers from 0 to 32 are allowed. 0 means use all available cores. If you are configuring a group of stations, please note that this parameter has an absolute value, not a percentage of the total number of available cores. Because of this, the same value may lead to a different relative load on stations with different numbers of processor cores.
- In the **[(Processor cores to use (%))]** drop-down list, specify the percentage of cores used to the total number of cores available.
- In the **[(Actions after scan)]** drop-down list, select which action will be automatically applied when the scan is completed:
  - **do nothing**—perform no actions on the user computer after the scan is completed.
  - **shutdown station**—shut down the user computer after the scan is completed. Before shutting down the computer, Dr.Web Agent Scanner applies the specified actions to detected threats.
  - **reboot station**—restart the user computer after the scan is completed. Before restarting the computer, Dr.Web Agent Scanner applies the specified actions to detected threats.
  - **suspend station**.
  - **hibernate station**.

8.5.2.2. Exclusions

In the **Exclusions** section, you can specify a list of files and folders to be excluded from a remote anti-virus scan performed by Dr.Web Agent Scanner.

Exclusions can be specified only for a custom scan.

Before adding any exclusions, make sure to check out recommendations on using anti-virus software on computers running Windows OS. The information can be found at https://support.microsoft.com/en-us/topic/virus-scanning-recommendations-for-enterprise-computers-that-are-running-windows-or-windows-server-kb822158-c067a732-f24a-9079-d240-3733e39b40bc. This article is intended to help you improve system performance in the presence of anti-virus software.

To edit lists of files and paths excluded from scanning

1. Specify a path to a file or folder in the **Excluded paths and files** field.
2. To add a new line, click  and specify a path in the new line.
3. To remove a path from the list, click  next to the corresponding line.

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

1. Direct object path in the explicit form:
   - a backslash `\` excludes the entire system disc in Windows OS,
   - a forward slash `/` excludes the entire root file system in a Unix-like OS,
   - a backslash `\` (or forward slash `/` in a Unix-like OS) at the end of a path excludes the folder from scanning,
   - a path that does not end with a backslash `\` (or forward slash `/` in a Unix-like OS) means that all subfolders of the selected folder are excluded from scanning.

   Example for Windows: `C:\Windows`—do not scan files in the `C:\Windows` folder and all its subfolders.

   Example for a Unix-like OS: `/etc`—do not scan files in the `/etc` folder and all its subfolders.
2. Masks for objects excluded from the scan. The `?` and `*` characters can be used to specify masks.

   Example for Windows: `C:\Windows\*\*.dll`—do not scan any files with the `dll` extension in all subfolders of the `C:\Windows` folder.

   Example for a Unix-like OS: `/etc/*/*.pub`—do not scan any files with the `pub` extension in all subfolders of the `/etc` folder.
3. Environment variables set in the operating system as parts of paths to objects to be excluded from the scan.

Example for Windows: `%WINDIR%\SysWOW64\`—do not scan any files in the `SysWOW64` subfolder of the `C:\Windows` folder.

Example for a Unix-like OS: `/home/*/network`—do not scan any files in the `network` subfolder of the `/home` folder.

4. Regular expression. Paths can be specified using regular expressions. Any file whose full name (with the path) corresponds to a regular expression is excluded from the scan.

Use the following regular expression syntax to specify excluded object paths:

`qr{`<*expression*>`}`<*flags*>

The most frequently specified flag is `i`: "ignore letter case difference".

Examples of specifying excluded paths using regular expressions

Regular expression	Value
`qr{\\pagefile\.sys$}i`	do not scan Windows OS swap files
`qr{\\notepad\.exe$}i`	do not scan `notepad.exe` files
`qr{^C:}i`	do not scan disk `C:`
`qr{^.:\\WINNT\\}i`	do not scan `WINNT` folders on all disks
`qr{(^C:)|(^.:\\WINNT\\)}i`	two previous cases combined
`qr{^C:\\dir1\\dir2\\file\.ext$}i`	do not scan `c:\dir1\dir2\file.ext`
`qr{^C:\\dir1\\dir2\\(.+\\)?file\.ext$}i`	do not scan `file.ext` if it is located in the `c:\dir1\dir2` folder or its subfolders
`qr{^C:\\dir1\\dir2\\}i`	do not scan `c:\dir1\dir2` and its subfolders
`qr{dir\\[^\\]+}i`	do not scan the `dir` subfolder located in any folder, but do scan its subfolders
`qr{dir\\}i`	do not scan the `dir` subfolder located in any folder and its subfolders

Regular expressions are briefly described in the **Appendices** document, in Appendix I. Regular Expressions Used in Dr.Web Enterprise Security Suite.

8.5.2.3. Actions

On the **Actions** tab, you can configure Dr.Web Agent Scanner reactions on detection of infected or suspicious files, malware, and malicious archives as a result of scanning.

The actions are applied automatically.

The following actions can be applied to detected threats:

- **Cure**—restore the original state of the object before the infection. If the object is incurable or the attempt to cure it fails, the action set for incurable objects is applied instead.

  Available for objects infected with known curable viruses only, except for trojans and infected files within compound objects (archives, email files, or file containers).
- **Delete**—delete the object.
- **Move to quarantine**—move the object to the special Quarantine folder on the station.
- **Report**—send a notification to the Control Center about the detection of a threat (see the Setting Notifications section on how to configure alerts).
- **Ignore**—skip the object without performing any action and do not send a notification in the scan statistics.

Table 8-2. Reactions of Dr.Web Agent Scanner to various threats

Object	Action				
	Cure	Delete	Move to quarantine	Report	Ignore
Malicious	+/*	+	+	available if one of the keys includes the AllowReportAction=Yes option	
Suspicious		+	+/*		+
Incurable		+	+/*		
Installation packages		+	+/*		
Archives		+	+/*		
Email files			+	+/*	+
Boot sectors	+/*			+	
Adware		+	+/*		+
Dialers		+	+/*		+

Object	Action				
	Cure	Delete	Move to quarantine	Report	Ignore
Jokes		+	+/*		+
Riskware		+	+/*		+
Hacktools		+	+/*		+

Conventions

+	action is enabled for this type of object
+/*	action is set as default for this type of object

To set actions for detected threats, use the following options:

- The **Malicious** drop-down list specifies the reaction to detecting a file infected with a known virus.
- The **Suspicious** drop-down list specifies the reaction to detecting a file presumably infected with a virus (upon an alarm of the heuristic analyzer).

If a scan includes the OS installation folder, it is recommended that you select the **Report** action for suspicious files.

- The **Incurable** drop-down list specifies the reaction to detecting a file infected with a known incurable virus, as well as if an attempt to cure a file fails.
- The **Malicious installation files** drop-down list specifies the reaction to detecting a malicious or suspicious file in a program installation package.
- The **Malicious archives** drop-down list specifies the reaction to detecting a malicious or suspicious file in a file archive.
- The **Malicious email files** drop-down list specifies the reaction to detecting a malicious or suspicious file in the email format.

If a threat or suspicious program code is detected within a compound object (archive, email file, or file container), the action selected for this object type is applied to the whole object, not just to the infected part.

- The **Infected boot sectors** drop-down list specifies the reaction to detecting a threat or suspicious program code in the boot sector area.
- In the following drop-down lists, set the reactions to detecting the corresponding type of unsolicited software:
  - **Adware**;

- **Dialers**;
- **Jokes**;
- **Riskware**;
- **Hacktools**.

If you select **Ignore**, no action is performed: no notifications are sent to the Control Center, as opposed to when you select **Report** on threat detection.

Set the **Show scan progress** flag to display a progress bar and the status bar of the remote scan process in the Control Center.

8.5.2.4. Limitations

Parameters that are not supported when scanning stations running Unix-like OSs and macOS are given in square brackets **[ ]**.

In the **Limitations** section, you can configure the following parameters of remote anti-virus scanning performed by Dr.Web Agent Scanner:

- **Maximum scanning time (ms)**—maximum scanning time per file in milliseconds. After the specified time the scan is terminated. 0 means no limit on scanning time.
- **Maximum archive nesting level**—maximum nesting level for scanning the contents of objects. The object contents are scanned up to the specified nesting level, the rest are ignored. 0 means that objects with any nesting level are scanned in full.
- **[Maximum archive size (KB)]**—maximum size of a compound object to be scanned in kilobytes. If the size exceeds the limit, unpacking and scanning is not performed. 0 means that objects of any size are scanned.
- **Maximum compression ratio**—maximum compression ratio of archives to be scanned. If the compression ratio exceeds the specified value, the archive is not scanned. 0 means that archives with any compression ratio are scanned.
- **[Maximum size of extracted files (KB)]**—maximum size that archive files may reach after unpacking, in kilobytes. If the expected size of archive files after unpacking exceeds the specified limit, archive unpacking and scanning is not performed. 0 means that archives of any size when unpacked are scanned.
- **[Compression check threshold (KB)]**—minimum size of a file inside the archive in kilobytes starting from which the compression ratio is checked to apply the **Maximum compression ratio** setting. 0 means that the size of files in the archive is not checked and the compression ratio check is not performed.

8.6. Viewing Workstation Statistics

Via the control menu of the **Anti-virus network** section, you can view the following information:

- Statistics—to view data on anti-virus components functioning on the stations, stations and anti-virus components status, to view and save the reports, that contains all statistic data or selective statistic tables.
- Charts—to view charts with information on infections, detected on the stations.
- Quarantine—remote access to the Quarantine contents on the station.

8.6.1. Statistics

You can configure the automatic generation of a statistic report that only includes the statistic tables you need. The report in a selected format can be either saved on Dr.Web Server or sent via email.

For this, configure the **Create statistic report** task in the Dr.Web Server schedule.

To view tables

1. Select the **Anti-virus network** item in the main menu of the Control Center. Click the name of the station or group in the hierarchical list in the window that opens.
2. Select a necessary item in the **Statistics** section of the control menu.

The **Statistics** section of the menu contains the following items:

- **Threats**—view information on events related to threats (a list of infected objects, threat names, anti-virus actions, etc.).

If URLs for viruses and miners are blocked, the action "Reported" is displayed in the table.

- **Errors**—view a list of scanning errors on a selected workstation for a certain period.
- Summary Data—view and save reports that contain all summary statistics or partial summaries for specified table types. This menu item will not be displayed if all other menu items are hidden in the **Statistic** section.
- Scan Statistics—view statistics on the operation of anti-virus components on workstations.
- **Start/Stop**—view a list of components that have been launched on workstations.
- **Threat statistics**—view information on threats detected on workstations. The information is grouped by threat type and number.
- Status—view information on unusual states of workstations which might need your attention.

- **Tasks**—view a list of tasks assigned to a workstation during a certain period.
- **Blocked devices**—view a list of devices blocked on stations by the Office Control component. If read and write access for users or user groups is configured for a device with its own file system, the table also contains information on the user the blocked operation was run as.
- **Products**—view information on the Dr.Web Server repository products installed on stations.
- **Virus databases**—view information on installed virus databases: name of the file containing a particular database, virus database version, total number of threat records in the database, database creation date. This menu item is available only if single stations are selected.
- **Modules**—view information on Dr.Web anti-virus software modules: functional name, MD5 hash, full version of the module, etc. This menu item is available only if single stations are selected.
- **Preventive protection events**—view information on events detected on stations by the Preventive protection component.
- Application Control Events—view information on events detected on stations by the Application Control component.
- **Dr.Web Agent installations**—view a list of Dr.Web Agent installations on a workstation or group of workstations.
- **Dr.Web Agent deinstallations**—view a list of workstations with uninstalled Dr.Web anti-virus software.

To show hidden items of the **Statistics** section, select **Administration** in the main menu, then select **Dr.Web Server configuration** in the control menu. On the **Statistics** tab, set the corresponding flags (see below), then click **Save** and restart Dr.Web Server.

Table 8-3. Correspondence between items in the Statistics section and flags in the Statistics section of the Dr.Web Server configuration

Statistics section items	Flags from the Statistics section in the Dr.Web Server configuration
Threats	Detected security threats
Errors	Scan errors
Scan statistics	Scan statistics
Start/Stop	Start/Stop of components
Threat statistics	Detected security threats
Status	Station statuses
Tasks	Station tasks execution log
Blocked devices	Blocked devices

Statistics section items	Flags from the Statistics section in the Dr.Web Server configuration
Virus databases	Station statuses Virus database statuses
Modules	List of the station modules
Preventive protection events	Detected security threats
Application Control events	Application Control statistics on processes activity Application Control statistics on processes blocking
Dr.Web Agent installations	Dr.Web Agent installations

The windows with the statistics for different components and the total statistics of workstations have the same interface, and the actions for managing the provided information are similar.

The following sections provide several examples for viewing the statistics via Dr.Web Security Control Center.

8.6.1.1. Summary Data

To view summary data

1. In the hierarchical list select a station or a group.
2. Select the **Summary data** item from the **Statistics** section of the control menu.
3. The window with report table data will be opened.

   To include specific data in the report, click on the toolbar and select necessary types in the drop-down list: **Scan statistics**, **Threats**, **Tasks**, **Start/Stop**, **Errors**. Statistics from this report sections are similar to statistics from the corresponding items of the **Table** section. To view the report with selected tables, click **Refresh**.
4. If the report contains the table with detected threads, the following options become available on the toolbar:

Option	Description
Exclude files from scan	Allows to add selected objects into the list of exclusions from the scan by protection components: a) In the **Threats** table, set the flag next to the one of several detected objects. b) Click . c) In the opened window, specify the following options:

Option	Description
	• **Exclude from the scan and set personal settings of SpIDer Guard**—add selected objects into the list of exclusions from the scan by SpIDer Guard component. At this, if the network nodes whose exclusions list will be changed are inheriting SpIDer Guard settings from their primary groups, then inheriting will be broken and personal settings will be set. • **Exclude from the scan and set personal settings of Dr.Web Scanner**—add selected objects into the list of exclusions from the scan by Dr.Web Scanner component. At this, if the network nodes whose exclusions list will be changed are inheriting Dr.Web Scanner settings from their primary groups, then inheriting will be broken and personal settings will be set. • In the **Exclude for the following objects** list, select the network nodes to add the selected object into exclusions list: either only for station on which the object was detected or for stations and user groups selected in the list. d) Click **Exclude**.
Scan	Rescan selected objects. Select the scan mode in the drop-down list.

5. To view the data for certain time period, specify the certain time period relatively today in the drop-down list, or select the arbitrary date range on the toolbar. To select the arbitrary date range, enter required dates or click the calendar icons next to the date fields. To load data, click **Refresh**.
6. To save the report for printing or future processing, click one of the following buttons:

   Save data in CSV file,

   Save data in HTML file,

   Save data in XML file,

   Save data in PDF file.

8.6.1.2. Scan Statistics

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

1. In the hierarchical list select a station or a group.

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

2. In the control menu select the **Scan Statistics** item from the **Statistics** section.
3. The Statistics window will be opened. The statistics for last 24 hours are displayed by default.
4. To view the data for certain time period, specify the certain time period relatively today in the drop-down list, or select the arbitrary date range on the toolbar. To select the arbitrary

date range, enter required dates or click the calendar icons next to the date fields. To load data, click **Refresh**. The tables with statistics will be loaded.

5. To view the detailed statistics of anti-virus components, click the station name in the table. A windows (or a section of current window) with detailed statistics will be opened.
6. To sort the data in columns of a table, click the certain point (decrease or increase) in the header of the table.
7. To save the table for printing or future processing, click one of the following buttons:

   Save data in CSV file,

   Save data in HTML file,

   Save data in XML file,

   Save data in PDF file.
8. To view the statistics as a charts, click **Charts** in the control menu. A statistics charts window will be opened (see detailed description below).

8.6.1.3. Status

To view data on workstations status

1. In the hierarchical list select a station or a group.
2. In the control menu select **Status** item from the **Statistics** section.
3. Status information are displayed according to the filter settings. Click on the table header, to change the following filter parameters:
   - In the **Search** field, enter the arbitrary string to search by all sections of the table.
   - In the **Severity** drop-down list, set the flags for necessary levels of messages severity: the list of messages on status will contain only messages with selected severity. All flags are set by default.
   - In the **Source** list, set the flags for those sources of messages appearance that will be displayed in the list:
     - **Agent**—display events from Dr.Web Agents connected to this Dr.Web Server.
     - **Server**—display events from this Dr.Web Server.
   - In the **Stations** list, set the flags for stations status types, messages on which will be displayed in the list:
     - **Online**—display events for stations which are connected to this Dr.Web Server and currently online.
     - **Offline**—display events for stations which are connected to this Dr.Web Server and currently offline.
     - **Deinstalled**—display the last event for stations with deinstalled Dr.Web anti-virus software.

   To manage filter settings, use the following buttons on the filter pane:

- **Default**—set the default values to all filter settings.
- **Refresh**—apply selected filter settings.

4. You can format the way the data are presented just like in the statistics window above.

To view operation results and statistics for several workstations, select those workstations in the network hierarchical list.

5. To save the report for printing or future processing, click one of the following buttons:

 **Save data in CSV file**,

 **Save data in HTML file**,

 **Save data in XML file**,

 **Save data in PDF file**.

8.6.1.4. Application Control Events

Receiving Statistics Configuration

To activate sending the information for the Application Control events from the stations

1. In the **Anti-virus network** section, in the network tree select station or station group with Application Control installed from which you want to receive information on applications launch.
2. In the control menu, select **Windows** → **Dr.Web Agent** if you selected a group, or **Dr.Web Agent** if you selected a station.
3. On the **General** tab, set the **Track Application Control events** flag to track processes activity at stations detected by Application Control and send events to Dr.Web Server. If there is no connection with Dr.Web Server, events are collected and sent upon connect. If the flag is cleared, processes activity is ignored.
4. Click **Save**.

To activate collecting the information for the Application Control events at Dr.Web Server

1. In the **Administration** → **Dr.Web Server configuration** section, go to the **Statistics** tab.
2. Set one of the following options:
   - **Application Control statistics on processes activity** to receive and write information on any activity of all processes: either allowed or prohibited to launch by Application Control. Setting this option will enable registration of applications in the catalog, as long as at least one profile is created and assigned, with one or several categories of functional analysis criteria selected.
     Before creating the profiles and assigning them to stations of anti-virus network, all applications are allowed to be launched.

- **Application Control statistics on processes blocking** to receive and write information on activity of all processes prohibited to launch by Application Control. For this option, applications will be written to the catalog only after creating profiles by the settings of which application launch will be blocked, and assigning these profiles on stations of anti-virus network.

The **Application Control statistics on processes activity** flag may significantly increase resource intensity of statistics collecting over all anti-virus network.

3. Click **Save**.
4. Restart Dr.Web Server.
5. After restarting, Dr.Web Server starts collecting statistics on applications launch received from all stations with Application Control installed.

Viewing Statistics

To view events detected on stations by Application Control component

1. In the hierarchical list select a station or a group.
2. In the control menu select **Application Control events** item from the **Statistics** section.
3. The window containing the list of applications which were prohibited or allowed to run at the selected stations will be opened.
4. The statistics for last 24 hours are displayed by default. To view the data for certain time period, specify the certain time period relatively today in the drop-down list, or select the arbitrary date range on the toolbar. To select the arbitrary date range, enter required dates or click the calendar icons next to the date fields. To load data, click **Refresh**. The tables with statistics will be loaded. The table below contains the description of the table columns.

Table 8-4. Description of the columns in the Application Control Events table

Column Name	Description
Identifier	Station identifier
Station	Station name
Station address	Station address
Security identifier	Security identifier of the user account
User	Station user
Event type	Type of event detected on the station
Applied action	Action applied to the application launched on the station

Column Name	Description
Functional analysis criterion	Criterion for allowing or blocking application on the station
Functional analysis mask	Parameter of the functional analysis criterion. This parameter determines whether the application is allowed to run on the station or not.
Profile ID	Profile identifier
Profile name	Profile name
Rule ID	Rule identifier
Rule name	Rule name
Operation mode	Operation mode of the rule
Process file path	Process file path
Process	A process that is allowed or prohibited to launch on the station
Bulletin with process hash	Bulletin containing the hash of the launched process file
Script file path	Script file path
Script	Script file
Bulletin with script hash	Bulletin containing the hash of the launched script file
Event occurrence	Date and time when the event occurred
Event notification	Date and time of event notification
File hash (SHA-256)	The hash value of the file (SHA-256 algorithm)
File description	File description
Publisher	Publisher of the file
Certificate issuer	Certification authority that issued the certificate
Certificate thumbprint (SHA-1)	The hash value of the certificate (SHA-1 algorithm)
Certificate start date	Certificate start date
Certificate end date	Certificate end date

5. To save the table for printing or future processing, click one of the following buttons:

   Save data in CSV file,

Save data in HTML file,

Save data in XML file,

Save data in PDF file.

When a profile or rule is in test mode, applications launched on assigned workstations are checked against each step of the entire Application Control scheme, top to bottom. Displayed statistics will include all cases when an application matched any of the criteria: functional analysis settings, rules, and trusted applications group. Therefore, one application may have several records in the **Applied action** column saying that it was allowed by one criterion and/or blocked by another.

Creating Rules

To create a new rule basing on the event statistics of the Application Control

1. In the **Statistics** → **Application Control events** section, select a row with the event in the attempt to launch an application for which you want to create the rule for controlling the launch.
2. The table row click opens the window with information on the selected event.
3. Click **Create rule** (based on object data or based on process data).
4. The window for creation of a new rule will be opened. Specify the following settings:
   a) In the **Profile name** drop-down list, select the Application Control profile for which the rule will be created.
   b) In the **Rule name** filed, specify the name of creating rule.
   c) For the **Rule type** option, select the type of creating rule: deny or allow.
   d) For the **Operation mode** option, select the operation mode of the creating rule (corresponds the **Switch rule to test mode** flag at rule creation in a profile):
   If you want to check the rule operation, select the **Test** option. Applications will not be blocked at stations, but the activity log will be written as for enabled settings.
   Application launch and block results based on a rule in test mode will be displayed in the **Application Control Events** section.
   With the **Active** option, the rule operates in active mode and blocks applications at stations by specified rule settings (see also modes of profiles operation).
   e) In the **Prohibit the launch of applications on the following criteria/Allow the launch of applications on the following criteria** section (depending on the rule type selected at step 4b), the fields will be automatically specified in accordance with the applications on the base of which the rule is creating. If necessary, you can edit the settings.
5. Click **Save**. The rule will be created in the specified profile of the Application Control.

8.6.2. Charts

Infection Charts

To view general charts with information on detected infections

1. Select **Anti-virus network** in the main menu of the Control Center, then in the opened window in the hierarchical list click the station or group name. In the opened control menu in the **General** section, select **Charts**.
2. A window with the following charts will open:
   - **Viral activity**—displays the total number of malware detected per each time slot for all selected stations and groups.
   - **Most common threats**—displays a list of top ten most detected threats in files. The chart displays numerical data on objects corresponding to a specific threat.
   - **Threat classes**—displays a list of threats corresponding to the malware specification. The pie chart displays percentage between all of detected threats.
   - **Actions performed**—displays a list of actions performed to detected malware. The pie chart displays percentage between all of performed actions.
   - **Most attacked stations**—displays a list of stations with detected security threats. The chart displays the total number of threats for each station.
3. To view the data for a certain time slot, specify it in the drop-down list on the toolbar: view a certain day or a month. Alternatively you can set an arbitrary date range. To do this, enter the required time and the date or click the calendar icons to set a time period. Click **Refresh** to view the data.

Total Statistics Charts

The **Charts** entry of the **General** section and some entries of the **Statistics** section have graphical and numerical data available for view. The table below lists charts and sections of the control menu where they are displayed.

Table 8-5. Correspondence between charts and sections of the control menu

Charts	Sections
Viral activity	Charts
Most common threats	Charts Threats Threat statistics
Threat Classes	Charts

Charts	Sections
	Threat statistics
Most attacked stations	Charts
Actions performed	Charts Threats
Count of errors by stations	Errors
Count of errors by components	Errors
Threats by components	Start/Stop
Errors by components	Start/Stop

- **Count of errors by stations**—displays a list of stations with detected operation errors in anti-virus components. The graph displays the total number of errors for each station.
- **Count of errors by components**—displays a list of anti-virus components with detected operation errors. The pie chart displays percentage between errors of all components.
- **Threats by components**—displays a list of anti-virus components which detected the threats. The chart displays the total number of threats detected by each component.
- **Errors by components**—displays a list of anti-virus components with detected operation errors. The chart displays the total number of errors for each component.

8.6.3. Security Identifiers

To view information on security identifiers on stations

1. Select **Anti-virus network** in the main menu of the Control Center, then click the station or group name in the hierarchical list in the window that opens. In the control menu on the left, in the **General** section, select **Security identifiers**.
2. A window with the following data will open:
   - **Identifier**—unique identifier of the station. It is specified when creating a station account and cannot be changed further.
   - **Station**—station name. It is specified when creating a station account and will be automatically replaced with the computer name after the Dr.Web Agent connects.
   - **Address**—station IP address.
   - **Security identifier**—the SID (security identifier) of the computer. The field is filled in automatically after the connection of a station under Windows OS to Dr.Web Server.
   - **Last connected on**—date of the last connection attempt of the station to the Dr.Web Server.

3. To view the data for a certain time slot, specify it in the drop-down list on the toolbar: view a certain day or a month, then click **Refresh**. Alternatively you can set an arbitrary date range. To do this, enter the required time and the date or click the calendar icons to set a time period, then click **Refresh** to view the data.

8.6.4. Quarantine

Quarantine Content

Files can be added to the quarantine by one of the anti-virus components, for instance, Dr.Web Scanner.

User can rescan files in quarantine via the Control Center or via the Quarantine Manager on the station.

To view and manage quarantine via the Control Center

1. Select the **Anti-virus network** item in the main menu, then click the name of the station or group in the hierarchical list. Select the **Quarantine** item in the **General** section of the control menu.
2. A new window with table that contains quarantine current state opens.

   If you select one workstation, a table in the window displays objects in quarantine at this station.

   If you select more than one stations or one or more groups, the windows displays a set of tables with quarantined objects for each station.

   Statistic on rescan of quarantined object that is given in the **Information** column, considers only rescans launched via the Control Center.

   If more than one threat has been moved to quarantine, click the number of moved objects in the **Information** column to view the list of threats in the popup window.

   If a quarantined object has the **Not malicious** status, it means that after the object was quarantined as a threat, a rescan has been performed and the object has been marked as safe.

   Restoring objects from the quarantine can be done only manually.

3. To filter files by time when they were quarantined, specify the certain time period relatively today in the drop-down list, or select the arbitrary date range on the toolbar. To select the arbitrary date range, enter required dates or click the calendar icons next to the date fields. To load data, click **Refresh**.
4. To change the table view, click the icon in the table header:
   - Specify rows display settings (most relevant for long strings).

- Select the columns to display in the table.

5. To filter quarantine files, click in the table header and specify the following filtering parameters:
   - **Search**—specify the arbitrary string to search by all sections of the table. The table will contain only rows that correspond to the search results.
   - **Moved by component**—select Dr.Web protection component which moved the files to quarantine.
   - **Threat**—select the name on detected threat according to the Doctor Web company classification.
   - **Original name**—enter the original name of the object before moving to quarantine.
   - **File size, B**—using the slider, specify sizes range of detected objects in bytes.

   Click **Apply** to display quarantine files according to the specified parameters of the filter.

   Click **Default** to reset all filtering parameters into default values.
6. To manage files in quarantine, set the flag for the corresponding file, group of files or for all files in the quarantine (at the table header). On the toolbar, select one of the following actions:

Option	Description
Delete files	
Delete selected files	Delete selected files from the quarantine and from the system.
Delete all files	Delete from the quarantine and from the system all files that match selected filter parameters. i.e. all files displayed in the quarantine window.
Export	Copy and save selected file. Once the suspicious files are moved to local quarantine on user's computer, you can copy and save these files via the Control Center. For instance, to send the files to Doctor Web virus laboratory for analysis. When exported, a file is placed into archive. The archive's name corresponds with a hash of the exported file. Besides the exported object, the archive contains a CSV file with general information about the object. By default, the archive is protected with a password `virus`.

Option	Description
Restore files	
	Use the restore option only if you are sure that objects are harmless.
	Restore selected files Restore the original location of the files selected in the window, i.e. restore the files on stations to the folders where they had resided before were moved to the quarantine.
	Restore files by parameters In the opened window, specify the following settings: • If the one object is selected: ▫ **Restore file as**—restore selected file from the quarantine and place it to specified path with specified name. In the **Restore file to the following path** field, specify the full path on the station by which the selected file will be restored. File name is obligatory. By default, the original location and file name is set (before moving). If necessary, you can change this parameter. ▫ **Restore files by threat type**—restore from the quarantine all files that have been classified with the same threat type as the selected file. The threat type is given in the **Restore files containing the following threat** field. ▫ **Restore files by path**—restore from the quarantine all files moved from the specific folder. In the **Restore all files moved to the quarantine from the following folder** field, specify the path to the folder at station. All files that have been moved to the quarantine from this folder will be restored. By default, the path to the folder where the selected file were resided is set. If necessary, you can change this parameter. • If several objects are selected: ▫ **Restore files**—restore the original location of the files on a computer, i.e. restore the files to the folders where they had resided before were moved to the quarantine. ▫ **Restore files by threat type**—restore from the quarantine all files that have been classified with the same threat type as the selected files. • In the **Restore on the following objects** list, select network nodes to restore the selected object from the quarantine: either only for station on which the object was detected or for user groups selected in the list. • **Add exceptions as personal settings of SpIDer Guard**—add selected objects into the list of exclusions from the scan by SpIDer Guard component. At this, if the network nodes whose exclusions list will be changed are

Option	Description
	inheriting SpIDer Guard settings from their primary groups, when inheriting will be broken and personal settings will be set. • **Add exceptions as personal settings of Dr.Web Scanner**—add selected objects into the list of exclusions from the scan by Dr.Web Scanner component. At this, if the network nodes whose exclusions list will be changed are inheriting Dr.Web Scanner settings from their primary groups, when inheriting will be broken and personal settings will be set.
	Restore all files Restore the original location of all files in the window, i.e. restore the files on stations to the folders where they had resided before were moved to the quarantine.
Scan files	
	Scan selected files Rescan selected in quarantine files.
	Scan all files Rescan all files in the quarantine window.

The request for restoring and rescanning will be sent to offline stations only after stations connect to Dr.Web Server.

7. Export data about the quarantine state to a file in one of the following formats:
   - **Save data in CSV file**,
   - **Save data in HTML file**,
   - **Save data in XML file**,
   - **Save data in PDF file**.

8.6.5. Technical Support Reports

Collecting system information

1. Select a station or group of stations to create a report for.
2. Click **Create a technical support report** on the toolbar.
3. Confirm the start of report creation.

After starting report creation for a station or group of stations, the icon remains active. However, it is impossible for a station to run several reports at the same time. For a group, if you click the icon again, the report creation will be launched only for those stations where the creation of the previous report has been completed or stopped, other stations will ignore this command.

4. To view the status of the report creation, click **Details**. If report creation has been started or delayed, a message will appear containing a link to the Control Center section with a table which displays the progress of report creation and the files of created reports.

Viewing reports

Information about the status of report creation as well as the files of created reports are available in the table in the **Anti-virus network** → **General** → **Technical support reports** section.

The table can store several reports for the same station.

The table contains the following data:

- **Identifier**—station ID.
- **Station**—station name.
- **Station address**—station address.
- **Report name**—report file name.
- **SHA-256 hash**—hash value of the file (SHA-256 algorithm).
- **Progress**—progress (of report creation) in percent.
- **State**—state of report creation (**Creating**/**Downloading**/**Done**/**Failed**).
- **Errors**—error message.
- **Starting time**—report creation start time.
- **Ending time**—report creation end time.

The buttons above the table allow you to start or cancel report creation, download reports, or delete report records from the table and the database. Once a record is deleted, the corresponding report file will be deleted from Dr.Web Server after running the **Purge old records** action in the **Administration** → Database management section or as a result of running a task with the corresponding action in the Dr.Web Server Task Scheduler.

The table does not store the state for pending reports (when Dr.Web Agent has not yet sent status information) or reports from stations that do not support this function.

8.7. Mailing of Installation Files

After a new stations account is created in the Control Center, the personal installation package for Dr.Web Agent installation is generated. Installation package contains the Anti-virus installer and the set of parameters for connecting to Dr.Web Server and for authorization of the station at Dr.Web Server (description of installation package and the process of Dr.Web Agent installation via this package is given in the **Installation Manual**, in the Local Installation of Dr.Web Agent section).

After the installation package is created, for the convenience of their distribution, you can send installation packages to the user's email.

To send installation packages, the email content is formed the following way:

a) If Dr.Web Server does not contain the packages for stations under Linux OS, macOS, Android OS (**Dr.Web enterprise products** are not downloaded on Dr.Web Server): the letter attachment contains the Dr.Web Agent for Windows installation package and the configuration file with the settings for connecting to Dr.Web Server for stations under Linux OS, macOS, Android OS.

b) If Dr.Web Server contains at least one package except packages for stations under Windows OS: the letter attachment contains the Dr.Web Agent for Windows installation package, the configuration file with the settings for connecting to Dr.Web Server for stations under Linux OS, macOS, Android OS, and the link to download installation packages for stations under Linux OS, macOS, Android OS.

To email installation files

1. Select the **Anti-virus network** item in the main menu of the Control Center and in the opened window, select the following objects in the hierarchical list:
   - select the station to email the file generated for this station.
   - select the group of stations to email all files generated for stations of this group.

   Use CTRL or SHIFT to select several objects at time.
2. On the toolbar, click **General** → **Mail installation files**.
3. In the **Mailing of installation files** opened section, specify the following parameters:
   - In the **General** section:
     - Set the **Pack in zip archive** flag to pack installation packages into a ZIP archive. Archiving can be useful if the user's email system contains filters that block sending of executable files in email attachment.
     - Set the **Send the link only** flag to email only the link to download the package. At this, the installation package file is not attached to the email. This option may be useful if the client mail server removes attachments from emails automatically.
   - In the **Recipient email addresses** section, specify the email address to send an email with the installation package or the download link to. If several stations or groups were

selected, specify the email addresses to send emails to each station separately next to each station name.

> Parameters of email sending are configured in the **Administration** menu, in the **Dr.Web Server configuration** section, on the **Network** tab, on the Email internal tab.

4. Click **Send**.

8.8. Sending Notifications to Stations

The system administrator may send the users informational messages including:

- message text;
- hyperlinks to internet resources;
- company logo (or any other graphic presentation).

The exact date of message reception is specified in the window title.

These messages are displayed on a user's computer as popup windows (see Figure 8-1).

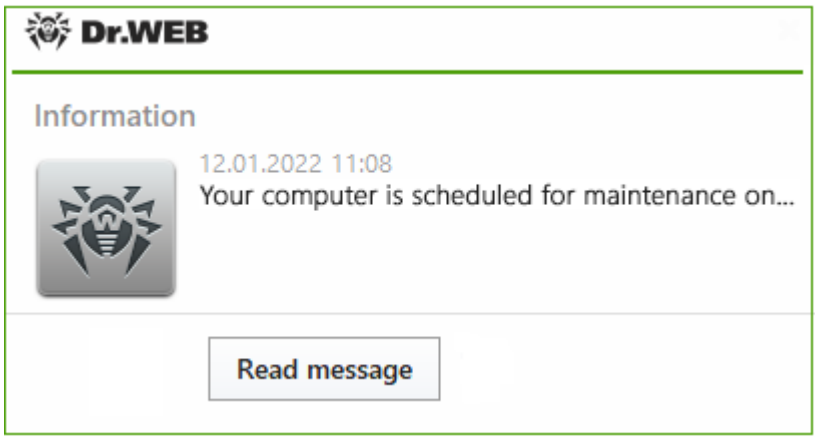


Figure 8-1. Message window on a station under Windows OS

To send a message to a user

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. In the window that opens, select a station or a group on the hierarchical list and click **General** → **Send message** on the toolbar.
3. Fill in the following fields in the window that opens:
   - In the **Message title** field, you can specify the title of the message, e.g. the company name. This text will be displayed in the message window title to the right of the logo. If you leave this field blank, information about the message will be displayed in the title of the message window.
   - **Message text**—a required field containing the message itself.

- Set the **Show logotype in the message** flag to display a graphical object in the message window title. Specify the following logotype parameters:
  - On the right of the **Logotype file** field, click  to load the logotype file from a local resource and select the necessary object in the file system browser (see Logo file format).
- Set the **Show link in the message** flag to include a hyperlink to web resources in the message.

To insert a link:

a) In the **Link name** field, specify the link name—text to be displayed in place of the link in the message.

b) In the **URL address for the link** field, specify the URL address of the web page to open on clicking the link.

c) In the **Message text** field, insert the `{link}` marker in all places where you want the link to appear. In the resulting message, the link with the specified parameters will be shown instead of the marker. You may use an unlimited number of the `{link}` markers in a text, however, all of them will have the same parameters from the **URL address for the link** and **Link name** fields. If one or several `{link}` markers are used, the link will be inserted instead of the markers.

d) If a `{link}` marker is not present in the **Message text** field, the link will be inserted once at the end of the message on a separate line.

- Set the **Send to online stations only** flag to send the message to online stations only. If the flag is set, messages are not sent to offline stations. If the flag is cleared, message sending to offline stations is postponed until they are connected.
- Set the **Show send status** flag to show a notification with the message send status.

4. Click **Send**.

Logo file format

A file with a graphic image (logotype) inserted into a message should meet the following requirements:

1. File graphic format: BMP, JPG, PNG, GIF, SVG.
2. Logo file size may not exceed 512 KB.
3. Overall image size is 72x72 pixels. Images of other sizes will be scaled to the default size when they are sent.
4. Any bit depth (8–24 bit).

If you want to use a logotype with a transparent background in the message, use the PNG or GIF file formats.

Before sending a message to a user (especially to multiple users), it is recommended to send it first to any computer with the Dr.Web Agent installed to check the adequacy of the result.

Message example

To send a message similar to the one displayed in Figure 8-1, the following parameters were set:

Message text:

```
Dear user!


The Dr.Web Firewall component was installed on your computer.

For details on the component functionality, click {link}.


Sincerely,

Administration
```

URL address for the link: `http://drweb.com/`

Link name: `here`

Chapter 9: Managing Stations in Virtual Environments

Dr.Web Enterprise Security Suite can be used for protecting virtual infrastructure—virtual machine clusters providing services to clients (hereinafter referred to as client VMs): virtual hosting, remote desktop services, corporate clouds, etc.

One or several virtual machines in the cluster are assigned as *service* VMs; by means of the special software (Dr.Web Scanning server) installed on them the service VMs process requests for anti-virus scanning from other VMs.

The Scanning server includes:

- the Scanning Engine that scans the received data for threats;
- virus databases and filter databases for Office control.

The Dr.Web Agent software is installed on the client VMs, after which it needs to be connected to the Scanning server so that Dr.Web Agent enters Dr.Web Virtual agent mode. In this mode it operates under the control of Dr.Web Server and transmits requests for anti-virus scanning as well as files to be scanned to the Scanning server on the service VM. This mode of operation allows to significantly reduce the load on client virtual machines due to the following factors:

- scanning is performed outside client VMs;
- there is no need to keep virus databases and filter databases updated on client VMs.

Configurations with the Scanning server allow to:

- save RAM;
- reduce the load on the disk subsystem of a VM;
- reduce the network load.

Such approach causes higher CPU usage. Configurations with the Scanning server are most efficient when the virtual network is arranged within one physical server. Only using a virtual (rather than physical) network for data transfer between VMs located on the same server (hypervisor) can ensure a high data exchange rate and scanning speed.

The Scanning server can be included in any group. It is also possible to combine Scanning servers into a separate group, including automatically on the basis of predefined rules.

Adding the Scanning server to groups and defining membership rules is performed in the same way as for any other station. Detailed information on group management can be found in the Including Stations into Groups section.

Dr.Web Agent operating in Dr.Web Virtual agent mode sends requests for scanning files and URLs to the Scanning server. After switching to this mode, Dr.Web Agent stops using virus databases and is left unprotected if the connection with the Scanning server is lost. Thus, Virtual agents can be used only if the Scanning server is installed and configured.

9.1. Connecting Stations to the Scanning Server

The Scanning server is a virtual machine with a special status and with special software for processing scanning requests from other VMs installed.

For detailed information concerning the installation and the initial configuration of the Scanning server, refer to **Dr.Web Enterprise Security Suite Installation Manual**, 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.

Connecting stations to the Scanning server is available only if it is permitted by the terms of your license.

To connect a station to the Scanning server

1. Select the **Anti-virus Network** item (icon) in the main menu of the Control center.
2. In the anti-virus network tree select a station (or if the station is turned off) or group of stations (icon) to be connected to the Scanning server (icon). Stations connected to the Scanning server are depicted on the tree as nested items.
3. In the **Configuration** section select **Virtual agent**.
4. Select **Use Scanning server** and specify the address of the Scanning server in the **Scanning server address** field.

For one Virtual agent only one address of the Scanning server can be specified.

If you do not have to specify a particular address, use the default setting `udp://18008`, and the Scanning server will be detected automatically irrespective of whether it has an IPv4 or IPv6 address.

The address can be specified in one of the following formats:

- `tcp://<IP address>:<port>` (IPv4 and IPv6 addresses are allowed; IPv6 addresses must be specified in square brackets, e.g. `tcp://[fd15:4ba5:5a2b:1008:edc8:733e:1dd7:789c]:7777`);
- `udp://:<port>` (only the protocol and the port for Dr.Web Agents to search the Scanning server are specified in this format);
- `srv://service@<domain>` (the address and the port are defined by searching the SRV record of the `<domain>` DNS; if the domain is not specified, it will be taken from the

`search` or `domain` field in the DNS settings, depending on which of them is the last in the configuration file).

5. Click the **Save** button.

Permissions

The following permissions are available to users of Unix-like OS stations:

- run Scanning server,
- stop Scanning server,
- change Scanning server configuration.

By default, only the permission to run the Scanning server is granted.

The set of granted permissions can be changed by the administrator of the anti-virus network if necessary. For detailed information about permissions refer to the Permissions of Station Users section.

Additional settings

You can specify additional settings on the Scanning server as well on the UNIX stations connected to it in the `drweb.ini` configuration file (`[MeshD]` section). You can edit the `drweb.ini` file via the Control center (select **UNIX** → **Dr.Web Agent** → **Configuration** in the station settings menu).

The detailed description of these settings is given in the table below.

For stations running on Windows you can specify the Scanning server address only. All the other settings described in the table are not supported.

Parameter	Description
`LogLevel` *{logging level}*	The level of detail for logs. The parameter can have one of the following values: • `DEBUG`—the most detailed logging level. All messages and debug information are registered. • `INFO`—all messages are registered. • `NOTICE`—all error messages, warnings, and notifications are registered. • `WARNING`—all error messages and warnings are registered. • `ERROR`—only error messages are registered. **Default value**: `Notice`

Parameter	Description
`Log` *{logging method}*	Logging method. The parameter can have one of the following values: • `Stderr[:ShowTimestamp]`—messages are displayed in the `stderr` standard error stream. • `Auto`—messages for logging are sent to the Dr.Web ConfigD configuration daemon, which saves them to one location according to its configuration. • `Syslog[:`<*facility*>`]`—messages are transmitted to the `syslog` system logging service. • Additional option <*facility*> is used to specify a level at which `syslog` registers messages. The following values are possible: ▫ `DAEMON`—messages of daemons. ▫ `USER`—messages of user processes. ▫ `MAIL`—messages of mail programs. ▫ `LOCAL0`—messages of local processes 0. … ▫ `LOCAL7`—messages of local processes 7. ▫ <*path*>—messages are to be saved directly to the specified log. **Default value**: `Auto`
`IdleTimeLimit` *{time interval}*	Maximum idle time for the Scanning server/Virtual agent. When the specified time period expires, the Scanning server/Virtual agent shuts down. The parameter can be set both for the Scanning server and the Virtual agent. If the `None` value is set, the Virtual agent/Scanning server will operate eternally, the `SIGTERM` signal will not be sent to it in case of inactivity. Minimal—`10s`. **Default value:** `30s`
`DebugSsh` *{boolean}*	Indicates whether it is necessary to log SSH events on the station if `LogLevel` is set to `Debug`. **Default value**: `No`
`ListenAddress` *{<IP address>:<port>}*	The network socket (address and port) on which the Scanning server awaits the connections from client stations. The parameter can be specified for the Scanning server only.

Parameter	Description
	The parameter must be specified so that the Scanning server listens on IPv6 and detects Virtual agents via IPv6. IPv6 address must be specified in square brackets. If the value of this parameter is specified as an empty string, the Scanning server stops operating. To set the value of this parameter to ' ' (i.e. an empty string) you must **simultaneously have the permissions to change the configuration of the Scanning server and to stop it**
`DnsResolverConfPath` *{path}*	Path to the configuration file of the domain name resolution subsystem (DNS resolver). The parameter is specified for the Virtual agent in case an SRV record is used as the address of the Scanning server. **Default value:** `/etc/resolv.conf`
`DiscoveryResponderPort` *{port}*	The port on which the Scanning server responds to requests of the clients via the UDP protocol. **Default value:** `18008`
`EngineChannel` *{On | Off}*	Enable or disable an option that allows the server to provide Scanning Engine services. The parameter can be specified for the Scanning server only. **Default value:** `On` To set the value of this parameter to `Off`, you must **simultaneously have the permissions to change the configuration of the Scanning server and to stop it**
`EngineUplink` *{address}*	The address of the Scanning server (specified in the same format as via the Control center). The parameter can be specified for the Virtual agent only. **Default value:** *Not set*
`EngineDebugIpc` *{boolean}*	Log the scanning service debug information if `LogLevel` is set to `Debug`. **Default value:** `No`
`UrlChannel` *{On | Off}*	Enable or disable an option that allows the server to provide URL check services.

Parameter	Description
	Default values: `On` To set the value of this parameter to `Off`, you must **simultaneously have the permissions to change the configuration of the Scanning server and to stop it**
`UrlUplink` *{address}*	The address of a higher host used for checking URLs. The parameter can be specified for the Virtual agent only. **Default value:** *Not set*
`UrlDebugIpc` *{boolean}*	Log the URL check debug information if `LogLevel` is set to `Debug`. **Default value:** `No`

For more detailed information on configuring the Scanning server and Virtual agents, see the **Administrator Manuals** for Dr.Web for Unix products, the **Dr.Web MeshD** section.

9.2. Integration with Virtual Desktop Infrastructure

Dr.Web Enterprise Security Suite supports integration with virtual desktop infrastructure (VDI). This is useful when working with *thin clients* capable of running in terminal mode via the RDP protocol.

In this case, the anti-virus network is organized in the following way:

1. An anti-virus network administrator creates *a reference virtual workstation* with pre-installed software and Dr.Web Agent and connects it to Dr.Web Server.
2. Required virtual workstations are cloned from the created reference station.
3. After a specified period, the virtual workstations are removed. In future, they are created once again from the reference station, if necessary.

To prepare the anti-virus network for integration with VDI

1. Select the **Anti-virus Network** item in the main menu of the Control Center and create a new station, which will be the reference station.
2. Install Dr.Web Agent along with all necessary software on the station you created. Connect the station to Dr.Web Server.
3. Appoint a virtual machine the Scanning Server and install the necessary software on it. You can create several Scanning Servers in your anti-virus network if necessary.
4. In the setting of the stations specify that they should use the Scanning Server. Specify for the stations the address of the Scanning Server to connect to.

5. In the same section of the Control Center, create a new group that will contain all future virtual workstations.
6. Set up the virtual workstation registration procedure. To do that, proceed to the **Administration** → User hooks section. Add a new hook based on the **Newbie connects to Dr.Web Server** event. In the **Hook text** field, type in:

```
local args = ... -- args.id, args.address, args.station

if args.id == '<reference_station_id>' then

  return { "id", dwcore.get_uuid(), "pgroup", "<primary_group_id>" }

end
```

   Specify ID of the reference station you created at step 1 as <*reference_station_id*>. Specify ID of the group you created at step 5 as <*primary_group_id*>. This information is always available in the **Anti-virus Network** object properties.

During the cloning, each new virtual workstation will get an ID matching the ID of the reference station. According to the hook above, upon connecting to Dr.Web Server the station gets a newly generated UUID. After that, the station is registered in a primary group that has the specified ID.

When creating the hook, it is recommended that you check with the pre-built **Newbie connects to Dr.Web Server** hook template. Select **Examples of the hooks** → **Newbies** → **Newbie connects to Dr.Web Server** in the hook tree of the Control Center to see the details, including possible alternative parameters and returned values.

The described procedure is relevant only for situations when the reference station is disconnected from Dr.Web Server and removed from the anti-virus network before connecting the cloned stations.

If it is undesirable to delete the reference station from Dr.Web Server, add a custom procedure based on the **Station authorization in progress** event. This procedure should be configured so that all cloned stations that have the same ID as the reference station, but have different other parameters (name, MAC address) are set to the newbie status. A description of this procedure is given in the **Appendices**, M9. Stations.

Example:

```
local args = ... -- args.id, args.connected,
args.current_address, args.current_name, args.last_address,

-- args.last_time, args.last_server, args.new_name,
args.new_address

if args.id == '<reference_station_id>' and args.current_name ~=
args.new_name then

return "newbie"
```

Scheduled removal of inactive virtual workstations

To allocate the available licenses efficiently and prevent accumulation of information about removed virtual workstations in the database, make sure to set up a task to automatically remove any inactive workstations. The inactive workstations here should be understood as the stations that have not connected to Dr.Web Server within a specified period.

To create a task for automatic removal of inactive stations

1. In the Control Center, proceed to the **Administration** → **Dr.Web Server Task Scheduler** section.
2. Create a new task by clicking the **Create task** button on the toolbar.
3. On the **Action** tab, select **Execute script** in the drop down list. After that, either import from a separate file or type in the following Lua script to the field below:

```
local adminName = 'admin'
-- specify the group ID
local gid       = '<primary_group_id>'
-- set the inactivity period (in seconds)
local interval  = 86400


require('st-db-state')
require('core/datetime')
require('core/admins/admins')
local lastseen = Datetime.timeUnixstampToDBFormat(Datetime.nowTimestamp()
- interval)
local stations = {}
-- run the database query
local res, err1 = DBuilder()
    :select('id, lastseenat')
    :from('stations')
    :where('gid', gid)
    :where('lastseenat '..dwcore.base64_decode('PA=='), lastseen)
    :where('state !=', st_db_state.st_db_state_logged_in)
    :get()
if res and next(res) then
  for i = 1, #res do
    table.insert(stations, res[i][1])
  end
end
```

```
-- remove inactive workstations
local function delete_stations(ids)
  local admin, err    = Admin:initWithLogin(adminName)
  require 'core/admins/admins'
  require('core/stations/stations')
  local status, results_stations = Stations:delete(ids, admin)
  return ''
end
return delete_stations(stations)
```

For <*primary_group_id*> specify ID of the group you created at step 5 of preparation for integration with VDI.

The script above accesses the database, gets ID of the stations that have not connected to Dr.Web Server within the last 24 hours (86400 seconds) and removes such stations from the group that has the specified ID.

It is recommended that you update the reference workstation every time after any anti-virus component updates, which requires the operating system restart. After the update, make sure to check and change the reference workstation ID in the hook text, if necessary.

Chapter 10: Configuring Dr.Web Server

This chapter contains a description of the following features for managing operation parameters of the anti-virus network and Dr.Web Server:

- License Management—licensing parameters;
- Logging—view the operation log of Dr.Web Server, view detailed statistic data on the Dr.Web Server operation;
- Setting Dr.Web Server Configuration—configure the Dr.Web Server operation parameters;
- Setting Dr.Web Server Schedule—configure scheduled tasks to maintain Dr.Web Server;
- Setting the Web Server Configuration—configure web server operation parameters;
- User Hooks—enable and configure user hooks;
- Setting Notifications—configure the system of administrator notifications about anti-virus network events with different methods of notification delivering;
- Administration of Dr.Web Server Repository—configure repository to update all anti-virus network components from the GUS and further propagation of updates on stations;
- Database Management—direct maintenance of the Dr.Web Server database;
- Peculiarities of a Network with Several Dr.Web Servers—configure multiserver anti-virus network and the neighbor connections;
- Integration with Virtual Desktop Infrastructure—configure Dr.Web Server for integration with a virtual desktop infrastructure (VDI).

10.1. License Management

10.1.1. License Manager

Detailed information on principles and features of Dr.Web Enterprise Security Suite licensing is given in the Licensing section.

License Manager Interface

Dr.Web Security Control Center contains the License Manager component. This component is used to manage licensing of anti-virus network objects.

To open the License manager, select **Administration** item in the main menu of Dr.Web Security Control Center. In the opened window select the **License manager** item in the control menu.

Hierarchical List of Keys

The main pane of the License manager contains the keys tree—the hierarchical list nodes of which are license keys of stations, groups and policies for which license keys are assigned.

Toolbar contains the following control elements:

Option	Description	Dependence on objects in the keys tree
Add license key	Add a new license key record.	Option is always available. Functional features depend on whether the object is selected in the key tree or not (see Add a new license key).
Remove selected objects	Remove the connection between the key and the licensing object.	Option is available if a licensing object (station, group or policy) or a license key is selected in the tree.
Propagate the key to groups and stations	Replace of add selected key to a licensing object.	Option is available if a license key is selected in the tree.
Export key	Save the local copy of the license key file.	
Check for updates and replace license keys	Check for updates that are placed on GUS, for all keys. If updates are available, download the keys and perform the replacement (see Automatic License Renewal).	Option is always available. The action is for all license keys in the tree.
Propagate the key to neighbor Dr.Web Servers	Donate licenses from the selected key to neighbor Dr.Web Servers.	Option is available if a license key is selected in the tree.

Settings of tree view allows to change hierarchical tree view:

- The **Show the number of licenses** flag enables/disables displaying in the keys tree the total number of licenses provided by the license key files.
- To change the tree structure, use the following options:
  - The **Keys** option prescribes to display all license keys of anti-virus network as a root nodes of the hierarchical tree. At this, all groups, stations and policies for which these keys are assigned, are presented as child elements of license keys. This tree view is a general view and allows to manage licensing objects ans license keys.
  - The **Groups** option prescribes to display those groups, to which the keys are personally assigned as a root nodes of the hierarchical tree. At this, stations and policies included in these groups and license keys that are assigned to these groups are presented as child

elements of groups. This tree view is intended for visualization convenience of information on licensing and does not allow to manage objects of the tree.

- To change the tree appearance, use the following options:
  - **Show clients identifiers**—enables/disables showing of stations unique identifiers.
  - **Show clients names**—enables/disables showing of stations names.
  - **Show clients addresses**—enables/disables showing of stations IP-addresses.
  - **Show descriptions**—enables/disables showing of stations and groups of stations descriptions.

Licenses Handling

Via the License Manager, you can perform the following actions under license keys:

1. View Information About a License.
2. Add a New License Key.
3. Update the License Key.
4. Replace the License Key.
5. Extend the List of Object License Keys.
6. Remove the License Key and the Object from the Licensing List.
7. Donate a License to a neighbor Dr.Web Server.
8. Edit Licenses Donated to a Neighbor Dr.Web Server.

View Information About a License

To view the summaries about a license key, in the main pane of the License manager, select the key record to view the detail information (click the key record name). In the opened pane you can view the following information:

- Provided and used number of licenses from this license key file.
- The owner of the license.
- The dealer, who sold the license.
- Identification and serial numbers of the license.
- License expiration date.
- Inclusion of the Anti-spam component.
- MD5 hash of the license key.
- Allowed lists of hash bulletins for notification about identity of detected threats. If the feature is not licensed, this parameter is absent.

Anti-virus protection level is not reduces if hash bulletins are not licensed. This license allows to notify the administrator that the detected threat is in the specialized bulletins of known hashes of threats.

- The list of anti-virus components which are allowed to use by this license.

Add a New License Key

To add a new license key

1. In the main pane of the License Manager, click **Add license key** on the toolbar.
2. On the opened panel, click and select the license key file.
3. Set the flag:
   - **Replace the license key of the Everyone group** if it is the first license key of the anti-virus network. The adding key will be assigned to the **Everyone** group automatically.
   - **Assign the license key to the Everyone group** if it is not the first license key of the anti-virus network. The current license key of the **Everyone** group will be replaced with the adding license key.

   If several keys are assigned to the **Everyone** group, the first key in the list will be replaced.

   If you want to replace specific license key of the **Everyone** group, use the Update the License Key procedure.
4. Click **Save**.
5. The license key will be added to the keys tree.

   If you did not set the corresponding flag at step 3, then added license key will not be assigned neither to one of the objects. In this case, to specify licensing objects, perform the Change the License Key or Extend the List of Object License Keys procedures described below.

Update the License Key

When updating a license key, the new license key is assigned to the same licensing objects to which the old one was assigned.

Use the key update procedure to replace an expired key or to replace a key with another one containing a different set of installable components. The key tree structure is preserved.

To update a license key

1. In the main pane of the License Manager in the keys tree, select the key you want to update.
2. On the opened key properties panel, click and select the license key file.

3. Click **Save**. A window with installed components settings described in Settings for License Key Changing, opens.
4. Click **Save** to update the license key.

Replace the License Key

When changing a license key, all current license keys are deleted for the licensing object and a new key is added.

To replace the current license key

1. In the main pane of the License Manager in the keys tree, select the key you want to assign to the licensing object: group of stations, station or policy.
2. Click **Propagate the key to groups and stations** on the toolbar. A window with hierarchical list of anti-virus network opens.
3. Select licensing object from the list. To select several objects, use CTRL and SHIFT.

> To assign a key to a policy, you must select the policy itself or the current version of this policy (a key is assigned automatically to a policy when selecting its current version and vice versa).
>
> A license key can be also assigned to any version of a policy which is not current. At this, a key is assigned only to this version, but not to the policy itself. Such key is not applied to stations until a current version of a policy will not be replaced with the one to which this key is assigned.
>
> A license key must be assigned to policies and their versions directly.

4. Click **Replace license key**. A window with installed components settings described in Settings for License Key Changing, opens.
5. Click **Save** to replace the license key.

Extend the List of Object License Keys

When adding a license key, the licensing object saves all current keys, and a new license key is added to the keys list.

To add a license key to the license keys list of an object

1. In the main pane of the License Manager in the keys tree, select the key you want to add to the objects keys list: group of stations, station or policy.
2. Click **Propagate the key to groups and stations** on the toolbar. A window with hierarchical list of anti-virus network opens.
3. Select licensing object from the list. To select several objects, use CTRL and SHIFT.

To assign a key to a policy, you must select the policy itself or the current version of this policy (a key is assigned automatically to a policy when selecting its current version and vice versa).

A license key can be also assigned to any version of a policy which is not current. At this, a key is assigned only to this version, but not to the policy itself. Such key is not applied to stations until a current version of a policy will not be replaced with the one to which this key is assigned.

A license key must be assigned to policies and their versions directly.

4. Click **Add license key**. A window with installed components settings described in Settings for Adding a License Key to the Keys List, opens.
5. Click **Save** to add the license key.

Remove the License Key and the Object from the Licensing List

You cannot remove the last license key record of the **Everyone** group.

For policies that are assigned to stations with no personal settings of a license key, a license key must be specified.

To remove the license key or the object from the licensing list

1. In the main pane of the License Manager in the keys tree, select the key you want to remove, or the object (station, group or policy), to which this key is assigned, and click **Remove selected objects** on the toolbar. At this:
   - If a group or station was selected, it will be removed from the list of objects on which its key is effects. Group or station for which a personal license key is removed, inherits a license key.
   - If a policy was selected, its current version is also removed from the list of objects on which a license key is assigned. If a current version of a policy was selected, the policy itself is removed as well. But when removing a policy version that is not current, a policy itself and its current version will not be removed.
   - If a license key was selected, this key record is removed from the anti-virus network. All groups and stations to which this license key was assigned, inherit a license key.
2. A window with installed components settings described in Settings for License Key Changing, opens.
3. Click **Save** to remove selected object.

Donate a License to a Neighbor Dr.Web Server

When donating a part of vacant licenses to a neighbor Dr.Web Server from the license key of this Dr.Web Server, number of donated licenses will not be available for use on this Dr.Web Server till the end of propagation time of these licenses.

To donate licenses to a neighbor Dr.Web Server

1. In the main pane of the License Manager in the keys tree, select the key a vacant licenses from which you want to donate to neighbor Dr.Web Server.
2. Click **Propagate the key to neighbor Dr.Web Servers** on the toolbar. A window with hierarchical tree of neighbor Dr.Web Servers opens.
3. Select from the list those Dr.Web Servers to which you want propagate licenses.
4. Specify the following parameters next to the each Dr.Web Server:
   - **Number of licenses**—number of vacant licenses, you want to donate from this key to a neighbor Dr.Web Server.
   - **License expiration date**—validity period of licenses donation. After specified time period, all licenses will be recall from the neighbor Dr.Web Server and got back to the list of vacant licenses in this license key.
5. Click one of the buttons:
   - **Add license key**—to add licenses to the list of presence licenses of neighbor Dr.Web Servers. A window with installed components settings described in Settings for Adding a License Key to the Keys List, opens.
   - **Replace license key**—to remove current licenses of neighbor Dr.Web Servers and set only propagated licenses. A window with installed components settings described in Settings for License Key Changing, opens.

Icons of elements in the hierarchical list

Icon	Description
	Dr.Web Server is started.
	Dr.Web Server is stopped.
	Sent key.
	Received key.

Edit Licenses Donated to a Neighbor Dr.Web Server

To edit licenses propagated to neighbor Dr.Web Server

1. In the main pane of the License Manager in the keys tree, select the neighbor Dr.Web Server, on which licenses were propagated.
2. On the opened properties panel, edit the following parameters:
   - **Number of licenses**—number of vacant licenses, which were donated from the key of this Dr.Web Server to the neighbor Dr.Web Server.
   - **License expiration date**—validity period of licenses donation. After specified time period, all licenses will be recall from the neighbor Dr.Web Server and got back to the list of vacant licenses in this license key.
3. Click **Save** to update information on propagated licenses.

Changing the List of Installable Components

Settings for License Key Changing

This section describes how to specify installable components for the following procedures:

- Update the License Key.
- Replace the License Key.
- Remove the License Key.
- Donate a License to a neighbor Dr.Web Server and replace the License Key.

To specify installable components when performing these procedures

1. In the window with the installable component settings, the following objects are listed:
   - Stations, groups and policies with their lists of installable components.
   - In the **Current key** column, you can find the list of object keys and the settings of installable components that are currently specified for the object.
   - In the **Assigning key** column, you can find the key and the settings of installable components that are specified in the key you want to assign to the selected objects.
   - If necessary, set the **Show only different** flag to list only those component settings that differ between the current key and the key to be assigned.
2. To configure the list of installable components:
   a) In the **Assigning key** column, you can configure the resulting list of installable components.
      - Installable component settings in the **Assigning key** column are calculated based on whether the component use is allowed (+) or not allowed (-) in the current settings and in the new key, as follows:

Current settings	Assigning key settings	Result settings
+	+	+
–	+	+
+	–	–
–	–	–

- You can change installable component settings (downgrade the permission to install) only if the settings of the **Assigning key** allow to use this component.

b) Set the flags for those objects (stations, groups and policies) for which settings will not be inherited and the installable component settings from the **Assigning key** column will be set as their personal settings. For other objects (for which flags are not set), initial settings from the **Assigning key** column are inherited.

Settings for Adding a License Key to the Key List

This section describes how to specify installable components for the following procedures:

- Extend the List of Object License Keys.
- Donate a License to a Neighbor Dr.Web Server and add a License Key.

To specify installable components when performing these procedures

1. In the window with the installable component settings, the following objects are listed:
   - Stations, groups and policies with their lists of installable components.
   - In the **Current key** column, you can find the list of object keys the and settings of installable components that are currently specified for the object.
   - In the **Assigning key** column, you can find the key and the settings of installable components that are specified in the key you want to add to the selected objects.
2. If necessary, set the **Show only different** flag to list only those component settings that differ between the current key and the key to be assigned. Note that in the **Assigning key** section not the assigning key settings are listed, but the resulting settings of installable components.
3. To configure the list of installable components:
   a) In the **Assigning key** column, you can configure the resulting list of installable components.
      - Installable component settings in the **Assigning key** column are calculated based on whether the component use is allowed (+) or not allowed (-) in the current settings and in the new key, as follows:

Current settings	Assigning key settings	Result settings
+	+	+
–	+	–
+	–	–
–	–	–

- You can change installable component settings (downgrade the permission to install) only if the settings of the **Assigning key** allow to use this component.

b) Set the flags for those objects (stations, groups and policies) for which settings will not be inherited and the installable component settings from the **Assigning key** column will be set as their personal settings. For other objects (for which flags are not set), initial settings from the **Assigning key** column are inherited.

10.1.2. License Usage Report

License usage report contains information on all licenses used by both this Dr.Web Server and neighbor Dr.Web Servers, including licenses that were donated using interserver connection.

Reports are created (and are sent for neighbor Dr.Web Servers) according to the settings specified in **Dr.Web Server configuration** → **Licenses**, the **Options for the report on license usage** section.

To view the report, select **Administration** item in the main menu of Dr.Web Security Control Center. In the opened window select the **License usage report** item in the control menu.

This section contains the following data:

- Report on all licenses managed by this Dr.Web Server. The report is given even if none of neighbor Dr.Web Servers are configured to be connected to this Dr.Web Server.
- Report on licenses managed by neighbor Dr.Web Servers reporting to this Dr.Web Server, including those that receive licenses from it using an interserver connection. At this, reports from all neighbor Dr.Web Servers in an interserver connections tree, are given.

Each report is displayed as a separate table and contains information only on licenses of one Dr.Web Server—the report creator.

The following information is given in the table header:

- **Dr.Web Server**—name of Dr.Web Server—the report creator.
- **Total licenses received from neighbors**—total number of licenses that Dr.Web Server received via interserver connection.

The report table contains the following data:

- **User**—the user of the license key, information on licenses of which is given in the report row.
- **Total licenses**—total number of licenses provided from this license key on this Dr.Web Server.
- **Available**—number of available, not used licenses in this key.
- **Total used**—total number of licenses that have been used (assigned to stations or neighbor Dr.Web Servers) at the time of the report creation.
- **Used by stations**—number of licenses that are used by stations connected to Dr.Web Server—the report creator.
- **Pending**—number of licenses that the report creator expects to receive. Particularly, if Dr.Web Server that used some licenses (either assigned to its stations, or donated via interserver connections), lost part of these licenses. For example, a license key was replaced with a key with fewer licenses or the number of licenses received from the parent Dr.Web Server was reduced.
- **Reserved**—number of licenses that were donated via interserver connections, but a recipient has not yet received assigned licenses: neighbor Dr.Web Servers have not yet connected to get licenses. These licenses are reserved from a license key and cannot be given to other stations or Dr.Web Servers.
- **Donated to neighbors**—number of licenses that Dr.Web Server—report creator donated via the interserver connections to its neighbor Dr.Web Servers.
- **Received from neighbors**—number of licenses that Dr.Web Server—report creator received via the interserver connections from its neighbor Dr.Web Servers.
- **Report date**—date of the report creation.

For licenses that are used by stations of Dr.Web Server—report creator, the additional information is available. To view the information, click the number of licenses in the **Used by stations** column (the number of licenses must be not null). In the **Use of licenses by groups** opened table, the following information is provided:

- **Group name**—the name of the station group to which the licenses were propagated.
- **Propagated licenses**—total number of licenses propagated to the station group.
- **Active stations**—number of active stations in the groups. Active means stations that were online during the time period specified in the settings for the report generated on Dr.Web Server—the license key owner.

10.2. Logging

10.2.1. Real Time Log

Real time log allows to view the list of events and changes related with the Dr.Web Server operation that are displayed at the moment of an event appearance.

Real time log displays information in the Control Center only and does not write events into a file. Dr.Web Server log file is kept separately with its own settings and does not depend on the real time log and its settings.

When you leave this section, all information displayed in the real time log, is deleted.

The log table contains the following data:

- **No.**—sequence number of an entry. The number is assigned in a sequence matching the order in which messages are coming from Dr.Web Server.
- **Time in log format**—event appearance time represented in Dr.Web Server log file. It can be used for searching the event in the Dr.Web Server log file.
- **Time**—event appearance time represented in human readable form.
- **Level**—log level according to which an event appeared.
- **PID**—process identifier within which an event occurred.
- **TID**—thread identifier within which an event occurred.
- **Thread**—thread name within which an event occurred.
- **Subsystem**—subsystem name within which an event occurred.
- **Message**—message text about an event occurred. Click a message in the table to open the window with the full message text. If the texts is an HTML code, set the **Format as HTML** flag to display information properly. Please note, if the text contains JavaScript, it will be executed.

To edit the data view in the table

- Using the icon:
  - Specify rows display settings (most relevant for long strings).
  - Select the columns to display in the table.
- Using the icon:
  - Specify the arbitrary string to search by all sections of the table. The table will contain only rows that correspond to the search results.
  - To display only specific levels, set the flags next to the necessary levels.
  - To display only specific subsystems, set the flags next to the necessary subsystems.

  To write messages to the log only with specific levels and from specific subsystems, specify the log settings.

The toolbar contains the following options to manage the log:

Set up data display—open the log settings window.

Clear the table—delete all the data shown in the table. You cannot undone this operation.

Stop data collection—stop displaying information on events in the table. The button is active when the data is collecting. On click, changes to **Start data collection**.

Start data collection—start displaying information on events in the table. The button is active when the data is not collecting. On click, changes to **Stop data collection**.

Configuring Real Time Log

1. On the toolbar, click **Set up data display**. The **Data display settings** window opens.
2. The **Maximum number of records** field sets the limitation on the number of records displayed in the log table. When the specified number is reached, old records are deleted when new ones are received.
3. The **Refresh rate, sec.** field defines the rate in seconds according to which new records will be displayed in the log.
4. The **Subsystem search** field allows to search by subsystem name given below. It can be used if you want to specify the log level of detail for specific subsystem in the case of a large number of subsystems in the list.
5. Subsystems table allows to configure the list of displayed data and their detail level:
   a) Set the flags next to the subsystems whose messages will be displayed in the table.
   b) For the selected subsystems, select the log level of detail.
   c) To show all subsystems, set the flag in the table header.
   d) To set the same log level of detail for all subsystems, select the value in the drop-down list next to the **all** subsystem. At this, the table will display only messages for subsystems with the set flags.
6. Click **Apply** to start displaying data according to the specified settings.
7. Click **Close** to close the window without saving changes in the log display settings.

10.2.2. Audit Log

Audit log allows to view the list of events and changes carried via the control subsystems of Dr.Web Enterprise Security Suite.

To view the audit log

1. Select the **Administrating** item in the main menu of the Control Center.
2. In the opened window, select the **Audit log** item of the control menu.
3. Window with the registered actions table opens. To configure viewing the log, specify on the toolbar the time period during which the actions have been performed. For this, you can select one of the proposed periods or specify arbitrary dates in the calendars which are opened on clicking the dates fields. Click **Refresh** to display the log for the selected dates.
4. To configure the table view, click the icon in the right corner of the table header. In the drop-down list, you can configure the following options:
   - Enable or disable line wrapping for long messages.

- Select the columns to display in the table (selected by the flag next to its name). To show/hide the column, click the line with its name.
- Select the order of the columns in the table. To change the order, drag and drop corresponding column in the list to the needed place.

5. The log table contains the following data:
   - **Time**—date and time when the action has been performed.
   - **State**—the brief result of the action performing:
     - **OK**—operation successfully executed.
     - **failed**—an error occurred during the operation execution. Operation is not executed.
     - **initiated**—operation execution is initiated. The result of operation execution will be known just after its completion.
     - **no rights**—administrator that launched the operation execution has no permissions to execute this operation.
     - **delayed**—action execution is postponed until a certain period or performing of a certain event.
     - **not allowed**—execution of the requested action is prohibited. For example, deleting of system groups.

Lines that correspond to actions executed with an error (the **failed** value in the **Result** column), are marked with red.

   - **Message / Error**—detailed description of the action or error occurred.
   - **Login**—login of the Dr.Web Server administrator. It is specified if the action was initiated directly by administrator or during connection to Dr.Web Server according to the administrator credentials.
   - **Address**—IP address from which the action execution has been initiated. It is specified only in case of an external connection to Dr.Web Server, particularly via the Control Center or via the Web API.
   - **Subsystem**—the name of the subsystem by which or via which the action has been initiated. The audit is logged for the following subsystems:
     - **Control Center**—the action was performed via Dr.Web Security Control Center, particularly by administrator.
     - **Web API**—the action was performed via the *Web API*, e.g., from an external software connected according to the administrator credentials (see also the **Appendices** document, Appendix K. Integration of Web API and Dr.Web Enterprise Security Suite).
     - **Server**—the action was performed by Dr.Web Server, e.g., according to its schedule.
     - **Utilities**—the action is initiated via the external utilities, particularly via Dr.Web Server remote diagnostics utility.

6. If necessary, you can export data for the specified period into a file. To do this, click on the following buttons on the toolbar:

Save data in CSV file,

Save data in HTML file,

Save data in XML file,

Save data in PDF file.

10.2.3. Dr.Web Server Log

Dr.Web Server logs the events connected with its operation.

The Dr.Web Server log is used for debugging and troubleshooting in case of any abnormalities in the anti-virus network.

By default, the log file name is `drwcsd.log` and it is located:

- On **UNIX** OS:
  - Linux OS: `/var/opt/drwcs/log/drwcsd.log`;
  - FreeBSD OS: `/var/drwcs/log/drwcsd.log`.
- On **Windows** OS: in the `var` subfolder of the Dr.Web Server installation folder.

The file has the plain text format (see the **Appendices** document, Appendix J. Log Files Format).

To view the Dr.Web Server log via the Control Center

1. Select the **Administration** item in the Control Center main menu.
2. In the opened window, select the **Dr.Web Server log** item of the control menu.
3. A window with a list of the Dr.Web Server logs will open. Based on the rotation mode settings, the following naming format is used for the Dr.Web Server log files: <*file_name*>.<*N*>.`log` or <*file_name*>.<*N*>.`log.gz`, where <*N*>—sequence number: 1, 2, etc. Therefore, if a log file name is `drwcsd`, the list of log files is the following:
   - `drwcsd.log`—current log file,
   - `drwcsd.1.log`—previous log file,
   - `drwcsd.2.log` and so on—the greater the number, the older the version of the log.
4. To manage the log files, set the flag next to a necessary file or files. To select all log files, set the flag in the table header. As a result, the following buttons will become available on the toolbar:

   Export selected log files—save a local copy of the selected log files. It can be useful, for example, to view the log file content from a remote computer.

   Delete selected log files—delete the selected log files, without possibility to restore.

   To change the Dr.Web Server logging mode via the Control Center, use the Log section.

Managing the Dr.Web Server log level of detail

Depending on specified settings, the Dr.Web Server log is filled with different level of detail. Enabling a more detailed logging for a specific message source or for all sources can be useful for debugging and troubleshooting and can also be necessary when contacting the Doctor Web technical support. There are multiple ways to configure this parameter:

- From the **Administration** → **Dr.Web Server configuration** → **Log** section in the Control Center. This way allows to specify the logging level of detail for all possible sources.
- Using the `-verbosity` switch when launching Dr.Web Server from the command line. This way provides more flexibility, since it allows to set up the logging level of detail for a single or several different sources. The switch format is described in the **Appendices** document, G3.8. The Description of Switches.
- From a separate configuration file named `logging.conf`. To do that, create a file with this name in the `etc` subfolder inside the Dr.Web Server installation folder. Add all necessary message sources and their desired levels of detail in the following format: <*message_source*>:<*level*>. The `-verbosity=all:all` switch is equal to the `-verbosity=all` switch. The levels of detail specified for message sources in the `logging.conf` override any levels configured for the same sources in any other way.

  Example of the `logging.conf` content:

  ```
  Alert:all, Server:err, SqLite3:inf
  ```

  Besides the comma, you can also use any whitespace characters, like a normal space, tab, newline, etc. as the separators. You can check the list of available message sources in the Dr.Web Server log file directly or by running the following command in the **Administration** → **Lua console** section of the Control Center: `drwcs.log_subsystems()`. All possible levels of detail are listed in the **Appendices** document, in Appendix J. Log Files Format.

  The levels of detail configured this way are inherited by subsystems. In other words, for instance, when you specify `Socket/Client:inf` and `Socket:all` at the same time, the `Socket/Client` will follow the direction of its parent and thus will log information about all events, not only the information messages.

- For Dr.Web Servers running a Unix-like OS, you can use a designated switch in the configuration file named `local.conf`. Please see below for information about this file.

Logging Setup for UNIX

It is possible to set up the logging on Dr.Web Servers running a Unix-like OS via a separate configuration file:

- for Linux OS: `/var/opt/drwcs/etc/local.conf`;
- for FreeBSD OS: `/var/drwcs/etc/local.conf`.

The `local.conf` file content:

```
# Log level.

DRWCS_LEV=info

# Log rotation.

DRWCS_ROT=10z,10m
```

Parameter values correspond with the values of command line switches for the Dr.Web Server launch:

- `-verbosity=<detail_level>`—level of detail of the Dr.Web Server log.
- `-rotate=<N><f>,<M><u>`—rotation mode of the Dr.Web Server log.

The switches are described in detail in the **Appendices** document, G3.8. The Description of Switches.

> If the `local.conf` file is edited when Dr.Web Server is running, you must reboot Dr.Web Server for new logging settings to come into effect. The reboot must be performed by means of the operating system.

During the Dr.Web Server update or removal, the `local.conf` file is backed up. That allows to manage the log level of detail in case of a package update of Dr.Web Server.

10.2.4. Repository Updates Log

Repository updates log allows to view the list of updates from GUS, that includes detailed information on updated products revisions.

To view the repository updates log

1. Select the **Administrating** item in the main menu of the Control Center.
2. In the opened window, select the **Log of repository updates** item of the control menu.
3. Window with the registered actions table opens. To configure viewing the log, specify on the toolbar the time period during which the actions have been performed. For this, you can select one of the proposed periods or specify arbitrary dates in the calendars which are opened on clicking the dates fields. Click **Refresh** to display the log for the selected dates.
4. To show only events of specific types in the table, click on the toolbar. In the drop-down list, you can select the necessary filtering options:
   - **Product name**—log table displays events related to the products you selected from the list.
   - **Update result**—log table displays the update sessions and their results. You can filter sessions by the following results:

- **Requested product not found on GUS servers**;
- **License key is not found on GUS servers**;
- **Update disabled**;
- **Update completed successfully**.

- **Initiator**—log table displays the update sessions initiated by the following systems:
  - **Launched from the command line**—update was initiated by administrator via the corresponding console command.
  - **Launched by Task Scheduler**—update wad launched according to the task in the Dr.Web Server schedule.
  - **Interserver update**—update was received via the interserver connection from the main Dr.Web Server. This initiator presents only in case of multiserver configuration of anti-virus network with propagation of update via the interserver connections.
  - **Launched from the Control Center**—update was launched by administrator via Dr.Web Security Control Center, from the Repository State section.
  - **Repository import**—update was loaded by administrator in the Repository Content section of the Control Center.

5. The log table contains the following data:
   - **Administrator**—registration name of the Dr.Web Server administrator. The name is displayed in the table if the action was initiated by the administrator.
   - **Network address**—IP address from which the action execution has been initiated. It is specified only in case of an external connection to Dr.Web Server, particularly via the Control Center or via the Web API.
   - **Initiator**—system that initiated the update process.
   - **Repository folder**—folder name of the Dr.Web Server repository that was modified according to the update process.
   - **Product name**—name of the repository product that was downloaded or was requested to be downloaded.
   - **Start**—date and time when an update of the certain product has been started from the GUS.
   - **Finish**—date and time when an update of the certain product has been finished from the GUS.
   - **Update result**—repository update result. Contains brief information on successful update completion or error reason.

     The **Update result** cells that correspond to actions executed with an error, are marked with red.

   - **Initial revision**—number of the revision (revisions are numbered according to the date of their creation) that was the last for this product before update process started.

- **Received revision**—number of the revision (revisions are numbered according to the date of their creation) that was downloaded during update process.
- **Updated files**—brief information on the changed files. Is given in the following format: *<files number> – <actions on files>*.

6. If necessary, you can export data for the specified period into a file. To do this, click on the following buttons on the toolbar:

   Save data in CSV file,

   Save data in HTML file,

   Save data in XML file,

   Save data in PDF file.

10.2.5. Message Log

The message log displays all text messages that were sent by administrator to stations of the anti-virus network (see Sending Notifications to Stations).

The log of the sent messages contains the following information:

- **Sent date**.
- **Sender**—login name of the administrator authorized in the Control Center when the message was sent.
- **State**—the number of messages sent by administrator and the number of messages successfully delivered to stations. If the numbers of sent and delivered massages are the same, information on these messages is marked with gray.
- **Message**—the text of the sent message. Optionally contains the information about the rest settings that were specified during sending.

Mouse click on the specific message in the table opens the window with delivering details: the list of all receivers and the date of the message delivery in case of successful operation and **Not delivered** in case of fail.

To manage the message log, use the following toolbar options:

Resend selected messages—option is available if one or several sent messages are selected in the log (see procedures below).

Save selected messages as a template—create a template from the sent message to reuse it in the future. The option is available when only one message is selected in the log. You can manage the saved templates in the Message Templates section.

In the drop-down list, select the period during which the messages that you want to display have been sent. The same period you can select in the fields with dates that are specified in the drop-down calendar. To apply the selected period, click **Refresh**.

To resend a single message

1. Set the flag next to the message you want to send.
2. Click **Resend selected messages**.
3. The **Sending a message** window opens. Specify the following settings:
   a) In the **Anti-virus network** tree, the stations to which this message was sent are selected. You can remain the previous receivers or select arbitrary receivers from the given list—whether separate stations or groups of stations.
   b) The message settings are the same as in the Sending Notifications to Stations section.
4. Click **Send**.

To resend multiple messages

1. Set the flag next to the messages you want to send.
2. Click **Resend selected messages**.
3. The **Sending multiple messages** window opens. The **List of messages** section contains the list of all message you have select for resending. The names of the messages correspond to the dates of their previous sending to stations.
4. Click **Send all**, to send all messages from the list.
5. To edit a message from the list, select it in the **List of messages** section. In the **Message settings** section, specify the following parameters:
   a) In the **Anti-virus network** tree, the stations to which this message was sent are selected. You can remain the previous receivers or select arbitrary receivers from the given list—whether separate stations or groups of stations.
   b) The message settings are the same as in the Sending Notifications to Stations section.
   c) To remove the selected message from the sending list, click **Remove**.

10.3. Setting Dr.Web Server Configuration

After each saving of changes in the **Dr.Web Server configuration** section, the backup copy of the previous version of the Dr.Web Server configuration file is saved automatically. Only 10 last copies are stored.

Files are placed in the same folder as the configuration file itself and named according to the following format:

`drwcsd.conf_<creation_time>`

You can use created backup copies particularly to restore the configuration file if the Control Center interface is not available.

To set the configuration parameters of Dr.Web Server

1. Select the **Administration** item in the main menu of the Control Center.
2. Select **Dr.Web Server configuration** in the control menu. A window with the Dr.Web Server configuration will be opened.

   Values of fields, marked with the * sign, must be obligatory specified.

3. On the toolbar, the following buttons to manage the section settings are available:

   Restart Dr.Web Server—restart Dr.Web Server to apply changes that have been specified in this section. The button become enabled after you specified the changes in the section settings ans click **Save**.

   Restore configuration from the backup—drop-down list with the backup of all section settings, which you can restore after making changes. The button become enabled after you specified the changes in the section settings ans click **Save**.

   Reset all parameters to initial values—restore the values that all parameters in this section had before current editing (last saved values).

   Reset all parameters to default values—restore default values of all parameters in this section.

4. To apply the changes specified in the section settings, click **Save**, after this Dr.Web Server must be rebooted. To do this, click **Restart Dr.Web Server** on the toolbar of this section.

10.3.1. General

On the **General** tab, you can configure the following Dr.Web Server parameters:

- **Server name**—the name of Dr.Web Server. If it is not specified, the name of the computer where Dr.Web Server software is installed is used.
- **Server language**—default language which is used by components and systems of Dr.Web Servers if failed to get language settings from the Dr.Web Server database. Particularly used by Dr.Web Security Control Center and administrator notification system if the database has been corrupted and the language settings cannot be obtained.

  If you select an interface language whose texts are not currently being updated, you will be prompted to enable the update for this language. To do this, follow the link to the **Administration → General repository configuration → Dr.Web Server → Dr.Web Security Control Center languages** section, set the flag for the necessary language and click **Save**. At the next repository update, the interface texts for the selected language will be updated. Also you can launch the update manually in the **Repository state** section.

- **Number of parallel requests from clients**—the number of threads processing data from clients: Dr.Web Agents, Dr.Web Agent installers, neighbor Dr.Web Servers, Dr.Web Proxy Servers. This parameter affects the performance of Dr.Web Server. Do not change the default

value when using the embedded database. The use of an external database may require a higher value (see **Appendices**, Dr.Web Server Load and Recommended Configuration Parameters). When working in an anti-virus network with a large number of client connections to Dr.Web Server, it is recommended that you consult with the Doctor Web technical support team before changing the value of the parameter.

Starting from version 10, the **Authorization queue** parameter cannot be edited via the Control Center.

On the new Dr.Web Server installation, this parameter takes the 50 default value. On the upgrade from the previous version saving configuration file, the authorization queue value is saved from the previous version configuration.

If you need to edit the authorization queue value, edit the following parameter value in the Dr.Web Server configuration file:

```
<!-- Maximum authorization queue length -->
<maximum-authorization-queue size='50'/>
```

- In the **Newbies registration mode** drop-down list, select the registration mode for new stations (see New Stations Approval Policy).
  - In the **Default primary group** drop-down list select the group which is set as a primary when access of stations to Dr.Web Server is allowed automatically.
- Set the **Reset unauthorized to newbie** flag to reset parameters to access Dr.Web Server for workstations which have not passed authorization check. This option can be helpful when you change the Dr.Web Server settings (such as public key) or change the DB. In such cases workstations will not be able to connect to Dr.Web Server and will need to get the new parameters to assess Dr.Web Server.
- Set the **Create station accounts automatically** flag to automatically create missing station accounts in the Control Center when installing Dr.Web Agents via the group installation package. If the flag is cleared, installation is possible only according to already created accounts in the group, installation package for stations of which is launched.
- In the **Allowed difference between time of Dr.Web Server and Agent** field specify allowed difference between system time at Dr.Web Server and Dr.Web Agents in minutes. If the difference is larger than specified value, it will be noted in the status of the station at Dr.Web Server. 3 minutes are allowed by default. The 0 value means that checking is disabled.
- Set the **Replace IP addresses** flag to replace IP addresses with DNS names of computers in the fields with workstation addresses in the Control Center.
- In the **Station name** drop-down list, you can select the format of workstation names. This setting defines the station name format in which Dr.Web Server expects to receive the names from Dr.Web Agents, as well as the format in which the station names are subsequently displayed in the Control Center directory of the anti-virus network. This setting is ignored if any option other than **No** is selected in the **Replace station name** setting.
- In the **Replace station name** drop-down list, you can specify whether to replace the displayed workstation names with their fully or partially qualified DNS names (if DNS names

cannot be detected, IP addresses are displayed). If **No** is selected, the **Station name** setting is applied. If any value other than **No** is selected, Dr.Web Server ignores the name received from Dr.Web Agent (the **Station name** setting is ignored) and determines the name of the station with Dr.Web Agent installed on its own using DNS.

By default, the **Replace IP addresses** flag is cleared and station names are not replaced. If the DNS service is not set up properly, enabling these options can considerably slow down the Dr.Web Server operation. When using any of these options, it is recommended that name caching on the DNS server is enabled.

If a replacement option is selected in the **Replace station name** drop-down list and a Dr.Web Proxy Server is used in the anti-virus network, then all stations connected to Dr.Web Server via Dr.Web Proxy Server display the name of the computer with Dr.Web Proxy Server installed instead of their own names.

- Set the **Synchronize stations descriptions** flag to synchronize descriptions on stations (**Computer description** field on the **System properties** page in Windows OS) with station descriptions in Dr.Web Security Control Center. If no description is given to a station in Dr.Web Security Control Center, the field will be filled in with the description from the user computer. If the descriptions differ, the description in Dr.Web Security Control Center will be replaced by the description from the user computer.
- Set the **Synchronize geolocation** flag to enable synchronization of stations geolocation between Dr.Web Servers in multiserver anti-virus network. If the flag is set, you can configure the following parameter:
  - **Startup synchronization**—number of stations without geographical coordinates, information on which is requested when establishing a connection between Dr.Web Servers.
- Set the **Use policies** flag to allow using policies for configuring settings of protected stations (see Policies).
  - **Policy versions number**—number of versions that can be created for each policy, in addition to the current version.
- In the **Number of backups for the Dr.Web Server versions** field, set the maximum number of stored backups created at update to a new revision of Dr.Web Server via the Control Center (see Updating Dr.Web Server and Restoring it from Backup). The 0 value prescribes to store all backups.
- Set the **Use the Agent protocol extension to transfer file data** flag, to allow the file data transfer from Dr.Web Agent to Dr.Web Server via SFTP protocol. If the flag is cleared, no data transfer is performed.
- In the **Number of Lua virtual machines** field, set the maximum number of preloaded Lua virtual machines for Dr.Web Server needs.
- In the **Script for loading Lua virtual machine** field, insert a script to execute during a background creation of Lua virtual machine for Dr.Web Server needs.

10.3.2. Traffic

10.3.2.1. Updates

On the **Updates** tab, you can configure limits for the network traffic bandwidth for transmitting updates from Dr.Web Server to Dr.Web Agents.

For more details see Workstation Traffic Limitations.

To set limits on Dr.Web Agents update traffic

1. In the **Number of simultaneous update processes** field, you can specify maximum allowable number of updates distribution sessions running at the same time from this Dr.Web Server. When the limit is reached, the Dr.Web Agent requests are placed into the waiting queue. The waiting queue size is unlimited. Set the **0** value to disable limitations on the number of simultaneous processes.
2. Set the **Limit updates traffic** flag to limit the network traffic bandwidth for transmitting updates from Dr.Web Server to Dr.Web Agents.

   If the flag is cleared, updates for Dr.Web Agents are transferred without limitation of network traffic bandwidth.
3. If the flag is set, specify in the **Maximal transmission speed (KB/s)** field the value of maximal speed for updates transmission. At this, updates will be transferred in ranges of specified bandwidth of summary network traffic for all Dr.Web Agents updates.

   It is allowed to configure up to five limits on updates transmission speed. To add one more field for the speed limitation, click  . To remove the limitation, click  next to the limit you want to remove.
4. In the schedule table, you can set the updates restrictions mode separately for each 30 minutes of each day of the week.

   To change the mode of limitations on data transmission, click the corresponding block of the table. Also, you can select several time blocks using drag and drop.

   Cells color is changed in cycle according to the color scheme under the table, starting from the option when updates transmission is allowed without traffic limitations, and to the option when updates transmission is forbidden.
5. After editing is complete, click **Save** to accept changes.

10.3.2.2. Installations

On the **Installations** tab, you can configure limits for the network traffic bandwidth for transmitting data during Dr.Web Agent installation on stations.

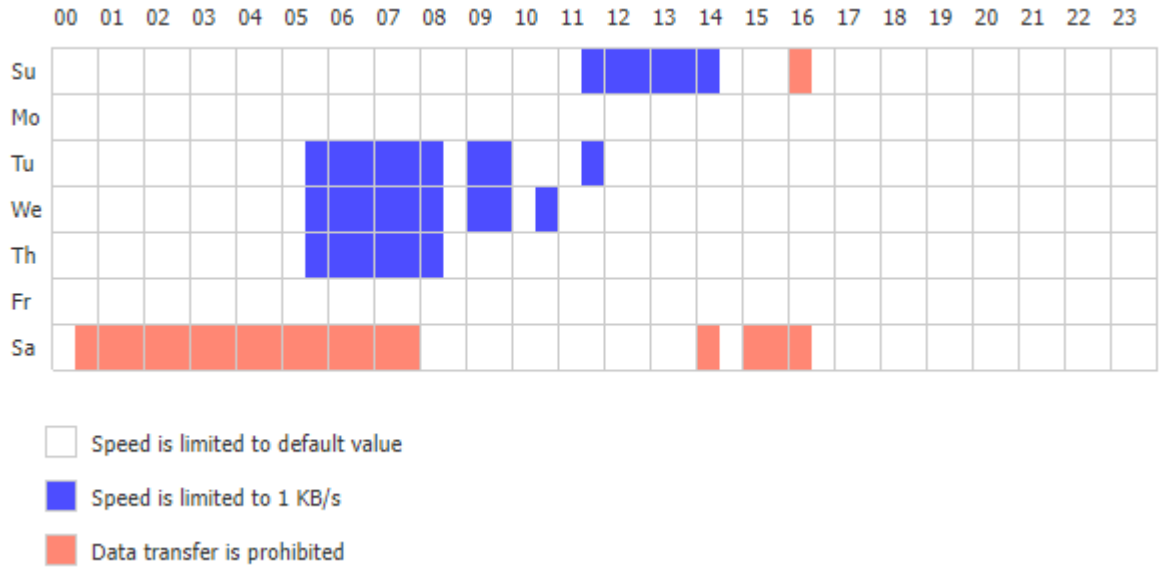
For more details see Workstation Traffic Limitations.

To set limits on the Dr.Web Agents installation traffic

1. In the **Number of simultaneous installation processes** field, you can specify maximum allowable number of the Dr.Web Agent installation sessions running at the same time from this Dr.Web Server. When the limit is reached, the Dr.Web Agent requests are placed into the waiting queue. The waiting queue size is unlimited. Set the 0 value to disable limitations on the number of simultaneous processes.
2. Set the **Restrict traffic on Dr.Web Agent installations** flag to limit the network traffic bandwidth for transmitting data from Dr.Web Server to stations during installations of Dr.Web Agents.

   If the flag is cleared, data on the Dr.Web Agent installations are transferred without limitation of network traffic bandwidth.
3. If the flag is set, specify in the **Maximal transmission speed (KB/s)** field the value of maximal speed for data transmission. At this, data for the Dr.Web Agent installations will be transferred in ranges of specified bandwidth of summary network traffic for all Dr.Web Agents.

   It is allowed to set up to five limits on data transmission speed for the Dr.Web Agent installations. To add one more field for the speed limitation, click  . To remove the limitation, click  next to the limit you want to remove.
4. In the schedule table, you can set the data transfer restrictions mode separately for each 30 minutes of each day of the week.



   To change the mode of limitations on data transmission, click the corresponding block of the table. Also, you can select several time blocks using drag and drop.

   Cells color is changed in cycle according to the color scheme under the table, starting from the option when data transmission is allowed without traffic limitations, and to the option when data transmission is forbidden.
5. After editing is complete, click **Save** to accept changes.

10.3.2.3. Workstation Traffic Limitations

You can limit the network traffic bandwidth for transferring data between Dr.Web Server and Dr.Web Agents in Dr.Web Enterprise Security Suite anti-virus network. You can separately configure limitations for transferring updates and limitations for transferring data during Dr.Web Agent installations.

The following options to limit the data traffic are available:

1. Limit data transfer bandwidth for all workstations.

   You can configure this option in the Dr.Web Server configuration section: select the **Administration** item in the main menu of the Control Center → the **Dr.Web Server configuration** item in the control menu → the **General** tab → the **Updates** or **Installations** internal tab → the **Restrict updates traffic** or **Restrict traffic on Dr.Web Agent installations** option correspondingly.
2. Limit update transfer bandwidth for certain stations or groups of stations personally.

   You can configure this option in stations configuration section: select the **Anti-virus Network** item in the main menu of the Control Center → select the station or group of stations in the network hierarchical list → the **Update restrictions** item of the control menu → the **Restrict updates traffic** option.

Data traffic is limited as follows:

1. If limitation is enabled for the common rate of data transferring in the Dr.Web Server settings, the summary rate of transferring data from Dr.Web Server to all stations will not exceed the specified value. At that:
   a) Not depending on the difference in bandwidth of channels between Dr.Web Server and stations, the transfer rate is equally distributed among all the stations.
   b) If the bandwidth of a channel between Dr.Web Server and a station is less than the average rate for one station calculated according to the **a)** item, the data transferring traffic for this station is limited to the maximum bandwidth of this channel. The rest limit of the common rate, is equally distributed among the set of stations as described in the **a)** item.
2. If the personal limitation for data transferring rate is set for a certain station or group of stations, the rate of transferring data to this group or stations will not exceed the specified value. This limitation does not affect on other stations and data are transferred to them at the maximum rate.
3. If both common and personal limitations are set in the Dr.Web Server settings and in the settings of a certain station or group, when:
   a) Rate of transferring data to the personally limited groups and stations will not exceed the value specified in their settings.

b) Rate of transferring data to the rest of stations is calculated as follows: the common limitation of data transferring rate, after subtraction of limitations in the **a)** item, is equally distributed among other workstations.

c) If the bandwidth of a channel between Dr.Web Server and a station, for which no personal limit is specified, is less than the average rate obtained in the **b)** item, the traffic for this station is limited to the maximum bandwidth of this channel. The rest rate similarly to the **b)** item is equally distributed among other stations, for which no personal limitations are specified.

10.3.3. Network

10.3.3.1. DNS

On the **DNS** tab, you can configure the following parameters of DNS server usage:

- **DNS queries time-out (sec.)**—time-out in seconds for resolving DNS direct/reverse queries. Set the 0 value to disable restriction on wait time until the end of the resolution.
- **Number of retried DNS queries**—maximum number of repeated DNS queries on fail while resolving the DNS query.
- Set the **Set the time to store DNS server responses** flag to specify time for storing responses from DNS server in the cache (TTL).
  - **For positive responses (min.)**—the storage time in the cache (TTL) of positive responses from the DNS server in minutes.
  - **For negative responses (min.)**—the storage time in the cache (TTL) of negative responses from the DNS server in minutes.
- **DNS-over-HTTPS server address**—compatible DNS-over-HTTPS server address.

For correct DoH operation, select **Any** in **Administration → General repository configuration → Dr.Web GUS → Allowed certificates**.

- **DNS servers**—list of DNS servers to replace the default system list.
- **DNS domains**—list of DNS suffixes to replace the default system list.

10.3.3.2. Proxy

On the **Proxy** tab, you can configure parameters of proxy server.

Set the **Use proxy server** flag to set up connections with Dr.Web Server via the proxy server. The following fields become available:

- **Proxy server**—IP address or DNS name of proxy server. If necessary, you can set the port in the address string in the following format: <*address*>:<*port*>. The `3128` port is used by default.

- To use authorization for access the proxy server according specified methods, set the **Use authorization** flag and specify the following parameters:
  - Specify the **Proxy server user** and **Password of proxy server user** fields.
  - Select one of authorization methods:

Option		Description
Any supported method		Use any authorization method supported by the proxy server. If the proxy server supports several authorization methods, the most secured is used.
Any safe supported method		Use any secured authorization method supported by the proxy server. In this mode, the Basic authorization method is not supported. If the proxy server supports several authorization methods, the most secured is used.
The following methods:	Basic authorization	Use Basic authorization. It is not recommended to use this method because transfer of authorization accounting data is not encrypted.
	Digest authorization	Use Digest authorization. Cryptographic authorization method.
	Digest authorization with IE support	Use Digest authorization. Cryptographic authorization method. Enables support for Internet Explorer browser of version 6 and earlier.
	NTLM authorization	Use NTLM authorization. Cryptographic authorization method. The NTLM protocol of Microsoft company is used for authorization.
	NTLM authorization via winbind	Use NTLM authorization via an external winbind application. Cryptographic authorization method.
	GSS-Negotiate authorization	Use GSS-Negotiate authorization. Cryptographic authorization method.

10.3.3.3. Transport

On the **Transports** tab, you can configure parameters of transport protocols used by Dr.Web Server to connect with clients.

- In the **Encryption** drop-down list, select the policy of traffic encryption between Dr.Web Server and connected clients: Dr.Web Agents, neighbor Dr.Web Servers, Network Installers.
- In the **Compression** drop-down list, select the policy of traffic compression between Dr.Web Server and connected clients: Dr.Web Agents, neighbor Dr.Web Servers, Network Installers. For more details on this parameters, read p. Traffic Encryption and Compression.

  For more details about these parameters see Traffic Encryption and Compression.

- When you select **Yes** or **Possible** for traffic compression, the **Compression level** drop-down list become available. In this list you can select data compression level from 1 to 9, where the 1 is minimal level and 9 is maximal compression level.

See the Traffic Encryption and Compression section for more details.

- In the **Encryption key for TLS session tickets** field, specify the path to encryption key for TLS session tickets. Used to resume a TLS session based on session tickets which are encrypted using the specified key.

In the **TCP/IP** subsection, parameters of connection with Dr.Web Server via TCP/IP are set:

- **Address** and **Port**—correspondingly the IP address and the port number of the network interface to which this transport protocol is bound. Dr.Web Server listens interface with specified parameters to communicate with Dr.Web Agents that installed on workstations.
- Set the **Discovery** flag to enable the Dr.Web Server discovery service.
- Set the **Multicasting** flag to use the *Multicast over UDP* mode for detecting Dr.Web Server.
- **Multicast group**—IP address of multicast group in which Dr.Web Server is registered. It is used for communication of Dr.Web Agents and Network installers when searching active Dr.Web Servers in the network. If field is not specified, the `231.0.0.1` group is used by default.
- **Name**—the name of Dr.Web Server. If no name is specified, the name set on the **General** tab is used (see above, if no name is set on the tab, the computer name is used). If the other name specified for the protocol than the name from the **General** tab, the name from the protocol description is used. This name is used by detection service to find Dr.Web Server by Dr.Web Agents and etc.
- Under Unix-like OS only: in the **Path** field, specify the path to the connection socket, e.g., with Dr.Web Agent.

See the Configuring Network Connections section for more details.

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

10.3.3.4. Email

On the **Email** tab, you can configure parameters of sending emails from the Control Center, e.g., as administrative notifications or when mailing installation packages of the stations or to restore the administrator password.

- **Sender email address**—email address which will be set as a sender of emails.
- **Server address**—SMTP server address which is used to send emails.
- **Port**—SMTP server port which is used to send emails.

- **User**, **Password**—if necessary, specify name and password of SMTP server user, if the SMTP server requires authorization.
- **SMTP server connection time-out**—time-out in seconds to establish a connection with SMTP server. The value is positive integer greater than or equal to 1.
- In the **Connection security** drop-down list, select the type of encrypted data exchange:
  - **STARTTLS**—switching to secured connection is performed by using the `STARTTLS` command. The 25 port is used by default for the connection.
  - **SSL/TLS**—establish a new secured TLS connection. The 465 port is used by default for the connection.
  - **No**—do not use encryption. Data exchange will be over an unprotected connection.
- Set the **Use CRAM-MD5 authentication** flag to use *CRAM-MD5* authentication on a mail server.
- Set the **Use DIGEST-MD5 authentication** flag to use *DIGEST-MD5* authentication on a mail server.
- Set the **Use LOGIN authentication** flag to use *LOGIN* authentication on a mail server.
- Set the **Use AUTH-NTLM authentication** flag to use *AUTH-NTLM* authentication on a mail server.
- Set the **Use the plain authentication** flag to use *plain text* authentication on a mail server. Set the **Validate the Dr.Web Server certificate** flag to enable validating the TLS certificate of a mail server.
- Set the **Validate the certificate** flag to validate the TLS certificate of mail server. In the **TLS certificates** field specify the path to the TLS certificates.
- Set the **Debug mode** flag to get SMTP session detailed log.
- In the **Recipient email addresses** field, you can specify the email addresses to check the email sending. Click **Send test message** to send the test email (same as the Dr.Web Server notification) according to the settings specified in this section.

10.3.3.5. Cluster

On the **Cluster** tab, you can configure parameters of Dr.Web Servers cluster for data exchange in multiserver anti-virus network configuration.

To use the cluster, specify the following parameters:

- **Multicast group**—IP address of multicast group through which Dr.Web Servers will be exchanging information.
- **Port**—port number of network interface to which transport protocol is bound to transmit the information into multicast group.
- **Time to live**—time to live of a datagram for data transfer within Dr.Web Servers cluster.
- **Interface**—IP address of network interface to which transport protocol is bound to transmit the information into multicast group.

Peculiarities of Dr.Web Server clustering are given in the Dr.Web Server Cluster section.

10.3.3.6. Download

On the **Download** tab, you can configure the Dr.Web Server parameters for generating Dr.Web Agent installation files for an anti-virus network stations. Further these parameters are used for connecting Dr.Web Agent installer to Dr.Web Server:

- **Dr.Web Server address**—IP address, NetBIOS or domain name of Dr.Web Server. If Dr.Web Server address is not specified, computer name returned by the operating system is used.

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

- **Port**—port number which is used for connecting Dr.Web Agent installer to Dr.Web Server.

  If the port number is not specified, the 2193 port is used (it is configured in the Control Center, at **Administration** → **Dr.Web Server configuration** → **Network** tab → the **Transport** tab).

The settings of the **Download** section are saved in the `download.conf` configuration file (see the **Appendices** document, F3. Download.conf Configuration File).

10.3.3.7. Multicast Updates

On the **Multicast updates** tab, you can configure updates transmission on workstations via the multicast protocol.

Set the **Enable multicast updates** flag to enable transmission of updates to stations via the multicast protocol.

General principles of multicast updates:

1. If multicast updates are enabled, when for all stations connected to this Dr.Web Server updating is performed in two stages:
   a) Stations are listening the specified multicast groups into which Dr.Web Server is included. When multicast updates are ready, stations download them via *multicast over UDP*.
   b) After multicast updates are transmitted, Dr.Web Server sends standard notification to stations about updates to get. All that failed to download via the multicast updates, stations download using a standard TCP update.
2. If multicast updates are disabled, updating of all stations is performed only in general mode —via the TCP protocol.

To setup multicast updates, use the following parameters:

- **UDP datagram size (bytes)**—size of UDP datagrams in bytes.

  Allowed range is 512–8192. To avoid fragmentation, it is recommended to set a value less than MTU (Maximum Transmission Unit) of the network.
- **File transmission time (ms.)**—during specified time, single update file is transmitted, after that Dr.Web Server starts sending the next file.

  All files which failed to transmit at step of multicast protocol update, will be transmitted at standard update process over the TCP protocol.
- **Multicast updates duration (ms.)**—duration of update process via multicast protocol.

  All files that failed to transmit during update stage via multicast protocol will be transmitted in process of standard update via TCP protocol.
- **Packages transmission interval (ms.)**—interval of packages transmission to a multicast group.

  The low interval value may cause significant losses during package transfer and network overload. It is not recommended to change this parameter.
- **Interval between retransmission requests (ms.)**—with this interval Dr.Web Agents send requests for retransmission of lost packages.

  Dr.Web Server accumulates these requests after that sends lost blocks.
- **"Silence" interval on the line (ms.)**—when a file transmission is over before allowed time has expired, if during specified "silence" interval no requests from Dr.Web Agents for retransmission of lost packages are received, Dr.Web Server considers that all Dr.Web Agent received updates files and starts sending the next file.
- **Retransmission requests accumulation interval (ms.)**—during specified interval, Dr.Web Server accumulates requests from Dr.Web Agents for retransmission of lost packages.

  Dr.Web Agent request lost packages. Dr.Web Server accumulates these requests during specified time slot after that sends lost blocks.

To specify the list of multicast groups from which multicast updates is available, setup the following parameters in the **Multicast groups** section:

- **Multicast group**—IP address of multicast group in which stations receive multicast updates.
- **Port**—port number of Dr.Web Server network interface, to which transport multicast protocol is bound for updates transmission.

  For multicast updates, you must specify any unused port, particularly, different from the port that is specified in the settings of transport protocol for the Dr.Web Server operating.
- **Time to live**—Time to live of a datagram for data transfer during multicast updates.
- **Interface**—IP address of Dr.Web Server network interface, to which transport multicast protocol is bound for updates transmission.

  Every line contains setup of one multicast group. To add one more multicast group, click  .

When you configure several multicast groups, please note the following features:

- For different Dr.Web Servers, which will distribute multicast updates, must be different multicast groups specified.
- For different Dr.Web Servers, which will distribute multicast updates, must be different **Interface** and **Port** parameters specified.
- For using several multicast groups, sets of stations which are included into these groups must not overlap. Thus, each station of anti-virus network can be included only into one multicast group.

In the **Access control list** section, you can configure restrictions for network addresses of stations to which multicast updates can be sent:

- Stations that are allowed to receive multicast updates, listen specified multicast groups and receive updates using the standard scheme (see procedure 1).
- Stations that are denied to receive multicast updates, do not listen specified multicast groups for updates but download all updates via TCP (see procedure 2).

Configuration of the lists is the same as the configuration of the lists in the Security section.

10.3.4. Statistics

On the **Statistics** tab, you can configure statistics information that will be written to the log file, to the Dr.Web Server database, and further can be viewed in the statistics section of the Control Center.

To add corresponding type of information to the DB, set the following flags:

- **Quarantine state**—logs stations Quarantine state.
- **Hardware and software composition**—enables monitoring of hardware and software composition and storing the information in the database.
- **List of the station modules**—enables monitoring of the list of the station modules and storing the information in the database.
- **List of installed components**—enables monitoring of the list of the installed components (Scanner, monitors, etc) and storing the information in the database.
- **Sessions of stations users**—enables monitoring of user sessions and storing in the database the logins of users which are loged in the system with installed Dr.Web Agent.
- **Start/Stop of components**—enables monitoring of the information on the start and stop of the components (Scanner, monitors, etc) and storing the information in the database at stations.
- **Detected security threats**—enables monitoring of infections detecting and storing the information in the database.

  If the **Detected security threats** flag is set, you can also configure additional parameters of statistic on infections.

- Set the **Track epidemic** flag to notify the administrator of malware outbreak cases. If the flag is cleared, notifications on threat detection are performed in the standard mode. If the flag is set, you can configure the following parameters of malware outbreak tracking:
  - **Prohibition period on sending notifications**—time period in seconds after sending the notification about epidemic, during which single notifications about infected stations will not be sent.
  - **Period of infected stations counting**—time period in seconds, during which specified number of messages on infected stations must be received, to send the corresponding notification about epidemic.
  - **Messages number**—the number of messages on infections that must be received in specified time period, so that Dr.Web Server may send to the administrator a single notification on epidemic on all cases of infection (the **Epidemic in the network** notification).
  - **Number of the most common threats**—number of the most frequently occurring threats which must be included in the epidemic report.
- Set the **Group reports of Preventive protection** flag to send a single summary report on multiple events of Preventive protection. If the flag is cleared, the Preventive protection events are sent in separate notifications, not depending on their number. If the flag is set, you can configure the following parameters of summary reports:
  - **Prohibition period on sending notifications**—time period in seconds after sending a summary report on Preventive protection events, during which notifications about single events will not be sent.
  - **Period of counting terminated connections**—time period in seconds, during which specified number of Preventive protection events must be occurred to send a summary report.
  - **Events number**—the number of the Preventive protection events that must be received in specified time period, so that Dr.Web Server may send to the administrator a single summary report on these events (the **Summary report of Preventive protection** notification).
  - **Number of the most active processes**—number of the most frequently occurring processes that have performed a suspicious action, which must be included in the Preventive protection report.
- Set the **Send statistics to Doctor Web company** flag, to activate sending statistics on detected stations security threats to the Doctor Web company. The following fields will become available:
  - **Interval**—an interval in minutes for sending statistics;
  - **Identifier**—an MD5 key (located in the Dr.Web Server configuration file);

Interval for sending statistics is the only obligatory field.

- **Abnormally terminated connections**—enables monitoring of abnormally terminated connections with clients and be able to send corresponding notifications to the administrator.

  Specify the following settings of abnormally terminated connections:

- **Prohibition period on sending notifications**—time period in seconds after sending the notification on multiple connections termination, during which notifications about single terminated connections will not be sent.
- **Period to counting terminated connections**—time period in seconds, during which specified number of connections with clients must be terminated, to send the corresponding notification.
- **Number of connections for notification on single terminations**—minimum number of connections with a single address that must be terminated during the counting period, to send the notification about single abnormally terminated connection (the **Connection terminated abnormally** notification).
- **Number of connections for notification on multiple terminations**—minimum number of connections that must be terminated during the counting period, to send the common notification about multiple abnormally terminated connections (the **Large number of abnormally terminated connections detected** notification).
- **Duration of short connections**—if duration of terminated connection with a client is less than specified value, then specified number of connections is reached, notification about single terminated connections will be sent not depending on the counting period. At this, the connection must not be terminated further by the longer connections, and the notification about multiple abnormally terminated connections must not be sent (the **Large number of abnormally terminated connections detected** notification).

- **Scan errors**—enables monitoring of scan errors occurring and storing the information in the database.
- **Scan statistics**—enables monitoring of the statistics of scanning and storing the information in the database.
- **Dr.Web Agent installations**—logs the information about Dr.Web Agent installations on the stations.
- **Blocked devices**—enables monitoring of information on devices blocked by the Office Control component and storing the information in the database.
- **Application Control statistics on processes activity**—enables monitoring of processes activity at stations detected by Application Control and write the information to the database.
- **Application Control statistics on processes blocking**—enables monitoring the blocking of the processes at stations by Application Control and write the information to the database.
- **Multiple blockings by Application Control**—allows to track multiple blockings of processes by Application Control and be able to send corresponding notifications to the administrator.

  Specify the following events settings:
  - **Prohibition period on sending notifications**—time period in seconds after sending a summary report on processes blocked by Application Control, during which notifications about single blockings will not be sent.
  - **Period of counting blocked processes**—time period in seconds, during which specified number of processes must be blocked to send a summary report.

  - **Events number**—the number of events on processes blocked by Application Control that must be received in specified time period, so that Dr.Web Server may send to the administrator a single summary report on these events (**Large number of blocks by the Application Control detected** notification).
  - **Number of the most common profiles**—number of the most common profiles according to which the block was made, and which must be included in the notification on multiple blockings.
- **Station tasks execution log**—log results of tasks execution on workstations and store the log in the DB.
- **Station statuses**—log status changes for workstations and store the log in the DB.
  - **Virus database statuses**—log changes in virus databases status and contents on workstations and store the logs in the DB. The flag is available only if the **Station statuses** flag is set.
- **Location data**—get information on stations location and store the information in the database.
- **Disk space on stations**—monitor disk space data on stations and store the information in the database.
- **Collect device information**—allows Dr.Web Server to collect data on devices connected to stations.
- **Collect user information**—allows Dr.Web Server to collect information about users on stations.

Similar information collection settings that allow sending data from Dr.Web Agent to Dr.Web Server are available in the Dr.Web Agent. The settings above determine whether Dr.Web Server will store and process data received from the Dr.Web Agent.

To view statistics information

1. Select the **Anti-virus network** item of the main menu.
2. Select a station or a group in the hierarchical list.
3. Open the corresponding section of the control menu (see the table below).

Detailed information about statistical data is described in the Viewing Workstation Statistics section.

The table below describes correspondence between flags in the **Statistics** tab of the Dr.Web Server settings and items of the control menu on the **Anti-virus network** page.

If you clear flags on the **Statistics** tab, corresponding items of the control menu become hidden.

Table 10-1. Correspondence between flags of Statistics data section and items of the control menu

Dr.Web Server parameters	Menu options
Quarantine state	General → Quarantine Configuration → Windows → Dr.Web Agent → Quarantine remote control flag
Hardware and software composition	General → Hardware and software General → Detected devices
List of the station modules	Statistics → Modules
List of installed components	General → Installed components
Sessions of stations users	General → User sessions
Start/Stop of components	Statistics → Start/Stop
Detected security threats	Statistics → Threats Statistics → Threat statistics Statistics → Preventive protection events
Scan errors	Statistics → Errors
Scan statistics	Statistics → Scan statistics
Dr.Web Agent installations	Statistics → Dr.Web Agent installations
Blocked devices	Statistics → Blocked devices
Application Control statistics on processes activity	Statistics → Application Control events
Application Control statistics on processes blocking	Administration → Application Control → Application Catalog
Station tasks execution log	Statistics → Tasks
Station statuses	Statistics → Status Statistics → Virus databases
Virus database statuses	Statistics → Virus databases

10.3.5. Security

On the **Security** tab, you can configure restrictions for network addresses from which Dr.Web Agents, network installers and other ("neighboring") Dr.Web Servers will be able to access the current Dr.Web Server.

To manage the Dr.Web Server audit log, use the following flags:

- **Audit of administrator operations** allows to log operations of administrator with Dr.Web Security Control Center and writing the log into the DB.
- **Audit of server internal operations** allows to log Dr.Web Server internal operations and writing the log into the DB.
- **Audit of Web API operations** allows to log operations via XML API.

To view the audit log, select the **Administration** option in the main menu, then **Audit log** item in the control menu.

The **Security** tab contains additional tabs on which you can set the restrictions for the correspondent types of connections:

- **Agents**—the list of limitations on IP addresses from which Dr.Web Agents can connect to this Dr.Web Server.
- **Installations**—the list of limitations on IP addresses from which Dr.Web Agents installers can connect to this Dr.Web Server.
- **Neighbors**—the list of limitations on IP addresses from which neighbor Dr.Web Servers can connect to this Dr.Web Server.
- **Discovery service**—the list of limitations on IP addresses from which broadcast queries can be received by the Dr.Web Server Detection Service.

To set access restrictions (separately for Dr.Web Agents, Installations, Neighbor Dr.Web Servers or Discovery service)

1. Set the **Use this ACL** flag to specify lists of allowed or denied addresses. If the flag is cleared, all connections are allowed.
2. To allow the access from a specific TCP address, include it into the **TCP: Allowed** or **TCPv6: Allowed** list.
3. To deny specific TCP address, include it into the **TCP: Denied** or **TCPv6: Denied** list.
4. The addresses not included into any of the lists are allowed or denied depending on whether the **Denial priority** flag is set. If the flag is set, the **Denied** list has a higher priority than the **Allowed** list. Addresses not included in any of the lists or included into both of them are denied. Allowed only addresses that are included in the **Allowed** list and not included in the **Denied** list.

To edit the address list

1. Specify network address in the corresponding field in the following format: <*IP address*>/[<*network prefix*>].
2. To add a new field, click the  button in the corresponding section.
3. To delete a field, click  next to the deleting address.
4. Click **Save** to apply settings.

Lists for TCPv6 addresses will be available, if the IPv6 interface is installed on the computer.

Examples of prefix usage:

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

   Containing 254 addresses.

   Host addresses look like: `195.136.12.*`
2. Prefix 8 stands for a network with a network mask: `255.0.0.0`

   Containing up to 16777214 addresses (256*256*256-2).

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

10.3.6. Cache

On the **Cache** tab, you can configure the following parameters of the Dr.Web Server cache cleanup:

- **Cache flush period**—period of full cache flush.
- **Quarantined files**—cleanup interval of quarantined files.
- **Repository files**—cleanup interval of files in repository.
- **File cache**—cleanup interval of file cache.
- **Installation packages**—cleanup interval of personal and group installation packages.

  Click **Delete all installation packages now**, to delete all personal and group installation packages created before and resided in the `installers-cache` folder of the `var` folder. Please note: when accessing these packages for downloading, they will be created anew which may take some time.

When setting numerical values, please note the drop-down lists with unit of measure for intervals.

10.3.7. Database

On the **Database** tab, you can configure the DB required for Dr.Web Server operation.

Dr.Web Server database structure is available in the form of a separate manual of the same name. The document can be opened from the **Support** section in Dr.Web Security Control Center.

To specify parameters for working with the database

1. In the **Number of connections** field, specify the maximum number of Dr.Web Server connections with the database.

   Do not change the default value when using the embedded database. The use of an external database may require a higher value. Recommendations on determining the optimal value are given in **Appendices**, in the Dr.Web Server Load and Recommended Configuration Parameters section.

   The embedded DB is intended for use in networks where about 400–600 stations are connected to Dr.Web Server. If the hardware configuration of the computer on which Dr.Web Server is installed and the load level of other executing tasks permit, between 1000 and 1500 stations can be connected.

   Otherwise, you must use an external DB. Depending on the configuration and the load level of the computer running Dr.Web Server, the external DB may be used on the same or on a dedicated computer.

   If you use an external DB in an anti-virus network with more than 10 000 stations, it is recommended that you follow these minimal system and hardware requirements:

   - 3 GHz processor CPU,
   - at least 6 CPU cores,
   - at least 4 GB RAM for Dr.Web Server and at least 8 GB RAM for the DB server,
   - Unix-like OS.

   When working in an anti-virus network with a large number of client connections to Dr.Web Server, it is recommended that you consult with the Doctor Web technical support team before changing the value.

2. Set the **Automatically purge the database after maintenance procedures** flag to automatically perform delayed purging of the database after its initialization, upgrade, and import. If the flag is cleared, automatic purging is not performed. In this case it is recommended to configure the **Purge database** task in the Dr.Web Server schedule or purge the database manually in the Database Management section.

   To perform automatic purging, a hidden task is created in the Dr.Web Server schedule. The task is executed the next night after the designated maintenance procedures, at 01:17 local time of Dr.Web Server. The task is executed only if the Dr.Web Server schedule does not

contain another **Purge database** task within the next 24 hours relative to the maintenance procedures.

3. Select the database type in the **Database** drop-down list:
   - **MySQL**—external DB,
   - **ODBC**—to use an external DB via an ODBC connection (for Microsoft SQL Server/Microsoft SQL Server Express),

   If warnings or errors occur while Dr.Web Server interacts with the Microsoft SQL Server DBMS via the ODBC, please make sure that you are using the latest available DBMS version for this edition.

   You can learn how to determine whether an update is available on the following Microsoft company page: https://learn.microsoft.com/troubleshoot/sql/general/determine-version-edition-update-level.

   - **Oracle**—external DB for all platforms except FreeBSD,

   If you use an Oracle external DBMS via an ODBC connection, install the latest version of the ODBC driver delivered with the DBMS. It is strongly recommended not to use the Oracle ODBC driver supplied by Microsoft.

   - **PostgreSQL**—external DB,
   - **SQLite3**—embedded DB (a component of Dr.Web Server).
4. Set the necessary settings for working with the DB:
   - For the embedded DB, if necessary, enter the full path to the database file in the **File name** field and specify the cache size and the flush mode.
   - The parameters of an external DB are described in detail in the **Appendices** document, Appendix A. The Description of the DBMS Settings. The Parameters of the DBMS Driver.
5. Click **Save** to apply the specified settings.

The Dr.Web Server distribution kit contains embedded clients for the supported DBMS, so note the following:

- If you plan to use the embedded DBMS clients supported within Dr.Web Server, then during installation (upgrading) of Dr.Web Server make sure that installation of the corresponding embedded DBMS client is enabled in the **Database support** section of the installer settings.
- If you plan to use the Oracle DB via an ODBC connection as your external database, then during installation (upgrading) of Dr.Web Server, in the installer settings, disable installation of the Oracle DBMS embedded client (in the **Database support** → **Oracle database driver** section). Otherwise you will be unable to work with the Oracle DB via ODBC because of a library conflict.

The Dr.Web Server installer supports product modification mode. To add or remove separate components, for instance, database management drivers, run the Dr.Web Server installer and select the **Change** option.

The embedded DB is intended for use by default. This mode considerably increases the load on Dr.Web Server. It is recommended to use an external DBMS in large anti-virus networks. The procedure for changing the DB type is described in the **Appendices**, document, the Changing the Type of the DB for Dr.Web Enterprise Security Suite section.

It is possible to perform operations related to purging the database used by Dr.Web Server, in particular: deleting records of events, as well as information about workstations that have not visited Dr.Web Server for a certain period of time. To purge the database, open the Setting Dr.Web Server Schedule and create an appropriate task.

10.3.7.1. Database Restore

If the **SQLite3** embedded database get malformed, the corrupted database can be restored by regular means.

If the database get corrupted, the following actions performed:

1. If the database corrupted, the Dr.Web Server startup and operation is not performed:
   a) During the Dr.Web Server operation: if the corruption detected during regular interaction with embedded database, Dr.Web Server stops automatically.
   b) During the Dr.Web Server startup: if in the **SQLite3** database settings, in the **Image integrity verification** drop-down field, the **Quick** or **Full** option is set, then automatic verifying of the database image integrity is performed. If corruption detected, the Dr.Web Server startup is not performed.
2. To be able to start Dr.Web Server, the corrupted database must be repaired:
   a) If the **Restore corrupted image automatically** flag is set in the **SQLite3** database settings, the automatic restoring of the corrupted database image at Dr.Web Server startup is performed.
   b) If automatic restoring of the database image is disabled, you can use the `repairdb` switch to start Dr.Web Server from the command line (see also the **Application** document, G3.3. Database Commands).

10.3.8. Modules

On the **Modules** tab, you can configure protocols for interaction of Dr.Web Server with other Dr.Web Enterprise Security Suite components.

- Set the **Dr.Web Agent protocol** flag to enable protocol that allows interaction of Dr.Web Server with Dr.Web Agents.
- Set the **Microsoft NAP Health Validator protocol** to enable protocol that allows interaction of Dr.Web Server with the Microsoft NAP Validator component of system health validating.
- Set the **Dr.Web Agent installer protocol** flag to enable protocol that allows interaction of Dr.Web Server with Dr.Web Agent installers.
- Set the **Dr.Web Servers cluster protocol** flag to enable protocol for interaction between Dr.Web Servers in the cluster system.
- Set the **Dr.Web Server protocol** flag to enable protocol that allows interaction of Dr.Web Server with other Dr.Web Servers. The protocol is disabled by default. If you use multi-server network configuration (see Peculiarities of a Network with Several Dr.Web Servers), set the **Dr.Web Server protocol** flag to enable this protocol.
- Set the **Dr.Web Proxy Server protocol** flag to enable protocol that allows interaction of Dr.Web Server with Dr.Web Proxy Servers.
- Set the **Dr.Web Security Control Center extension** flag for managing Dr.Web Server and anti-virus network via the Control Center.

If you clear the **Dr.Web Security Control Center extension** flag, when after reboot of Dr.Web Server, Dr.Web Security Control Center will be not available. You will be able to manage Dr.Web Server and anti-virus network only via the remote diagnostics utility, if the **Dr.Web Server FrontDoor extension** flag is set.

- Set the **Dr.Web Server FrontDoor extension** flag to use Dr.Web Server FrontDoor extension that allows connections of the Dr.Web Server remote diagnostics utility (see also Dr.Web Server Remote Access).
- Set the **Dr.Web SNMP agent extension** flag to allow Dr.Web Server to exchange information with network management systems via SNMP (see also Dr.Web SNMP Agent Configuration).
- Set the **Yandex.Locator extension** flag to allow the use of Yandex.Locator extension to determine location of mobile devices connected to Dr.Web Server.
  - In the **API key** field, enter your API key registered in corresponding service of Yandex company.

If you enable the Yandex.Locator extension but have not specify the API key, the extension will not be active.

You can find detailed information on using and configuring the Yandex.Locator extension in the **Appendices** document, in the Automatic Location of Stations under Android OS section.

10.3.9. Location

On the **Location** tab, you can specify additional information about the physical location of the computer on which Dr.Web Server is installed.

Also on this tab you can view the Dr.Web Server location on a geographical map.

To view the Dr.Web Server location on a map

1. In the **Latitude** and **Longitude** fields, specify the Dr.Web Server geographical coordinates in the Decimal Degrees format.
2. Click **Save** to save specified data to the Dr.Web Server configuration file.

   To view the map, you do not need to restart Dr.Web Server. But to apply changed geographical coordinates, you must restart Dr.Web Server.
3. On the **Location** tab, the OpenStreetMap preview will be shown containing a mark according to the specified coordinates.

   If the preview cannot be loaded, the **Show on map** text displays.
4. To view the full size map, click the preview or the **Show on map** text.

10.3.10. Licenses

On the **Licenses** tab, you can configure settings of licenses propagation between Dr.Web Servers and also options for reports on license usage.

Options for notification on limitation on a number of licenses in the license key

- **Number of remaining licenses**—maximal number of remaining licenses for which the **Limitation on a number of licenses in the license key** notification will be sent.
- **Percentage of remaining licenses**—maximal percentage of remaining licenses for which the **Limitation on a number of licenses in the license key** notification will be sent.

Options for the report on license usage

At sending reports between Dr.Web Servers, these options must be specified on a parent Dr.Web Server but are used by child Dr.Web Servers.

If connections with neighbor Dr.Web Servers are not configured, these options are used only by the current Dr.Web Server for its personal reports.

- **Period of report creation**—period of reports creation by Dr.Web Server on license keys it uses.

  If a report on license usage is created by a child Dr.Web Server, then after it is created, this report is sent to the main Dr.Web Server.

  Created reports are additionally sent at each connection (including restart) of Dr.Web Server, and also at changing the number of donated licenses at the main Dr.Web Server.
- **Period of active stations counting**—period for counting the number of active stations for creating the report on licenses usage. The 0 value prescribes to count all stations in the report not depending on their activity status.

Options for Dr.Web Server that donates licenses

- **Automatic renewal period of donated licenses**—time period for which licenses are donated from the key on this Dr.Web Server. After this period, the donated licenses are automatically renewed for the same period. Automatic renewal is performed before the expiration of the license propagation period specified in the License Manager at step 5. This mechanism provides returning of licenses to the parent Dr.Web Server if the child Dr.Web Server will be turned off and will not be able to return donated licenses.
- **License synchronization period**—interval for synchronizing information about donating licenses between Dr.Web Servers. Licenses synchronization allows to detect that the number of licenses donated by the parent Dr.Web Server and received by the child Dr.Web Server are not equal. This mechanism allows to detect malfunctions and cases of forgery during licenses donation.

Options for the Dr.Web Server that receives licenses

- On the **Licenses** tab, specify the **Interval for preliminary renewal of accepted licenses**—time interval before the expiration of the licenses automatic renewal period, received from a neighbor Dr.Web Server starting from which, this Dr.Web Server requests the preliminary automatic renewal of these licenses.

  Using this option depends on the type of connection selected in the **Connection options** setting in the neighbor Dr.Web Servers configuration (see Setting Connections between Several Dr.Web Servers):

  - For the periodic connection type: if the reconnection period specified in the neighbor settings is greater than **Automatic renewal period of donated licenses** specified on the

Dr.Web Server that donated licenses, when automatic renewal of these licenses will be initiated earlier than the **Automatic renewal period of donated licenses** expires.

- For the permanent connection: this option is not used.

Detailed information on licenses propagation between Dr.Web Servers is described in the Donating Licenses via Interserver Connections section.

10.3.11. Log

On the **Log** tab, you can configure the settings of Dr.Web Server operation log:

- In the **Dr.Web Server log verbosity level** drop-down list, select the detail level for Dr.Web Server operation log.
- **Maximum number of files**—maximal number of log files (including the current and the archived) that will be stored.
- **Dr.Web Server log rotation mode**—rotation mode of the Dr.Web Server operation log. Select one of the given values:
  - **rotation by size** defines the limitation on the size of each log file.

    Maximum size of each file—maximal allowed size of each log file. When the current file reaches specified size, it becomes archived with corresponding change of a name, and a new log file is created.
  - **rotation by time** defines the time to write each log file.

    Maximum time to write the file—maximal duration to write each log file. When the write time of the file reaches specified duration, it becomes archived with corresponding change of a name, and a new log file is created.
- Set the **Archive log files** flag to archive old log files at rotation.

To apply specified changes, Dr.Web Server restart required.

The restart can be launch either via the Control Center or by using corresponding console command.

Detailed information on the Dr.Web Server log is given in the Dr.Web Server Log section.

10.4. Dr.Web Server Remote Access

For connection of the Dr.Web Server remote diagnostics utility, you must enable Dr.Web Server FrontDoor extension. To do this, in the **Dr.Web Server configuration** section, on the Modules tab, set the **Dr.Web Server FrontDoor extension** flag.

For connection of the Dr.Web Server remote diagnostics utility, administrator that connects via the utility, must have the **Use additional features** permission. Otherwise, access to Dr.Web Server via the remote diagnostics utility will be forbidden.

To configure parameters for Dr.Web Server remote diagnostics utility

1. Select the **Administrating** item in the main menu of the Control Center, in the opened window, select **Dr.Web Server remote access** in the control menu.
2. Specify the connection protocol settings:
   - Set the **Use TLS** flag to enable connections of the remote diagnostics utility to Dr.Web Server via TLS protocol. If the flag is cleared, only TCP connections are allowed.
     For TLS connection, specify the following settings:
     - **Certificate**—TLS certificate file which will be verified on connection. The drop-down list contains available certificates from the Dr.Web Server folder.
     - **SSL private key**—SSL private key file which will be verified on connection. The drop-down list contains available private keys from the Dr.Web Server folder.
     - In the **Encryption key for TLS session tickets** field, specify the path to encryption key for TLS session tickets. Used to resume a TLS session based on session tickets which are encrypted using the specified key.
     - **Allowed cipher list**—the string defining the list of ciphers from OpenSSL package that allowed for use in client connections. Leave the field blank to use the `DEFAULT` value that means `ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2`.
3. Specify the connection interface settings:
   - **Address**—IP address that is listened on the Dr.Web Server side for connecting the remote diagnostics utility.
   - **Port**—port that is listened on the Dr.Web Server side for connecting the remote diagnostics utility. The 10101 port is used by default.

   To add one more connection interface, click  and specify the values of added fields.

   To forbid a connection from the previously allowed interface, remove it from the list by clicking  next to the line with this interface.
4. Click **Save**.

You can view the usage description of the console version of the Dr.Web Server remote diagnostics utility in the **Appendices** document, G7.3. Dr.Web Server Remote Diagnostics Utility.

10.5. Dr.Web SNMP Agent Configuration

Dr.Web SNMP agent is designed for integration of Dr.Web Enterprise Security Suite with network management systems via SNMP. Such integration will allow to control operational status of Dr.Web components as well as collect statistics on detected and neutralized threats.

Monitoring systems or any SNMP managers can call Dr.Web Server that will provide requested information through Dr.Web SNMP agent extension.

To get information that can be provided by Dr.Web SNMP agent, you can use the MIB supplied with Dr.Web Server. The `DRWEB-ESUITE-STAT-MIB.txt` file is located in the `etc` subdirectory of the Dr.Web Server installation directory.

To allow Dr.Web Server to exchange information with network management systems via SNMP protocol, you must enable Dr.Web SNMP agent extension. To do this, in the **Dr.Web Server configuration** section, on the Modules tab, set the **Dr.Web SNMP agent extension** flag.

To configure parameters for connecting to Dr.Web SNMP agent

1. Select the **Administrating** item in the main menu of the Control Center, in the opened window, select **Dr.Web SNMP agent configuration** in the control menu.
2. In the **Community** field, specify SNMPv2c community name. Default is **public**.
3. Specify the interface settings for connection with network management systems:
   - **Interface**—IP address that is listened on the Dr.Web Server side for incoming connections from network management systems.
   - **Port**—port that is listened on the Dr.Web Server side for incoming connections from network management systems.

   To add one more connection interface, click  and specify the values of added fields.

   To forbid a connection from the previously allowed interface, remove it from the list by clicking  next to the line with this interface.
4. Set the **Allow access from local networks only** flag allow connecting to Dr.Web SNMP agent from local networks only.

   At this, specify the **List of local addresses**, from which connection to Dr.Web SNMP agent is allowed.
5. Click **Save**.

10.6. Setting Dr.Web Server Schedule

To edit Dr.Web Server schedule

1. Select the **Administration** item in the main menu of the Control Center. Select **Dr.Web Server Task Scheduler** in the control menu of the window that opens. The list of Dr.Web Server tasks will open.
2. To manage the schedule, use the corresponding elements from the toolbar:
   a) General elements on the toolbar are used to create new tasks and manage the schedule section. These tools are always available on the toolbar.

   Add tasks from default schedule—add all tasks from the default schedule to the current schedule. All current tasks on the list are preserved, and all tasks from the default schedule are added to them. The default schedule tasks are added in any case, even if the current schedule already contains these tasks (original or modified), or fully coincides with the default schedule.

   Set default schedule—remove all tasks from the current schedule and set the default task schedule.

   The default schedule is a list of tasks that are created during the initial Dr.Web Server installation. This schedule cannot be changed.

   Create task—add a new task. This action is described in detail below, in the Task Editor section.

   Export settings from this section to the file—export schedule to a file of a special format.

   Import settings to this section from the file—import schedule from a file of a special format.

   Import of the Task Scheduler list for Dr.Web Server into the Task Scheduler for workstations and vice versa is not allowed.

   b) To manage existing tasks, set flags next to the necessary tasks or in the table header to select all tasks from the list. The following elements on the toolbar for managing the selected tasks become available:

Option		Action
Run type	**Synchronous type**	Run all tasks marked below synchronously. The task with the specified periodicity will be placed in the general queue of the Scheduler tasks to be executed sequentially.
	Asynchronous type	Run all tasks marked below asynchronously. The task with the specified periodicity will be executed in parallel with other tasks, out of turn.

Option		Action
Status	**Enable execution**	Activate execution of the selected tasks according to their schedule, if they were disabled.
	Disable execution	Disable execution of the selected tasks. Tasks remain on the list but will not be executed according to the schedule.
 The same option can be set in the task editor on the **General** tab by setting the **Enable execution** flag.		
Severity	**Make critical**	Perform an extra execution of the task if the scheduled execution is skipped.
	Make noncritical	Execute the task only at the scheduled time regardless of whether its execution has been skipped or not.
 The same option can be set in the task editor on the **General** tab by setting the **Critical task** flag. The reason for missing the launch of a critical task may be, for example, that Dr.Web Server is turned off. Executing another task is not the reason for missing the task start.		
Duplicate settings		Duplicate tasks that are selected in the current schedule. When you use the **Duplicate settings** option, new tasks are created with the same settings as the selected tasks.
Schedule to repeat		For tasks which are executed once: execute the task one more time according to the specified time settings (see how to change how many times a task is executed below, in the Task Editor section).
Remove selected tasks		Remove the selected task from the schedule.
Execute task		Execute the tasks selected on the list immediately. A task will be launched even if it is disabled for execution on a schedule.
Edit task		Change task parameters. The **Task editor** window described below opens.

Task Editor

The **Task Editor** allows you to specify settings to:

1. Create a new task.

   Click **Create task** on the toolbar.

2. Edit an existing task.

   Click the name of one of the tasks on the task list and click **Edit task** on the toolbar.

A window for editing a task will open. The settings for editing an existing task are the same as the settings for creating a new task.

Values of fields marked with the * character must be specified.

To edit task settings

1. On the **General** tab in the **General** section, specify the following parameters:
   - In the **Name** field, specify the name of the task that will be displayed in the schedule list.
   - Set the **Enable execution** flag to enable the task execution. If the flag is cleared, the task remains in the list but will not be executed according to the schedule.

The same option can be set in the main window of the Scheduler via the **Status** toolbar option.

   - Set the **Critical task** flag to perform an extra execution of the task if its scheduled execution is skipped for any reason. The Scheduler rechecks the task list every minute and executes any skipped critical task if it is found. If the task has been skipped several times at the moment of its execution, it will be executed only once.

The same option can be set in the main window of the Scheduler via the **Severity** toolbar option.

   - If the **Run the task asynchronously** flag is cleared, the task will be added to the general queue of Scheduler tasks that are executed sequentially. Set the flag to execute this task in parallel to the queue.
2. In the **Time** section, specify the task launch parameters:
   - In the **Periodicity** drop-down list, select when the task will be executed according to the specified periodicity:

Execution type	Parameters and description
Shutdown	The task will be launched at the Dr.Web Server shut down. No additional parameters required to run the task.
Startup	The task will be executed at Dr.Web Server startup. No additional parameters are required to run the task.
N minutes after initial task	In the **Initial task** drop-down list, select the task in relation to which the execution time of the current task is set.

Execution type	Parameters and description
	In the **Minute** field, specify or select the number of minutes that should pass after the execution of the initial task to execute the task being edited.
Daily	Specify the hour and the minute for the task to be executed at.
Monthly	Specify the day of the month, the hour, and the minute for the task to be executed at.
Weekly	Select the day of the week, specify the hour and the minute for the task to be executed at.
Hourly	Specify a number from 0 to 59 to set the minute of every hour at which the task will be executed.
Every N minutes	The **N** value should be specified to set the time interval for the execution of the task. At **N** equal to `60` or more, the task will be run every **N** minutes. At **N** of less than `60`, the task will be run every minute of the hour multiple of **N**.

- Set the **Disable after the first execution** flag to execute the task only once at the specified time. If the flag is cleared, the task will be executed multiple times according to the specified periodicity.

To repeat the execution of a once executed task, use the **Schedule to repeat** option on the toolbar of the schedule section.

3. On the **Action** tab, in the **Action** drop-down list, select the type of the task and specify the task parameters needed to perform the task:

Task type	Parameters and description
Available licenses are close to the limit	The task is designed to send the **Number of stations in the group is close to the license limit** notification if the number of licenses in all keys assigned to the selected groups of stations is close to the end. License keys assigned of the selected groups can also be assigned to other licensing objects. Specify the following parameters: • **Number of available licenses**—maximum number of licenses left in the license keys assigned to the selected groups, at which the notification will be sent to the administrator. • **Percentage of available licenses**—maximum percentage of licenses left in the license keys assigned to the selected groups, at which the notification will be sent to the administrator.

Task type	Parameters and description
	• **Groups**—the list of groups which will be checked on the number of licenses left. Use CTRL and SHIFT to select several groups.
Back up critical Dr.Web Server data	The task is designed to backup the following critical data of Dr.Web Server: • database, • license key file, • private encryption key. Specify the following parameters: • **Path**—path to the directory where the data will be saved (blank field means that the default directory will be used). • **Maximum number of copies**—maximum number of backup copies (the 0 value means no limitation). For details see the **Appendices** document, p. Appendix G3.5. ⚠ Backup folder must be empty. Otherwise, the folder content will be deleted during the back up.

Back up repository	The task is designed for periodic backups of the repository.
	Specify the following parameters:
	• **Path**—full path of the directory where the backup copy will be stored.
	• **Maximum number of copies**—maximum number of repository backup copies which are stored by the task in the specified directory. If the maximum number of copies is reached, the oldest copy will be overwritten by the new one.
	• **Repository area** defines which part of information on anti-virus component will be saved:
	  ▫ **Entire repository**—save all revisions from the repository for the components that are selected in the list below.
	  ▫ **Only critical revisions**—only revisions marked as **Current** or **Stored** will be saved for the components that are selected in the list below. If there are no such revisions, only the revision marked as **Distributed** will be saved.
	  ▫ **Only configuration files**—only configuration files will be saved for the components that are selected in the list below.
	• Set the flags for the components selected areas of which will be saved.

Task type	Parameters and description
	 Backup folder must be empty. Otherwise, the folder content will be deleted during the back up.
Create statistic report	The task is designed to create a statistical report on the anti-virus network. For a report to be created, the **Statistic report** notification (see Notification Configuration) must be enabled in an active notification profile. The generated report is saved on the computer where Dr.Web Server is installed. Report delivery depends on the type of notification: • For messages delivered via **Email**: an email with the report attached as well as a link to the report location is sent to the mail address which is specified in the notification settings. • For all other methods of delivery: a notification with a link to the report location is sent. To create this task in the schedule, specify the following parameters: • **Report language**—language of the data in the report. • **Date format**—format of dates in the statistical data. The following formats are available: ▫ European: `DD-MM-YYYY HH:MM:SS` ▫ American: `MM/DD/YYYY HH:MM:SS` • **Report format**—format of the document containing the statistical report. • **Report period**—time period for which the statistics will be included in the report. • **Groups**—list of anti-virus network station groups the data on which will be included in the report. To select multiple groups, use the CTRL or SHIFT key. • **Report tables**—list of statistical tables the data on which will be included in the report. To select multiple tables, use the CTRL or SHIFT key. • **Report retention period**—time period for storing a report on the computer with running Dr.Web Server, starting from report generation.
Execute script	The task is designed for executing lua script which is specified in the **Script** field.  Simultaneous execution of tasks with **Execute script** type on several Dr.Web Servers, which use one database may result in errors. When running Lua scripts, administrator gets the access to all file system within the Dr.Web Server folder and some system commands on

Task type	Parameters and description
	a computer with Dr.Web Server installed. To forbid the access to the schedule, disable the **Edit Server schedule** permission for the correspondent administrator (see Administrators and Administrative groups).
License key expiration	The task is designed to issue reminders about the license expiration of Dr.Web product. You have to set the period preceding license expiration starting from which the reminders will be issuing.
Neighbor Dr.Web Server has not connected for a long time	The task is designed to issue notifications in case the neighbor Dr.Web Servers have not been connected to the current Dr.Web Server for a long time. Notifications display settings can be configured in the Notification Configuration section using the **Neighbor server has not been connected for a long time** item. Set values in the **Hours** and **Minutes** fields to define a time period after which the neighbor Dr.Web Server will be considered as not connected for a long time.
Purge database	The task is designed to collect and purge unused records in the Dr.Web Server database using the `vacuum` command. No additional parameters required to run the task.
Purge expired stations	Specify the period after which the stations with expired access should be purged. You can view the date (day, month, year) when the station has the access to Dr.Web Server, in the station properties (on the **General** tab, the **Expiration date** field displays the certain date or **Never** to disable limitations). If the period is set to 0 days, all expired stations will be considered obsolete and deleted when the task is executed.
Purge old records	The task is designed to purge outdated information from the database. The types of

Task type	Parameters and description
	deleted records is given in the task parameters. You have to specify the number of days after which the records in the database are considered outdated and purged from Dr.Web Server. The period after which the records are purged is specified for each type of records separately. Records for which the period is set to 0 days will be considered outdated and deleted when the task is executed.
Purge old stations	The task is designed to purge outdated stations. You have to specify the time period (90 days by default) after which all stations that have not been connected to Dr.Web Server, are considered old and are moved to the **Deleted** group of the anti-virus network. The final deletion of such stations from the Dr.Web Server database is performed at execution of the **Purge old records** task (the time period of deleting the stations from the **Deleted** group is set in the **Purge old records** task parameters, for the **Deleted stations** type and counted from the moment of moving to the **Deleted** group). Outdated information is purged from the database to save disc space. The period in the **Purge old records** and **Purge old stations** tasks by default is 90 days. If you decrease the value, the statistics on the operation of the anti-virus network components will be less representative. If you increase the value, Dr.Web Server may need extremely more resources.
Purge outdated messages	The task is designed for purging the following messages from the database: • agent notifications, • notifications for the web console, • reports created according to the schedule. This also purges messages marked as obsolete, i.e. with expired retention period which can be configured: • for notifications: for appropriate sending method while creating a notification (see Notification Configuration). • for reports: in a task for creating reports. No additional parameters required to run the task.
Purge unactivated stations	Specify the period after which the unused station accounts should be purged. You can view the list of unused station accounts in the hierarchical list of the anti-virus

Task type	Parameters and description
	network, in the **Status** → **New** group (see the New Stations Approval Policy section for more details). If the period is set to 0 days, all non-activated stations will be considered obsolete and deleted when the task is executed.
Purge unsent events	The task is designed to purge unsent events from the database. You have to set the period for storing unsent events after which they will be purged. This refers to events that a subordinate Dr.Web Server sends to a master Dr.Web Server. If sending a message fails, it is moved to the unsent message list. A subordinate Dr.Web Server continues its attempts to send the message at the specified interval. When the **Purge unsent events** task is run, events will be purged if their storage time has reached and exceeded specified period.
Replace encryption key	The task is designed for periodic replacement of the following tools providing encryption between components: • the `drwcsd.pri` private key on Dr.Web Server, • the `*.pub` public key on workstations, • the `drwcsd-certificate.pem` certificate on workstations. Because some workstations can be turned off at the time of replacement, the procedure is divided into two steps. You have to create two tasks to perform each one of these steps, it is recommended to perform the second step some time after the first one, when certain stations will probably connect to Dr.Web Server. When creating a task, select the appropriate step from the drop down list: • **Adding a new key**—the first step of the procedure when the new inactive encryption key pair and certificate are created. The stations get the new public key and certificate upon the connection to Dr.Web Server. • **Deleting the old key and switching to the new key**—the second step when the stations are notified about switching to the new encryption keys and certificate, followed by replacing the existing tools with the new ones: public keys and certificate on the stations and a private key on Dr.Web Server. If for any reason some stations did not receive the new public key and the certificate, they will not be able to connect to Dr.Web Server. To resolve this problem, manually put the new public key and certificate on the station (you can view the procedure of replacing the key on station in the **Appendices** document, p. Connecting Dr.Web Agent to Other Dr.Web Server).

Task type	Parameters and description
Restart Dr.Web Server	The task is designed to restart Dr.Web Server. No additional parameters required to run the task.
Run program	The task is designed to run custom program. Programs launched under this task are executed in the background. Specify the following parameters: • The **Path** field—full name (with the path) of the program executable file to run. • The **Arguments** field—command line parameters to run the program. • Set the **Wait for the completion of the program** flag to wait for the completion of the program which has been launched by this task. At this, Dr.Web Server logging the start of the program, the returned code and the time of the program end. If the **Wait for the completion of the program** flag is cleared, the task become completed right after the launch of the program and the Dr.Web Server logging only the start of the program.
Send a message to station	The task is designed to send arbitrary message to users of a station or group of stations. A message settings are given in the Sending Notifications to Stations section.
Shut down Dr.Web Server	The task is designed to shut down Dr.Web Server. No additional parameters required to run the task.
Station has not connected for a long time	The task is designed to issue notifications in case the stations have not been connected to the current Dr.Web Server for a long time. Notifications display settings can be configured in the Notification Configuration section using the **Station has not been connected for a long time** item. In the **Days** field specify a time period after which the station will be considered as

Task type	Parameters and description
	not connected for a long time.
Synchronization with Active Directory	The task is designed to synchronize network structures: Active Directory containers which contains computers become groups of anti-virus network to which workstations are placed. Specify the following parameters: • **Active Directory controller**—Active Directory controller, e.g. `dc.example.com`. • **Login**—Active Directory user login. • **Password**—Active Directory user password. For Dr.Web Servers under Windows OS, settings of Active Directory search are not obligatory. Information of a user on whose behalf the Dr.Web Server process is run (usually, it is LocalSystem) is used as a default registration information. For Dr.Web Servers under Unix-like OS, the settings must be obligatory specified. • In the **Connection security** drop-down list, select the type of encrypted data exchange: ▫ **Use data encryption**—switching to a secure encrypted LDAP connection is performed using the `STARTTLS` command. By default, a connection is established via TCP or UDP protocol using port 389. ▫ **Use SSL**—establish a new secure LDAPS connection. By default, a connection is established via TCP protocol using port 636. ▫ **No**—do not use encryption. Data exchange will be performed over an unprotected LDAP connection via TCP protocol using port 389. The task is disabled by default. To activate the task execution, set the **Enable execution** option in the task settings or on the toolbar as described above. After completing the task, you can assign special Office Control settings for users and groups from Active Directory (**Office Control** → **Group settings** → **Access settings** → **Per-group settings**).
Update repository	The task is designed to launch the update of repository products from GUS. Specify the following parameters:

Task type	Parameters and description
	• In the **Product** list, set the flags next to those repository products which will be updated by this task. • Set the **Update license keys** to activate the procedure of license keys automatic update during repository update. Detailed information is given in the Automatic License Renewal section.
Wake stations	The task is designed to turn on stations, for example before running the scanning task. The following task parameters define which stations will be turned on: • **Wake all stations**—every station which is connected to Dr.Web Server will be turned on. • **Wake stations by specified parameters**—only stations that accord to the parameters below will be turned on: ▫ **IP addresses**—the list of IP addresses of the stations that will be turned on. The list is specified in the following format: 10.3.0.127, 10.4.0.1-10.4.0.5, 10.5.0.1/30. Use comma or newline to separate several addresses. You can also use DNS names of the stations instead of their IP addresses. ▫ **MAC addresses**—the list of MAC addresses of the stations that will be turned on. The MAC-address octets have to be separated by the ':' sign. Use comma or newline to separate several addresses. ▫ **Groups**—the list of groups of the stations that will be turned on. To edit the groups list, click **Edit** (or the group identifier if groups are already set) and select necessary groups in the opened window. Use CTRL and SHIFT to select several groups. ⚠ To run this task, all stations that are going to be turned on should be equipped with network cards with Wake-on-LAN support. To check whether your network card supports Wake-on-LAN, please refer to its documentation or see its properties (**Control Panel** → **Network and Internet** → **Network Connections** → **Change Adapter Settings** → **Configure** → **Advanced**, and for the **Wake on Magic Packet** property, set the **Value** → **Enabled**).
Write to log file	The task is designed to write to the Dr.Web Server log file specified string. **String**—message to be logged.

4. When all parameters for the task are specified, click **Save** to accept changes of edited parameters if you are editing an existing task, or to create a new task with specified parameters if you created a new task.

The result of task execution is displayed as a table in the **Administration** → **Tasks execution log** section.

10.7. Setting the Web Server Configuration

After each saving of changes in the **Web server configuration** section, the backup copy of the previous version of the web server configuration file is saved automatically. Only 10 last copies are stored.

Files are placed in the same folder as the configuration file itself and named according to the following format:

`webmin.conf_<creation_time>`

You can use created backup copies, particularly to restore the configuration file if the Control Center interface is not available.

To set the configuration parameters of the Web server

1. Select the **Administration** item in the main menu of the Control Center.
2. Select **Web server configuration** in the control menu. A window with Web server configuration will be opened.

Values of fields, marked with the * sign, must be obligatory specified.

3. On the toolbar, the following buttons to manage the section settings are available:

 **Restart Dr.Web Server**—restart Dr.Web Server to apply changes that have been specified in this section. The button become enabled after you specified the changes in the section settings ans click **Save**.

 **Restore configuration from the backup**—drop-down list with the backup of all section settings, which you can restore after making changes. The button become enabled after you specified the changes in the section settings ans click **Save**.

 **Reset all parameters to initial values**—restore the values that all parameters in this section had before current editing (last saved values).

 **Reset all parameters to default values**—restore default values of all parameters in this section.

4. To apply the changes specified in the section settings, click **Save**, after this Dr.Web Server must be rebooted. To do this, click  **Restart Dr.Web Server** on the toolbar of this section.

10.7.1. General

On the **General** tab, specify the following Web server settings:

- **Dr.Web Server address**—IP address or DNS name of Dr.Web Server.

  Parameter is specified in the following format:

  <Dr.Web Server IP address or DNS name> [**:** *<port>*]

  If the Dr.Web Server address is not specified, computer name returned by the operating system or the Dr.Web Server network address: DNS name, if available, otherwise—IP address are used.

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

  If the port number is not specified, the port from a request is used (e.g., for requests to Dr.Web Server from the Control Center or via the **Web API**). Particularly, for the requests from the Control Center it is the port specified in the address line for connection of the Control Center to Dr.Web Server.
- **Number of parallel requests from clients**—number of parallel requests processed by the Web server. This parameter affects server performance. It is not recommended to change this parameter without need.
- **IO threads number**—number of threads serving data transmitted in network. This parameter affects the Dr.Web Server performance. It is not recommended to change this parameter without need.
- **time-out of HTTP/1 session (sec.)**—HTTP version 1 protocol session time-out. For persistent connections, Dr.Web Server releases the connection, if there are no requests received from a client during specific time slot. time-out is relevant before the first data exchange within the session.
- **Minimal send rate via HTTP/1 (BPS)**—minimal acceptable data send rate. If outgoing network speed is lower than this value, connection will be rejected. Specify 0 to ignore this limit.
- **Minimal receive rate via HTTP/1 (BPS)**—minimal acceptable data receive rate. If incoming network speed is lower than this value, connection will be rejected. Specify 0 to ignore this limit.
- **Send time-out for HTTP/1 (sec.)**—data send time-out within opened session on HTTP/1 protocol. If unable to send data during specific time slot, the session is closed.
- **Receive time-out for HTTP/1 (sec.)**—Data receive time-out within opened session on HTTP/1 protocol. If there are no requests received from a client during specific time slot, the session is closed. time-out is relevant after the first data exchange within the session.
- **Send buffer size (KB)**—size of buffers used when sending data. This parameter affects server performance. It is not recommended to change this parameter without need.

- **Receive buffer size (KB)**—size of buffers used when receiving data. This parameter affects server performance. It is not recommended to change this parameter without need.
- **Max request length (KB)**—Maximum allowed size of HTTP request.
- **Enable flood attack protection**—set the flag to provide protective measures against flood attacks. Specify the following parameters of attack detection:
  - **Period (sec)**—time period in seconds during which the certain number of requests must be received to confirm the flood attack from the client.
  - **Requests number**—the minimum number of requests that must be received during certain time period to confirm the flood attack from the client.
  - **Ban duration (sec)**—connections from the client will be prevented for the specified number of seconds.

In the **Compression** section, you can specify parameters of a traffic compression for data transmission over a communication channel with the Web server via HTTP/HTTPS:

- **Maximal response size to compress (KB)**—maximal size of HTTP responses which will be compressed. Specify the 0 value to disable limitation on maximal size of HTTP responses to be compressed.
- **Minimal response size to compress (B)**—minimal size of HTTP responses which will be compressed. Specify the 0 value to disable limitation on minimal size of HTTP responses to be compressed.
- **Priority order of compression types**:
  - **Defined by client**—priority order of compression types is defined by a client considering the allowed compression types.
  - **Defined by server**—priority order of compression types is defined by the server considering the allowed compression types. In this case, specify the using order of compression types in the list below. To change the order, drag and drop corresponding block over the root.

  You can enable or disable and also set the order of use (if the order is defined by Dr.Web Server) the following compression types:
  - **Use GZIP compression**—set the flag to use this type of compression. In the **GZIP compression level** field, specify the value in the range 0-9. The 0 value disables compression.
  - **Use Deflate compression**—set the flag to use this type of compression. In the **Deflate compression level** field, specify the value in the range 0-9. The 0 value disables compression.
  - **Use Brotli compression**—set the flag to use this type of compression. In the **Brotli compression level** field, specify the value in the range 0-11. The 0 value disables compression.
- **Replace IP addresses**—set the flag to replace IP address with DNS names of computers in the Dr.Web Server log file.
- **Enable HTTP/2 support**—set the flag to support connections with the web server via HTTP protocol version 2.

  - **Time-out of HTTP/2 session (sec.)**—HTTP version 2 protocol session time-out. For persistent connections, server releases the connection, if there are no requests received from a client during specific time slot.
- **Keep-alive TLS connection**—set the flag to use keep-alive TLS connection. Older browsers may not work properly with regular TLS connections. Disable this parameter, if you have problems with TLS protocol.
- **Certificate**—path to TLS certificate file. The drop-down list contains available certificates from the Dr.Web Server folder.

Only PEM files with no empty lines between the header and body of the certificate are allowed. The file may be a certificate or a certificate chain.

- **SSL private key**—path to TLS private key file. The drop-down list contains available private keys from the Dr.Web Server folder.
- **Encryption key for TLS session tickets**—the path to encryption key for TLS session tickets. Used to resume a TLS session based on session tickets which are encrypted using the specified key.
- **Allowed cipher list**—the string defining the list of ciphers from OpenSSL package that allowed for use in client connections. Leave the field blank to use the `DEFAULT` value that means `ALL:!EXPORT:!LOW:!aNULL:!eNULL:!SSLv2`.

10.7.2. Additional

On the **Additional** tab, specify the following Web server settings:

- Set the **Show script errors** flag to display script errors in your web browser. This parameter is used by Doctor Web's technical support and developers. It is recommended that you do not change it, unless absolutely necessary.
- Set the **Trace scripts** flag to enable script tracing. This parameter is used by Doctor Web's technical support and developers. It is recommended that you do not change it, unless absolutely necessary.
- Set the **Abort scripts** flag to allow aborting the scripts. This parameter is used by Doctor Web's technical support and developers. It is recommended that you do not change it, unless absolutely necessary.
- Using the fields in the **Custom HTTP headers** section, you can add your own Web server HTTP response headers with any necessary values. The Web server uses three pre-installed custom security headers by default: `X-XSS-Protection`, `X-Content-Type-Options`, and `X-Frame-Options`. You can view and edit their values in the `webmin.conf` configuration file located in the `etc` subfolder of the Dr.Web Server installation folder.

10.7.3. Transport

On the **Transport** tab, you can configure network addresses to listen for accepting incoming connections by the Web server, e.g., for connection of the Control Center or executing requests via the Web API:

In the **Addresses to listen** section, you can configure the list of interfaces to listen for accepting connections via the HTTP protocol:

- **Address**—the IP address of the network interface from which connections can be accepted.
- **HTTP port**—the port number of the network interface from which HTTP connections can be accepted.
- **HTTPS port**—the port number of the network interface from which HTTPS connections can be accepted.

  By default, the following parameters are set to "listen" by the Web server:
  - **Address**: `0.0.0.0`—use "all network interfaces" for this computer, on which the Web server is installed.
  - **HTTP Port**: `9080`—use the standard 9080 port for the HTTP protocol.
  - **HTTPS Port**: `9081`—use the standard 9081 port for the HTTPS protocol.

To add a new address line, click  in the corresponding section. To delete the specific address line, click  next to the deleting address.

10.7.4. Security

On the **Security** tab, you can configure restrictions for network addresses from which the Web server receives HTTP and HTTPS requests.

General

- Set the **Redirect to a secure connection** flag to automatically redirect all HTTP connections to HTTPS.
- Set the **Return detailed header** flag to return environment details in the “Server” header by the web server.
- Set the **Convert URI to lowercase** flag to convert all URI in requests to the web server to lowercase. Only a fragment of URI hierarchical part that contains path is converted.
- Set the **Enable access control for User Agents** flag to forbid the access to the Control Center interface for bots and other User Agents from the list below.

  Define the list of forbidden User Agents:
  - In the **User Agent name** field specify User Agent name to forbid the access to the Control Center interface. Case sensitive. If not set, the application URI is used.

- In the **Defining regular expression** field, specify regular expression defining the application to forbid the access to the Control Center interface.

Access Restiction

To setup access limitations for any of connection type

1. To allow the access by HTTP or by HTTPS from definite addresses, add them to the **HTTP: Allowed** or **HTTPS: Allowed** lists correspondingly.
2. To deny the access by HTTP or by HTTPS from definite addresses, add them to the **HTTP: Denied** or **HTTPS: Denied** lists correspondingly.
3. The addresses not included into any of the lists are allowed or denied depending on whether the **HTTP denial priority** and **HTTPS denial priority** flags are set: if the flag is set, the addresses not included into any of the lists (or included into both of them) are denied. Otherwise, such addresses are allowed.

To edit the address list

1. Specify the network address in the corresponding field and click **Save**.
2. The network address is specified as: <*IP-address*>/[<*prefix*>].

Lists for TCPv6 addresses will be available, if the IPv6 interface is installed on the computer.

3. To add a new field, click  in the corresponding section.
4. To delete a field, click  .

Examples of prefix usage:

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

   Containing 254 addresses.

   Host addresses look like: `195.136.12.*`
2. Prefix 8 stands for a network with a network mask: `255.0.0.0`

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

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

10.7.5. Modules

It is not recommended to change the settings of this section without technical support instructions.

In the **Modules** section, you can configure Lua scripts that are load as other web interface scripts execute.

- The **Script folder in search paths** drop-down list defines where to add the current directory (directory where currently executed script resides) in the list from the **Paths** section:
  - **first**—to the top of the list,
  - **last**—to the end of the list,
  - **do not use**—do not add at all.
- The **Masks** section specifies the list of masks using which Lua modules are searched on the paths specified in the **Paths** section.
- The **Paths** section specifies paths on which Lua modules from the **Masks** section are searched. Paths must be specified relative to the root folder of the web server.

For example:

The script from the `var-root/webmin/esuite/include/head.ds` will not be found without additional configuration in the **Modules** section.

Modules from the `ds-modules` or `webmin/vfs` directories will be found without additional configuration in the **Modules** section, because they are global modules, not web interface modules.

10.7.6. Handlers

It is not recommended to change the settings of this section, except **Access** and **Authorization** subsections, without technical support instructions.

In the **Handlers** section, you can configure the way how and in what environment client request will be processed.

General

Settings are available depending on the handles type.

For web sockets, necessary handler is selected depending on the **Protocol** attribute.

For the rest of handlers types, necessary handler is selected depending on the **Prefix** attribute.

Types of handlers to use are selected in the **Type** drop-down list:

- **Handlers**

  Selected script is executed with the path from URL as a parameter. If the path is absent, the path of the **Directory** field is used.

- **Prefix**—prefix of the path in the URL of HTTP request.
- **Directory**—directory in the root of the web server relative to which the paths to the files to be transferred are considered.
- **Script**—processing script.

- **Mixed handlers**

  Depending on the type of the requested file, behaves like the **Static files** type or the **Scripts** type.
  - **Prefix**—prefix of the path in the URL of HTTP request.
  - The list of index files. Defines which files in what order will be downloaded if web client requests a directory index.
  - **Script**—the list of file extensions to consider as Lua scripts.

- **Scripts**

  Any requested file is executed as Lua script.
  - **Prefix**—prefix of the path in the URL of HTTP request.
  - **Directory**—directory in the root of the web server relative to which the paths to the files to be transferred are considered.

- **Static files**

  Files content is given as it is.
  - **Prefix**—prefix of the path in the URL of HTTP request.
  - **Directory**—directory in the root of the web server relative to which the paths to the files to be transferred are considered.
  - The list of index files. Defines which files in what order will be downloaded if web client requests a directory index.

- **Virtual file system**

  Analogue of the **Static files** type, but files are loaded from the archive of the `dar` internal format, specified in the **Directory** field.
  - **Prefix**—prefix of the path in the URL of HTTP request.
  - **Directory**—directory in the root of the web server relative to which the paths to the files to be transferred are considered.

- **Predefined web sockets**

  Websocket application implemented by the shared library supplied with the server (`dll` or `elf shared object`). The library file name corresponds to web socket protocol, files are located in`lib-root/websockets`.

- **Authorization script**—name of the Lua script file that authorizes a user.
- **Protocol**—the `WebSocket-Protocol` field value that is transmitted in the HTTP request for connection to web socket.

- **User-defined web**

  Websocket application implemented by the Lua script. The script file name corresponds to web socket protocol, files are located in`home-root/websockets`.

  - **Authorization script**—name of the Lua script file that authorizes a user.
  - **Protocol**—the `WebSocket-Protocol` field value that is transmitted in the HTTP request for connection to web socket.

Access

Access Control Lists (ACL) specify restrictions for network addresses from which clients will be able to access the web server.

Settings are the same as Dr.Web Server security settings.

If the settings are not specified, all addresses are allowed.

Authorization

Available for all types of hadlers except web sockets.

The section settings define the list of resources for requests to which the basic http authentication must be requested from the web client.

- **Realm**—value that the web server passes to a client in the `WWW-Authenticate: Basic realm="ADMIN"` parameter. Generally, it is a short description of who should be authorized. It has not relation with a login.

To setup access limitations for any of connection type

1. To allow free access at clients connection via HTTP or HTTPS to a certain paths, add these paths to the **HTTP: free access** or **HTTPS: free access** lists correspondingly.
2. To request authorization at clients connection via HTTP or HTTPS to a certain paths, add these paths to the **HTTP: require authorization** or **HTTPS: require authorization** lists correspondingly.
3. When accessing paths that are not included into any of the lists, authorization is requested or not depending on whether the **Authorization request priority** flag is set: if the flag is set, to access paths not included into any of the lists (or included into both of them) authorization is required. Otherwise, access to such paths is free.

To edit the address list

1. Specify a regular expression that defines the path relative to the directory specified in the **Directory** field.
2. To add a new field, click  in the corresponding section.
3. To delete a field, click  .

10.8. User Hooks

When running Lua scripts, administrator gets the access to all file system within the Dr.Web Server folder and some system commands on a computer with Dr.Web Server installed.

To forbid the access to the user hooks, disable the **Edit Dr.Web Server configuration and repository configuration** permission for the correspondent administrator (see Administrators and Administrative groups).

User hooks, implemented as a Lua scripts, are meant for automation of the administrator work enabling quicker performance of certain tasks of Dr.Web Server.

User hooks are located in the following subfolder of the Dr.Web Server installation folder:

- for Windows OS: `var\extensions`
- for FreeBSD OS: `/var/drwcs/extensions`
- for Linux OS: `/var/opt/drwcs/extensions`

After the Dr.Web Server installation, pre-installed user hooks are located in this folder.

It is recommended to edit user hooks via the Control Center.

Before updating Dr.Web Server, save user procedures and scripts. Please note that when upgrading to a newer version of Dr.Web Server, user procedures and scripts that worked in the previous version may not work. If a problem occurs, contact technical support.

To configure user hooks execution

1. Select the **Administration** item in the main menu of the Control Center.
2. In the opened window, select the **User hooks** item in the control menu. User hooks settings window will be opened.

A detailed description of user procedures and their parameters is given in **Appendices**, Appendix M. User Hooks.

Hooks Tree

Hooks hierarchical list displays the tree view, nodes of which are hook groups and user hooks included into them.

Initially, hooks tree contains the following pre-installed groups:

- **Examples of the hooks**—contains templates of all available user hooks. On the base of these templates you can create your own user hooks. You cannot edit or execute the hook templates.
- **IBM Syslog**—contains templates of user hooks used in integration with IBM Tivoli system. Events corresponding to the enabled hooks, are written in the *Syslog* format.

  All events are written into one file on the following path:
  - for Windows OS:
    `var\export\tivoli\syslog\drwcs_syslog.log`
  - for FreeBSD OS:
    `/var/drwcs/export/tivoli/syslog/drwcs_syslog.log`
  - for Linux OS:
    `/var/opt/drwcs/export/tivoli/syslog/drwcs_syslog.log`
- **IBM W7Log**—contains templates of user hooks used in integration with IBM Tivoli system. Events corresponding to the enabled hooks, are written in the *IBM W7Log XML* format.

  For each event, the separate file is created on the following path:
  - for Windows OS:
    `var\export\tivoli\w7log\<event_name>_<unix_timestamp>`
  - for FreeBSD OS:
    `/var/drwcs/export/tivoli/w7log/<event_name>_<unix_timestamp>`
  - for Linux OS:
    `/var/opt/drwcs/export/tivoli/w7log/<event_name>_<unix_timestamp>`

The icon of the tree element depends on the type and status of this element (see table 10-6).

Table 10-6. Icons of elements in the hooks tree

Icon	Description
Hooks groups	
	Hooks group for which hook execution is enabled.
	Hooks group for which hook execution is disabled.
Hooks	
	Hook is enabled to execute.
	Hook is disabled to execute.

Hooks Tree Managing

To manage objects in the hooks tree, use the following elements of the toolbar:

—drop-down list for adding an element to the hooks tree:

Add hook—add a new user hook.

Add hooks group—add a new user group for placing hooks in it.

Remove selected objects—remove user hook or hooks group which is selected in the hook tree.

Enable hook execution—the same action is performed in the hooks editor if you set the **Enable hook execution** flag. See also Hooks activating.

Disable hook execution—the same action is performed in the hooks editor if you clear the **Enable hook execution** flag. See also Hooks activating.

Hooks Groups Managing

To create a new group

1. On the toolbar, select → **Add hooks group**.
2. In the opened window, specify the following parameters:
   - Set the **Enable hook execution** flag to activate hooks which will be included into this group. See also Hooks activating.
   - In the **Group name** field, specify an arbitrary name for the creating group.
3. Click **Save**.

To change the order of groups using

1. In the hooks tree, drag and drop the hooks group and place it in the necessary order relative to the other groups.
2. The order of hooks usage is automatically changed after changing groups order: the first will be performed the hooks from the groups that are placed higher in the hooks tree.

To move a hook to the other group

1. In the hooks tree, select a hook you want to move.
2. On the opened properties pane, in the **Parent group** drop-down list, select the group into which you want to move the hook.
3. Click **Save**.

Hooks Managing

To create a new hook

1. On the toolbar, select → **Add hook**.
2. In the opened window, specify the following parameters:
   - Set the Enable **hook execution** flag to activate the creating hook. See also Hooks activating.
   - In the **Parent group** drop-down list, select the group into which you want to place the creating hook. Further, you can move the hook into other group—see above.
   - In the **Hook** drop-down list, select the hook type. The hook type defines an action for which the hook will be called.
   - In the **Hook text** field, enter the Lua script which will be executed when the hook called. The **Information on hook** subsection contains an action for which the hook will be called; information whether the Dr.Web Server database is available or not for this hook; and also contains the lists of input parameters and returned values for this type of hook.
3. Click **Save**.

To edit a hook

1. In the hooks tree, select a hook you want to edit.
2. In the right part of the window, the properties pane for this procedure automatically opens. You can edit all parameters which are specified on creating the hook except the **Hook** parameter. This parameter defines an action for which the hook will be called, and cannot be edited after the hook has been created.
3. Click **Save**.

Hooks Activation

Activation of hooks and hooks groups defines whether the hooks will be executed on corresponding event or not.

To activate a hook or a group of hooks

1. In the hooks tree, select a hook or a hooks group you want to activate.
2. Perform one of the following actions:
   - On the toolbar, click **Enable hook execution**.
   - In the right part of the window on the properties pane of the selected object, set the **Enable hook execution** flag if it is cleared. Click **Save**.

Hooks activation features

To execute a hook on corresponding event, the following is necessary:

a) the hook itself must be activated;

b) the group that contains the hook must be activated.

> If a hooks group is disabled, its hooks will not be executed even if they are activated.
>
> On group activating, only whose hooks will be executed that are directly activated.

10.9. Message Templates

In the **Message template** section contains the templates list of arbitrary text messages sent by administrator to stations of the anti-virus network (see Sending Notifications to Stations).

Messages can get into the templates list by one of the following ways:

1. A template can be created based on messages which were once sent by the administrator. You can create such template in the Message Log section.
2. A completely new template can be created. To do this, click **Create template** on the toolbar in the **Message templates** section. The message settings are the same as in the Sending Notifications to Stations section.

To manage message templates, use the following toolbar options:

Delete—delete selected message templates.

Create template—create a new message template (see above).

Edit—edit the settings of an existing template. The option is available only if one template in the list is selected.

Send message to stations—send one of several messages to station based on templates selected in the list (see below).

To send a single message

1. Set the flag next to the message template you want to send.
2. Click **Send message to stations**.
3. The **Sending a message** window opens. Specify the following settings:
   a) In the **Anti-virus network** tree, select receivers of the message from the given list—whether separate stations or groups of stations.
   b) The message settings are the same as in the Sending Notifications to Stations section.
4. Click **Send**.

To send multiple messages

1. Set the flag next to the message templates you want to send.
2. Click **Send message to stations**.
3. The **Sending multiple messages** window opens. The **List of messages** section contains the list of all message you have select for resending. The names of the messages correspond to their templates names.
4. Click **Send all**, to send all messages from the list.
5. To edit a message from the list, select it in the **List of messages** section. In the **Message settings** section, specify the following parameters:
   a) In the **Anti-virus network** tree, select receivers of the message from the given list—whether separate stations or groups of stations.
   b) The message settings are the same as in the Sending Notifications to Stations section.
   c) To remove the selected message from the sending list, click **Remove**.

10.10. Setting Notifications

Dr.Web Enterprise Security Suite can send notifications about detected threats, anti-virus network component states and other events to administrators of Dr.Web Enterprise Security Suite anti-virus network.

10.10.1. Notification Configuration

To configure notifications on anti-virus network events

1. Select the **Administration** item in the main menu of the Control Center. In the window that opens, select **Notifications configuration** in the control menu.
2. Notifications are configured separately for each Control Center administrator. The name of the administrator whose notification settings are displayed is given in the **Administrator who receives notifications** field. To configure notifications for another administrator, click and select the administrator in the window that opens.
3. At initial setup, one default notification block (profile) is added for the main **admin** administrator. If the administrator notification list is empty, click **Add notification** in the **Notification list** section.
4. To enable notification sending, set the toggle button to the left of the notification block header to the corresponding position:
   —notifications from this block are sent.
   —notifications from this block are not sent.
5. You can create several notification blocks (profiles), for example, for different notification methods. To add one more block, click to the right of the notification block settings. A

notification block will be added at the bottom of the page. Different notification blocks are configured independently.

6. In the **Title** field, specify the name of the new notification block. This name is used, for instance, when configuring the **Create statistical report** task in the Dr.Web Server schedule. To edit the header after the block is created, click the header and enter the new name. If you have more than one notification block, when you click the header text, a drop-down list of headers of the existing notification blocks is shown.
7. To configure notification sending, select a notification method from the **Notifications send method** drop-down list:
   - Dr.Web Agent—send notifications via the Dr.Web Agent protocol.
   - Web console—send notifications to the Web console.
   - Email—send notifications via email.
   - Push-notifications—send push notifications to Dr.Web Mobile Control Center. This option is available in the **Notifications send method** drop-down list only after Dr.Web Mobile Control Center has been connected to this Dr.Web Server.
   - SNMP—send notifications via the SNMP protocol.
   - Syslog—send notifications via the Syslog protocol.

   Descriptions of settings for each notification type are given further in this section.
8. In the list of notifications, set the flags next to those notifications that will be sent via the notification method of the current notification block.
9. Notifications use texts from predefined notification templates.

A description of the predefined notifications and their parameters is given in the **Appendices** document, in Appendix C2. The Parameters of Notification Templates.

To change a notification template:

a) Click **Switch to notification editing mode** in the section header.

b) Click the notification you want to edit. The notification template will open.

c) If necessary, edit the notification text. You can use template variables (in braces) in the notification text. To add variables, use the drop-down lists in the upper part of the window. When a message is generated, the system replaces the template variables with text strings as defined by the current configuration. The list of available variables is given in the **Appendices** document, C2. The Parameters of Notification Templates.

   To restore the default template values, click **Default template**.

d) After making all necessary changes, click **Exit notification editing mode** in the section header.

For the **SNMP** notification method, the notification template texts are set on the receiver's side (*management station* in RFC 1067 terms) and thus cannot be edited via the Control Center.

10. For notifications from the **Station** subsection, you can specify groups of stations on whose events notifications will be sent.
    a) Click to the left of a notification.
    b) Select groups of stations to monitor events and send corresponding notifications about in the **Groups of monitored stations** tree. To select several groups, use CTRL or SHIFT.
    c) After selecting all the groups you want, click **Save**.
11. Click **Save** to apply all changes.

A separate set of templates is stored for each language. To edit templates for multiple languages, changes must be made for each language separately.

When updating Dr.Web Server, texts of predefined templates can also be updated. To keep the default template text unchanged:

1. make changes to the required template, thus unlocking the saving mechanism,
2. save them,
3. delete the changes,
4. save the template again.

Thus, the template will become personalized and will not be changed during the update.

Notifications via the Dr.Web Agent protocol

For notifications via the Dr.Web Agent protocol, specify the following parameters:

- In the **Resend by Dr.Web Server** section, specify the settings for notification resend attempts performed by Dr.Web Server when a message fails to send:
  - **Number**—number of resend attempts performed by Dr.Web Server when a message fails to send. The default is 10.
  - **Time-out**—period in seconds after which Dr.Web Server attempts to send the message again. The default is 300 seconds.
- **Stations**—list of stations and groups of stations to which notifications are sent. To edit the list, click **Edit**, select the stations and station groups you want in the tree, then click **Apply**.
- **Send test message**—send a test message using the specified settings of the notification system.

Notifications displayed in the Web console

For notifications displayed in the Web console, specify the following parameters:

- In the **Resend by Dr.Web Server** section, specify the settings for notification resend attempts performed by Dr.Web Server when a message fails to send:
  - **Number**—number of resend attempts performed by Dr.Web Server when a message fails to send. The default is 10.

- **Time-out**—period in seconds after which Dr.Web Server attempts to send the message again. The default is 300 seconds.

- **Notification storing time**—time period for storing a notification starting from the moment it is received. The default is 1 day. After the specified period the notification is marked as outdated and deleted according to the **Purge outdated messages** task in the Dr.Web Server schedule settings.

  You can specify an unlimited storage period for notifications of this type in the Web Console Notifications section.

- **Send test message**—send a test message using the specified settings of the notification system.

Notifications via email

For email notifications, specify the following parameters:

- In the **Resend by Dr.Web Server** section, specify the settings for notification resend attempts performed by Dr.Web Server when a message fails to send:
  - **Number**—number of resend attempts performed by Dr.Web Server when a message fails to send. The default is 10.
  - **Time-out**—period in seconds after which Dr.Web Server attempts to send the message again. The default is 300 seconds.
- **Recipient email addresses**—email addresses of notification recipients, one email address of a recipient per each field. To add one more recipient field, click  . To remove the field, click  .

  Parameters of email sending are configured in the **Administration** menu, in the **Dr.Web Server Configuration** section → **Network** tab → Email internal tab.

- **Send test message**—send a test message using the specified settings of the notification system.

You can also add custom headers in the **Headers** additional section of the template editor (see 9a above) for each email notification. Such headers may be used, for instance, in setting up email filters. Headers must be formed according to the RFC 822 and RFC 2822 standards and must not coincide with fields defined in the email standards. Particularly, the RFC 822 standard guarantees that its specification does not contain headers that start with `X-`; thus it is recommended to use the following naming format: `X-<header-name>`. For example: `X-Template-Language: English`.

To add or edit a header of a specific notification

1. Click **Switch to notification editing mode** in the section header.
2. Select **Email** from the **Notifications send method** drop-down list.
3. Click the notification you want to edit. The notification template will open.

4. Enter one or several headers in the `X-<name>: <value>` format in the **Headers** filed. You can use the template variables (in braces) provided in the drop-down lists in the upper part of the window in the header values. Headers must be separated by an empty line.
5. Click **Save**.
6. Click ✖ to close the template editor.
7. After making all necessary changes, click **Exit notification editing mode** in the section header.
8. Click **Save** to apply all changes.

You can also specify common headers for email notifications.

> ⚠ Common headers are added to all notifications sent via email. Once you add a common header, it is treated as a regular custom header, thus common headers cannot be mass edited separately from others. To edit or delete common headers, you must follow the general procedure for custom headers and edit each individual notification template.

To add a common header

1. Click **Edit common headers** in any email notification block.
2. Enter one or several headers in the `X-<name>: <value>` format in the **Common headers for all templates** window that opens. You can use the template variables (in braces) provided in the drop-down lists in the upper part of the window in the header values. Headers must be separated by an empty line.
3. Click **Add**. If the operation is successful, the text you entered disappears from the text field.
4. Click ✖ to close the template editor.
5. Click **Save** to apply all changes.

Example:

- Notification A has a custom header `X-Header-A: A`.
- Notification B has a custom header `X-Header-B: B`.

Once you add a common header `X-Header-C: C`:

- Notification A will have headers `X-Header-A: A`, `X-Header-C: C`.
- Notification B will have headers `X-Header-B: B`, `X-Header-C: C`.

To delete header `X-Header-C: C` from all notification templates, you must edit the templates of notifications A and B separately (see 9a above).

To remove or replace all custom headers of all notifications

1. Click **Edit common headers** in any email notification block.
2. Enter one or several headers in the `X-<name>: <value>` format in the **Common headers for all templates** window that opens. The new headers will replace all previously specified

headers for all email notifications. You can use the template variables (in braces) provided in the drop-down lists in the upper part of the window in the header values. Headers must be separated by an empty line.

To remove all previously specified headers, leave the field empty.

3. Click **Replace**. If the operation is successful, the text you entered disappears from the text field.
4. Click ✖ to close the template editor.
5. Click **Save** to apply all changes.

Example:

- Notification A has headers `X-Header-A: A`, `X-Header-C: C`.
- Notification B has headers `X-Header-B: B`, `X-Header-C: C`.

If you enter `X-Header-D: D` in the text field and click **Replace**:

- Notification A will have the header `X-Header-D: D`. The old headers will be deleted.
- Notification B will have the header `X-Header-D: D`. The old headers will be deleted.

If you leave the text field empty and click **Replace**:

- All notification A headers will be deleted.
- All notification B headers will be deleted.

Push notifications

For push notifications sent to the Mobile Control Center, specify the following parameters:

- In the **Resend by Dr.Web Server** section, specify the settings for notification resend attempts performed by Dr.Web Server when a message fails to send:
  - **Number**—number of resend attempts performed by Dr.Web Server when a message fails to send. The default is 10.
  - **Time-out**—period in seconds after which Dr.Web Server attempts to send the message again. The default is 300 seconds.
- **Send test message**—send a test message using the specified settings of the notification system.

Notifications via the SNMP protocol

For notifications via the SNMP protocol, specify the following parameters:

- In the **Resend by Dr.Web Server** section, specify the settings for notification resend attempts performed by Dr.Web Server when a message fails to send:
  - **Number**—number of resend attempts performed by Dr.Web Server when a message fails to send. The default is 10.

  - **Time-out**—period in seconds after which Dr.Web Server attempts to send the message again. The default is 300 seconds.
- In the **Resend by SNMP subsystem** section, pecify the settings for notification resend attempts performed by the SNMP subsystem when a message fails to send:
  - **Number**—number of resend attempts performed by the SNMP subsystem when a message fails to send. The default is 5.
  - **Time-out**—period in seconds after which the SNMP subsystem attempts to send the message again. The default is 5 seconds.
- **Receiver**—entity that receives SNMP requests. IP address or DNS name. You can enter only one receiver per field. To add another receiver field, click  . To remove a field, click  .
- **Sender**—entity that sends SNMP requests. IP address or DNS name (recognizable by the DNS server). An empty value is used by default.
- **Community**—SNMP community or context. The default is `public`.
- **Send test message**—send a test message using the specified settings of the notification system.

You can use the MIB provided with Dr.Web Server to get descriptions of OIDs during SNMP trap parsing. The `DRWEB-ESUITE-NOTIFICATIONS-MIB.txt` and `DRWEB-MIB.txt` files are located in the `etc` subfolder of the Dr.Web Server installation folder.

Notifications via the Syslog protocol

For notifications via the Syslog protocol, specify the following parameters:

- In the **Resend by Dr.Web Server** section, specify the settings for notification resend attempts performed by Dr.Web Server when a message fails to send:
  - **Number**—number of resend attempts performed by Dr.Web Server when a message fails to send. The default is 10.
  - **Time-out**—period in seconds after which Dr.Web Server attempts to send the message again. The default is 300 seconds.
- **Receiver**—address of the Syslog notification receiver. The transfer protocol is TCP or UDP. The default protocol is UDP, port 514.
- **Format**—notification format: RFC 5424, RFC 3164 or CEF (Common Event Format). The default is RFC 5424.
- **Receiver connection time-out (sec.)**—period in seconds during which Dr.Web Server attempts to connect to the notification receiver via TCP. The default is 5 seconds.
- **Facility**—represents the process which created a message (kernel, mail system, etc.). The value must be between 0 and 23. The default is 14.
- **Sender**—Dr.Web Server ID (FQDN, host name, IP address). The default value is empty.
- **Send test message**—send a test notification based on the specified settings.

10.10.2. Web Console Notifications

Via the Control Center, you can view and manage administrator notifications which are received via the **Web console** method (sending of administrator notifications is displayed in the Notification Configuration section).

To view and manage wen console notifications

1. Select the **Administration** item in the main menu of the Control Center. In the opened window, select **Web console notifications** in the control menu. The list of notifications which were sent to the Web console will be opened.
2. To view the notification, click corresponding row of the table. The window with notification texts will be opened. At this, notification will be automatically marked as read.
3. To manage notifications list using options on the toolbar
   a) To view notifications that were received during specific time period, use one of the following ways:
      - Select one of the predefined time periods from the drop-down list on the toolbar.
      - Select arbitrary dates of beginning and ending of time period from the drop-down calendars.

      After editing these settings values, click **Update** to view notifications list according to the specified settings.
   b) To manage separate notifications, set the flags next to the necessary notifications or the common flag in the table header to select all notifications from the list. At this, the following elements on the toolbar become available:

      Delete notifications—delete all selected notifications without possibility of restore.

      Mark notifications as read—mark all selected notifications as read.
   c) To manage specific notification types, set the flags next to the notifications of corresponding types. At this, the following elements on the toolbar become available:

      Unapproved stations—option is available only when you select notifications with the **Station is waiting for approval** type. In the drop-down list, you can approve the registration or deny the access to Dr.Web Server for stations from the selected notifications.

      Scan—option is available only when you select notifications with the **Epidemic in the network**, **Scan error**, **Security threat detected** types. In the drop-down list, you can specify the parameters of Dr.Web Scanner launch on stations from the selected notifications.

      Components management—option is available only when you select notifications with the **Critical error of station update** type. In the drop-down list, you can set the launch type of anti-virus software update on stations from the selected notifications.

      Reboot station—option is available only when you select notifications with the **Station reboot required to apply updates** type. The option initiates reboot of the stations from the selected notifications.

d) If necessary, you can export notifications into a file. Those notifications will be exported that are currently displayed in the table according to the time interval settings and the table columns filter (see 4.b).

To export notifications, click one of the following buttons on the toolbar:

Save data in CSV file,

Save data in HTML file,

Save data in XML file,

Save data in PDF file.

4. To manage notifications list using the options provided by the table

a) Set the **Store message without automatic deletion** icon next to those notifications that should not be deleted after expiration of storage period (storage period is set before sending notification in the Notification Configuration section in the **Web console** sending method settings). Such notifications are stored until you delete them manually in the **Web console notifications** section or clear the icon next to these notifications.

b) To display only specific notifications, click the header of a column you want to filter in the notifications table. In the opened menu, set the flags for notification parameters you want to display in the table.

The following sections are available for the filtering:

Column	Option	Action
Severity	**Critical**	Display only notifications only with the specified severity level. To display all notifications, set all the flags.
	High	
	Medium	
	Low	
	Minimal	
Source	**Agent**	Display notifications related to events on stations.
	Dr.Web Server	Display notifications related to events on Dr.Web Server.

c) To configure the table view, click the icon in the right corner of the table header. In the drop-down list, you can configure the following options:

- Enable or disable line wrapping for long messages.
- Select the columns to display in the table (selected by the flag next to its name). To show/hide the column, click the line with its name.
- Select the order of the columns in the table. To change the order, drag and drop corresponding column in the list to the needed place.

10.10.3. Unsent Notifications

Via the Control Center you can track and manage administrative notifications failed to be sent according to the settings of the Notification Configuration section.

To view and manage unsent notifications

1. Select the **Administration** item in the main menu of the Control Center. In the opened window, select **Unsent Notifications** in the control menu. The list of unsent notifications of this Dr.Web Server will be opened.
2. To the unsent notifications list whose notifications are placed that was failed to be sent to the recipients, but number of resend attempts which is specified in this notification settings is not yet expired.
3. The table of unsent notifications contains the following information:
   - **Notification**—the name of notification from the list of preinstalled notifications.
   - **Title**—the name of notification block according to whose settings this notification is sent.
   - **Resends remained**—number of remained resend attempts that are taken after notification send failed. Initial number of resend attempts is specified at notifications setup in the Notification Configuration section. After notification has been sent, you cannot change the number of remained resends for this notification.
   - **Time of next resend**—date and time of the next notification resend attempt. Period to perform notification resend attempts is specified at notifications setup in the Notification Configuration section. After notification has been sent, you cannot change the period of remained resends for this notification.
   - **Receiver**—addresses of notification receivers.
   - **Error**—error that caused the failure of notification sending.
4. To manage unsent notifications:
   a) Set the flags next to the specific notifications of the flag in the notifications table header to select all notifications in the list.
   b) Use the following buttons on the toolbar:

      Resend—send selected notifications immediately. At this, the immediate attempt to send the notification is performed. If sending failed, the number of remained attempts is decremented by one and the time of the next attempt will be counted from the moment of the current sending with periodicity specified in the Notification Configuration section.

      Delete—permanently delete all selected unsent notifications.
5. Unsent notifications are removed from the list in the following cases:
   a) Notification is successfully sent to the receiver.
   b) Notification is deleted by administrator manually via the **Delete** button on the toolbar.
   c) The number of resend attempts is over and notification was not sent.

d) In the Notification Configuration section, the notification block according to whose settings this notifications have been sending, is removed.

10.11. Administration of Dr.Web Server Repository

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

The repository deals with sets of files called *products*. Each product resides in a separate subfolder of the `var/repository` Dr.Web Server folder. The functions of the repository and their management are made separately for each product.

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

Update of Repository Products

Update of the product revisions can be performed as follows:

a) Download updates to Dr.Web Server from Dr.Web GUS.

The Dr.Web Server repository updates automatically from GUS according to tasks in the Dr.Web Server schedule.

- To view the tasks for repository updating, go to the General Repository Configuration section, the **Task Scheduler** tab.
- To change update from GUS schedule, go to the Setting Dr.Web Server Schedule section.
- To check for updates and download them manually, go to the Repository State section and click **Check for updates**.

See also Updating the Repository of a Server not Connected to the Internet.

b) Propagate updates between different Dr.Web Servers in a multi-server configuration.

If you have several Dr.Web Servers installed in your anti-virus network, you can configure interserver connections to transmit repository updates:

- For the *parent-child* type of connection, Dr.Web Servers receiving updates from GUS are parent, and child Dr.Web Servers receive all updates from parent automatically.
- For the *peer-to-peer* type of connection, any of them can receive updates from GUS. At this, other Dr.Web Servers receive all updates from it automatically.

Description of interserver connections configuration is given in the Peculiarities of a Network with Several Dr.Web Servers section.

If interserver connections are configured in the network, and other neighbor Dr.Web Servers receive updates from your Dr.Web Server, you must enable updates of all systems and interface languages of these neighbor Dr.Web Servers on your Dr.Web Server.

c) **Distribute updates from Dr.Web Server to workstations.**

Updates of stations software are checked, downloaded from Dr.Web Server, and installed on stations automatically at each connection of Dr.Web Agents to Dr.Web Server, and also, with some periodicity during the Dr.Web Agents operation (it cannot be configured and performed transparent for the administrator).

If necessary, you can configure limitations for time and traffic of the Dr.Web Agent updates in the Update Restrictions for Workstations section.

Configure of Repository Parameters

The repository allows the anti-virus network administrator to configure the following parameters:

- **The list of product update sites in a) operations.**

  Parameters of connection to GUS are configured in the General Repository Configuration section.

- **Restrictions to the number of products requiring synchronization of a) type.**

  Compound of downloaded products from GUS are configured in the General Repository Configuration and Detailed Repository Configuration sections.

  Thus, administrator is enabled to track only necessary changes of certain files or categories of files.

- **Restrictions to product components requiring synchronization of c) type.**

  Administrator of Dr.Web Server an select what should be installed on the workstation. Anti-virus components list is configured in the Installable Components of the Anti-Virus Package section.

- **Control of switching to new revisions.**

  Revisions are configured for each repository product separately in the Detailed Repository Configuration section.

  Independent testing of products before installation is possible.

- **Repository content management as files and folders.**

  The Repository Content section allows to view and manage current repository content as files and folders of repository: perform export and import either separate products or all repository content and its settings.

Composition of Repository Products

Currently, the following products are provided:

- **Dr.Web administrative utilities**

  Utilities for all supported operation systems:
  - Digital keys and certificates generation utility
  - Dr.Web Agent for UNIX remote installation utility
  - Dr.Web Agent for Windows remote installation utility
  - Dr.Web for Windows removal utility
  - Dr.Web Mobile Control Center (the links to App Store and Google Play)
  - Dr.Web Repository Loader (graphical and console versions)
  - Dr.Web Server remote diagnostics utility
  - Dr.Web Server remote scriptable diagnostics utility
  - Dr.Web utility for collecting information on a system.

  All utilities are available for downloading via the Control Center **Administration** → **Utilities** section.

- **Content filter databases for UNIX**

  Databases of built-in filters and Anti-spam, and Dr.Web Anti-spam for UNIX engine.

- **Dr.Web Agent for Windows**

  The anti-virus components software for stations under Windows OS.

- **Dr.Web Anti-spam databases**

  Databases of Dr.Web Anti-spam for Windows.

- **Virus databases for Android**

  Virus databases for stations under Android OS.

- **Dr.Web enterprise products**

  Installation packages for the following products:
  - Products for installation on protected stations under UNIX (including LAN servers), Android, macOS
  - Dr.Web Mail Security Suite (IBM Lotus Domino Windows)
  - Dr.Web Mail Security Suite (Microsoft Exchange Server)
  - Dr.Web Proxy Server—package for separate installation of Proxy Server not connected with Dr.Web Agent for Windows

- 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.

All installation packages of enterprise products are available for downloading on the installation page at the following address:

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

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

- **Dr.Web Proxy Server**

  Software to install Dr.Web Proxy Server connected with Dr.Web Agent for Windows.

- **Dr.Web Server**
  - Dr.Web Server software
  - Dr.Web Security Control Center software.
- **Dr.Web Server security data**

  A bundle of keys, scripts, and certificates ensuring secured update of the anti-virus network components and data exchange between Dr.Web Server and Dr.Web Agents.

- **Dr.Web Updater**

  Update module for Dr.Web Agent for Windows from version 6 to actual version.

- **Dr.Web virus databases**

  Virus databases, anti-virus engines for stations under Windows OS and Unix-like OS.

- **Doctor Web News**

  News feed from Doctor Web company website.

- **Documentation**

  Collection of manuals and reference materials available via the **Support** section in the Control Center.

- **Hashes of known threats**

  Lists of hashes of known threats.

- **SpIDer Gate databases**

  Databases of built-in filters of anti-virus components for Windows.

- **Trusted Applications**

  Trusted applications groups for the Application Control component for stations under Windows OS.

  The **Trusted applications** product is not updated from GUS. This product is propagated only between neighbor Dr.Web Servers via interserver connection.

  For more details on repository configuration for the **Trusted applications** product, refer the Trusted Applications section.

10.11.1. Repository State

To view the repository status or update anti-virus network components

1. Select the **Administration** item in the main menu of the Control Center and click **Repository state** in the control menu of the opened window.
2. In the opened window you can view the list of products in the repository, the date of the currently used revision, the date of the last downloaded revision, and the status of the products.

   The **State** column displays the status of the products in the Dr.Web Server repository at the time of the last update.

3. To manage the repository contents, use the following buttons:
   - Click the **Check for updates** button to check whether updates for all of the products are available on the GUS servers. If the checked component is outdated, it will be updated automatically during the check.
   - To save the log of repository updates, click one of the following buttons on the toolbar:
     - **Save data in CSV file**,
     - **Save data in HTML file**,
     - **Save data in XML file**,
     - **Save data in PDF file**.
   - Click **Reload repository from disk**, to reload the current version of the repository from disk.

   At startup, Dr.Web Server loads the repository contents to memory. If during the Dr.Web Server operation the administrator changed the contents without using the Control Center, for example, when updating the repository using an external utility or manually, reload the repository to enable the use of its downloaded version.

10.11.2. Delayed Updates

In the **Delayed Updates** section, you can view the list of products which updating is temporarily disabled on the following page: **Detailed repository configuration** → <*Product*> → Delayed Updates. A delayed revision is considered *frozen*.

The table of frozen products contains the following information:

- **Repository folder**—name of the folder where a frozen product resides:
  - 05-drwmeta—Dr.Web Server security data,
  - 10-drwbases—virus databases,
  - 10-drwgatedb—SpIDer Gate bases,
  - 10-drwspamdb—Anti-spam bases,
  - 10-drwupgrade—Dr.Web Updater,
  - 15-drwhashdb—known hashes of threats,
  - 20-drwagent—Dr.Web Agent for Windows,
  - 20-drwandroid11—virus databases for Android,
  - 20-drwcs—Dr.Web Server,
  - 20-drwunix—content filter databases for UNIX,
  - 25-drwcsdoc—documentation,
  - 40-drwproxy—Dr.Web Proxy Server,
  - 70-drwextra—Dr.Web enterprise products,
  - 70-drwutils—Dr.Web administrative utilities,
  - 80-drwnews—Doctor Web News.
- **Revision**—number of the frozen revision.
- **Delayed till**—time until update of the product is delayed.

When clicking the table row, another table with detailed information on the frozen revision of the corresponding product opens.

The option to delay updates is useful when you need to temporarily cancel distribution of last product revision on all stations of the anti-virus network, e.g., if you want to perform preliminary testing of this revision on a limited number of stations.

To use delayed updates functions, perform the actions described in the **Detailed repository configuration** → Delayed Updates section.

To manage delayed updates

1. Set the flags next to the products, for which you want to specify actions on delayed updates. To select all products, set the flag in the heading of frozen products table.
2. On the toolbar, select the required action:

Execute immediately—disable the frozen state for the product and add the revision to the list of revisions propagating according on stations according to the general procedure.

Cancel update—disable the frozen state for the product and forbid the revision. Updating from the GUS will be restored. The unfrozen revision will be removed from the product revision list. Upon receipt of the next revision, the unfrozen one will be removed from the disk.

Change updates delay time—specify the time period for the product revision to be delayed. The reference time for a freeze is the moment of receiving the revision from the GUS.

3. If you did not specify an action to be applied upon removal of the frozen status, the revision becomes unfrozen when the time is out and is included to the list of revisions distributed to stations according to the general procedure.

10.11.3. General Repository Configuration

In the **General repository configuration** section, you can specify parameters for connection to GUS and for updating repositories of all products.

To edit repository configuration

1. Select the **Administration** item in the main menu of the Control Center.
2. In the opened window, select the **General repository configuration** item in the control menu.
3. Configure all necessary parameters for updating from the GUS as described below.
4. If you need to discard any changes during parameters editing, use the following buttons next to each parameter:

   Reset to initial value—restore the value that parameter in this section had before current editing.

   Reset to default value—restore parameter from this section to its default, specified in the Dr.Web Server configuration file.
5. Click **Save** to save all changes into repository configuration files. At that, the current version of the repository is reloaded from the disk.

It takes some time to apply the new settings of repository configuration. At immediate update of the repository from GUS once the configuration is changed, the previous settings can be used.

10.11.3.1. Dr.Web GUS

On the **Dr.Web GUS** tab, you can configure parameters for connection to Dr.Web Global Update System. Updates are downloaded using the protocols listed in the **Update receiving protocol** drop-down list:

Protocol type	Description
HTTP/HTTPS	Protocols for receiving updates from the web server
FTP/FTPS	Protocols for receiving updates from the FTP server
FILE	Protocol for receiving updates from the local directory on a computer with Dr.Web Server installed
SMB/SMBS	Protocols for receiving updates from a common file system (available only for UNIX operating systems). The SMB protocol support is implemented using `curl` (supports SMBv1 only)
SCP/SFTP	Protocols for receiving updates using a secure connection

To edit GUS connection settings

- In the **Update receiving protocol** drop-down list, select the protocol type to receive updates from update servers. For all protocols, updates are downloaded according to the settings from the **List of Dr.Web Global Update System Servers** section.
- In the **Base URI** field, specify the GUS servers folder where updates of Dr.Web products are located. For updating from Dr.Web GUS servers, do not change this setting without necessity.
- If in the **Update receiving protocol** list, you have selected one of the secure protocols that support encrypting, then in the **Allowed certificates** drop-down list, select the type of TLS certificates that will be automatically accepted for the connection established by the selected protocol.
- If in the **Allowed certificates** list, you have selected the **User-defined** option, then specify the path to the file with your TLS certificate in the **Certificate** field.
- **Login**—user login to authenticate on updates server, if the updates server requires authorization.
- **Password**—user password to authenticate on updates server, if the updates server requires authorization.
- In the**Authorization method** drop-down list, select the authorization method on an update server.
- The **Number of temporary stored revisions** field specifies the number of revisions for each product temporary stored on disk not including revisions which are marked on the **Revisions list** tab, in the **Detailed repository configuration** section.

  If necessary, you can configure this setting separately for each product in the Synchronization section, but after the changes in the general configuration are saved, the setting will be changed to the general value.
- Set the **Use CDN** flag to allow receiving updates from GUS via Content Delivery Network.
- If necessary, edit the list of GUS servers from which the repository is updated, in the **List of Dr.Web Global Update System Servers** section:

- To add a GUS server to the list of servers used for updates, click  and specify the address of the GUS server in the appeared field.
- To remove a GUS server from the list of used, click  next to the server which you want to delete.
- GUS servers are listed in the order Dr.Web Server contacts them when updating the repository. To change the order of GUS servers, move a server as necessary by dragging the left root line of the server.

After installation of Dr.Web Server, the list contains only update servers of the Doctor Web company. If necessary, you can setup your own update zones and include them into the list of servers to receive updates.

10.11.3.2. Task Scheduler

On the **Task Scheduler** tab, you can view all tasks on the repository update from the Dr.Web Server schedule.

Creating, removing and editing tasks on repository update is performed in the Setting Dr.Web Server Schedule section.

10.11.3.3. Dr.Web Agent

- On the **Content filter databases for UNIX** tab, select for which Unix-like OSs you want to update the content filter databases on workstations (used by SpIDer Gate and Anti-spam).

To disable updating the content filter databases for UNIX from the GUS, open the **Detailed repository configuration** section, select the **Content filter databases for UNIX** item, navigate to the **Synchronization** tab, and set the **Disable product update** flag.

- On the **Dr.Web Agent for Windows** tab, in the group of selection buttons, specify whether you want to update all components that will be installed on stations under Windows OS or update only virus databases.
- On the **Dr.Web Agent for Windows languages** tab, specify languages for Dr.Web Agent and the anti-virus package interface of Windows OS, which will be downloaded from the GUS.

10.11.3.4. Dr.Web Server

- On the **Dr.Web Server** tab, specify the operating system that you want to update the Dr.Web Server files for:
  - To receive updates for Dr.Web Server installed on any of the supported operating systems, set the **Update all platforms available on GUS** flag.
  - To receive updates for Dr.Web Server installed on specific operating systems only, set the flags next to desired system names.

To completely disable all updates from GUS for Dr.Web Server, open the **Detailed repository configuration** section, then select the **Dr.Web Server** item, and on the **Synchronization** tab, set the **Disable product update** flag.

- On the **Dr.Web Security Control Center languages** tab, specify the languages to download from GUS for the Control Center interface.
  - In the **Languages in use** section, you can see a list of languages assigned to at least one administrator in the settings.
  - In the **Unused languages** section, you can see a list of languages that are not assigned to any of the administrators.
- On the **Documentation** tab, select languages of manuals that will be available in the Help → **Documentation** section.
  - The split between **Languages in use** and **Unused languages** follows the same principle as on the **Dr.Web Security Control Center languages** tab.
  - Make sure you set the **Update documentation** flag in the **Documentation in PDF** subsection below the languages to have access to manuals in PDF format.

10.11.3.5. Doctor Web News

On the **Doctor Web News** tab, specify a list of languages for the news feed.

You can configure subscription settings on news lines at the Preferences → **Subscription** section.

You can read news of Doctor Web company in the main menu of the Control Center, in the **Support** → **News** section.

10.11.3.6. Dr.Web Installation Packages

- On the **Dr.Web enterprise products** tab, in the drop-down list, select the products you want to update from GUS:
  - **Update all products**—all available enterprise products will be updated when the repository receives updates from GUS.
  - **Update selected products only**—update only products with flags set in the list below when the repository receives updates from GUS.

  After loading from GUS, enterprise products become available in the **Administration** → **Additional features** → Enterprise products section and on the installation page:

  `https://<Dr.Web_Server_address>:<port_number>/install/`

  where *<Dr.Web_Server_address>* is IP address or DNS name of the computer on which Dr.Web Server is installed; and the *<port_number>* should be `9081` (or `9080` for http).
- On the **Dr.Web administrative utilities** tab, in the drop-down list, select the utilities you want to update from GUS:

- **Update all products**—all available administrative utilities will be updated when the repository receives updates from GUS.
- **Update selected products only**—update only utilities with flags set in the list below when the repository receives updates from GUS.

After loading from GUS, administrative utilities become available in the **Administration** → **Additional features** → Utilities section.

10.11.3.7. Dr.Web Proxy Server

On the **Dr.Web Proxy Server** tab, specify the operating system that you want to update the Dr.Web Proxy Server files for:

- To receive updates for Dr.Web Proxy Server installed on any of the supported operating systems, set the **Update all platforms available on GUS** flag.
- To receive updates for Dr.Web Proxy Server installed on specific operating systems only, set the flags next to desired system names.

10.11.4. Detailed Repository Configuration

The **Detailed repository configuration** section provides you with options to configure revision for each repository product separately.

To edit repository configuration

1. Select the **Administration** item on the main menu of the Control Center.
2. In the opened window, in the **Detailed repository configuration** subsection of the control menu, select the product you want to edit.
3. Configure all necessary repository settings for the selected product, described below.
4. The following options to manage the whole repository product are available on the toolbar:
   - **Delete product from repository**—delete the product from repository completely. At this, all revisions of the product will be deleted and update of the product from GUS will be disabled. The button is available if the product has not yet been deleted from the repository. After the product has been deleted, the button changes its name to **Restore product in repository**.

     After the product has been deleted from the repository, the **Revision list** tab will be empty, the other tabs in this section remain in the normal state but their settings do not applied because the product is not in the repository.

   - **Restore product in repository**—restore the product in the repository if it was deleted earlier using the **Delete product from repository** button. At this, update of the product from GUS will be enabled. The most fresh revision of the product available on GUS will be downloaded to the repository. Please note the possible data amount to download. You can configure updates downloading in the General repository configuration section. After

the product has been restored, the button changes its name to **Delete product from repository**.

- **Save and reload from disk**—save all your changes. At that, the current version of the repository is reloaded from the disk (see also Repository State).

10.11.4.1. Revision List

On the **Revision list** tab, you can view information on all revisions available on Dr.Web Server for this product.

To delete any revisions, set the flags next to these revisions and click **Delete selected revisions** on the toolbar.

You cannot delete all revisions. A product must contain at least one revision.

To delete the whole product, use the **Delete product from repository** button.

Deleting revisions cannot be undone.

The table of revisions contains the following columns:

Column name	Description
Distributed	Automatic marker in this column defines the state of product revisions. Two types of markers are available: —*Distributed revision*. Revision used for updating Dr.Web Agents and the anti-virus software on workstations. Revision for distribution is selected as follows: 1. Revision indicated with the marker in the **Current** column is distributed. Only one revision can be marked. 2. If no revision is marked in the **Current** column, the latest revision is distributed. The automatic marker always indicates the distributed revision. —*Frozen revision*. A frozen revision is not distributed to stations, new revisions are not downloaded from Dr.Web Server. For more on frozen revisions, refer to Delayed Updates. If a revision is frozen, the revision for distribution is selected as follows: 1. If the marker in the **Current** column is set, the current revision is distributed to stations. 2. If the marker in the **Current** column is not set, the revision that precedes the current one is distributed to stations.

Column name	Description
Current	Set the marker to specify the revision used for updating Dr.Web Agents and the anti-virus software on stations. Only one revision can be selected as current. Alternatively, you can choose to not set the marker that indicates the current revision. See also Downgrade Product Revision.
Stored	Set the marker to save the revision when the repository is automatically cleaned up (see also Synchronization). The marker can be set for multiple revisions simultaneously. Alternatively, you can choose to not set the marker. If the product revision is stable, you can mark it as stored. If an unstable revision gets downloaded from the GUS, you will be able to roll back to the previous one.
Held	An automatic marker denotes that components from this revision are installed on stations with update restrictions (in the Update Restrictions for Workstations section, the **Update only bases** and **Forbid all updates** options are set). The revision is not deleted when the repository is purged automatically and can be used if failed components must be reinstalled on a station or additional components of this revision must be installed.
Revision	The date the product revision was received. If the revision is frozen, the blocking status displays in the column as well.

Downgrade product revision

The ability to downgrade products installed on stations to previous versions is determined by the following:

- Products with databases (virus databases, SpIDer Gate databases, Anti-spam databases) can be downgraded at any time.
- To downgrade Dr.Web Agent for Windows, enable the **Allow revisions downgrade** option in the Update Restrictions for Workstations section.

  If you downgrade Dr.Web Agent for Windows to a previous revision (to install an earlier version of Dr.Web Agent on stations), the stations will be forced to restart in five minutes. You cannot change the interval or cancel the restart. Station users are notified about the upcoming restart in the popup message.

- Other products (particularly, Trusted applications of the Application Control component) will ne downgrade if the **Receive the latest updates** flag is set in the Update Restrictions for

Workstations section, or they are downgraded to revision marked as **Current** in the detailed configuration of the repository. In all other cases the downgrade is not performed, Dr.Web Server waits for new revision.

10.11.4.2. Synchronization

On the **Synchronization** tab, you can configure parameters for updating the Dr.Web Server repository from GUS:

- The **Number of temporary stored revisions** field specifies the number of product revisions temporary stored on disk not including revisions which are marked at least in one column of the **Revisions list** tab. When a new revision is received and the number of temporary stored revisions already reached the specified allowed value, the oldest temporary stored revision is removed. Revisions marked as **Current**, **Stored**, **Distributed** and **Held** are not automatically removed and are not taken into account when calculating temporary stored revisions.

  This setting will be overwritten with a single value for all products if the Dr.Web GUS section is edited.
- Set the **Disable product update** flag to disable receiving updates for this product from the GUS servers. Dr.Web Agents will be updated to the current revision on Dr.Web Server (or according to the procedure used to select the distributed revision).
- Set the **Update on demand only** flag to update the product from GUS only when this product is requested from stations. Otherwise, product updates are not downloaded from GUS.

  If your Dr.Web Server is connected to the internet for receiving repository updates from GUS automatically, then using this option, additional configuration by administrator is not required: updates will be automatically downloaded as soon as one of the stations requests updates of this product from Dr.Web Server.

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

  By default, after installing Dr.Web Server version 13 or immediately after upgrading Dr.Web Server to 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.

- In the **Propagation via interserver connections** section you can configure the following parameters:
  - Set the **Prevent sending updates to neighbor Dr.Web Servers** flag to forbid sending the product updates via the interserver connections. The option does not affect the product update settings from GUS.
  - Set the **Prevent receiving updates from neighbor Dr.Web Servers** flag to forbid receiving the product updates via the interserver connections. The option does not affect the product update settings from GUS.

For some products, the following settings are also available:

- Set the **Update only following files** flag to receive updates from GUS only for the file listed below.
- Set the **Do not update only following files** flag to disable updating from GUS only for the file listed below.

  Files can be specified in the format of regular expressions.

If both flags are set, files for an update are selected as follows:

1. From the complete list of product files only those are selected that are specified in the **Update only following files** lists.
2. From the selection at step 1, files specified in the **Do not update only following files** lists are removed.
3. Files resulting from the selection at step 2 are updated from GUS.

10.11.4.3. Notifications

On the **Notifications** tab, you can configure notifications on repository updates:

- Set the **Do not notify only about following files** flag to disable notifications on events of the files listed below.
- Set the **Notify only about following files** flag to enable notifications on events of the files listed below.

  Files can be specified in the format of regular expressions.

If exceptions list are not specified, all notifications enabled on the Notification Configuration page are sent.

Parameters of notifications on repository updates are configured in the Notifications configuration page, in the **Repository** section.

10.11.4.4. Delayed Updates

On the **Delayed updates** tab, you can delay distribution of updates on stations for the specified period of time. A delayed revision is considered *frozen*.

The option to delay updates is useful when you need to temporarily cancel distribution of last product revision on all stations of the anti-virus network, e.g., if you want to perform preliminary testing of this revision on a limited number of stations.

It is not recommended to freeze revisions when switching between major versions. After disabling freezing, you may have problems when updating anti-virus software at stations.

To use delayed updates functional

1. For the product, update of which you want to freeze, configure delayed updates as described below.
2. To disable distribution of the last revision, set one of the previous revisions as a current on the Revision List tab.
3. For the group of stations that will receive the last revision, set the **Receive the latest updates** flag on the **Anti-virus Network** → Update Restrictions for Workstations section. Other workstations will receive the revision which you selected as current at step 2.
4. The next downloaded from the GUS revision which is satisfying the conditions specified for the **Delay updates for the following files only** option, will be frozen and delayed for the time period specified in the **Change updates delay time** list.

To configure delayed updates

1. Set the **Delay updates** flag to temporarily disable downloading updates from GUS servers for this product.
2. In the **Updates delay time** drop-down list, select the time period to delay downloading updates starting from the moment of their receive from the GUS servers.
3. If required, set the **Delay updates for the following files only** flag to delay distribution of updates that contain files which corresponds to the masks specified below. Masks are specified in the format of regular expressions.

   If the flag is cleared, all updates from the GUS are frozen.

To disable the frozen state

- On the **Revision list** tab, click **Execute immediately** to disable the frozen state for the product and add the revision to the list of revisions distributed to stations according to the general procedure.
- On the **Revision list** tab, click **Cancel update** to disable the frozen state for the product and forbid the revision. Updating from the GUS is restored. Unfrozen revision will be removed from the list of product revisions. After the next revision is received, the unfrozen revision will be removed from the disk.
- When the time specified in the **Change updates delay time** list is out, the revision becomes unfrozen and is included to the list of revisions distributed to stations according to the general procedure.

You can manage frozen revisions for all products on the Delayed Updates page.

10.11.5. Repository Content

The **Repository content** section allows to view and manage current repository content as files and folders of repository folder.

The main window of the **Repository content** section is represented as a hierarchical tree of repository content displaying all folders and files of the current repository version, with a list of all revisions available for each product.

View Repository Information

To view information about all repository objects, select an object in the hierarchical tree. The properties panel with the following information will be opened:

- The **Selected objects** subsection contains detailed information about the object selected in the repository content tree: **Type**, **Size** (for separate files only), **Created on** and **Modification date**.
- The **Repository state** subsection contains general information about all repository objects: current list of objects and the date of the latest update.

Manage Repository

To manage repository content, use the following buttons on the toolbar:

Export repository file to an archive,

Import archive with repository files,

Delete selected objects—permanently delete objects selected in the repository content tree.

Repository Export

To save repository files into a zip archive

- To save the entire repository into an archive, click **Export repository files to an archive → All repository content** on the toolbar. This will export the entire repository regardless of an object selected in the hierarchical tree.
- To save only the latest revisions of all products into an archive, click **Export repository file to an archive → Last revisions of all products** on the toolbar.
- To save all configuration files of the repository into an archive, click **Export repository file to an archive → Configuration files** on the toolbar. This will export all files from the root folder of the repository and the products.
- To save specific repository objects into an archive, select them using the CTRL or SHIFT keys and click **Export repository file to an archive → Selected objects** on the toolbar.

When exporting a large amount of data, the duration of export may exceed the session time. If the session expires before the export is completed, the export process will be terminated automatically and the export data archive will not be generated.

Please note the general types of exported objects:

a) Zip archives of repository products. Such archives contain one of the following repository object types:
   - The entire repository.
   - The entire product.
   - The entire revision of a product.

   Exported archives of these objects can be imported via the **Repository content** section. The name of such archives contains the `repository_` prefix.

b) Zip archives of separate repository files.

   Exported archives of separated files and folders, which are lower than the objects from the **a)** in the hierarchical tree, cannot be imported via the **Repository content** section. The name of such archives contains the `files_` prefix.

   Such archives can be used as a backup copy for manual replacement. However, it is recommended that you do not replace any repository files manually by bypassing the **Repository content** section.

Repository Import

To load repository files from a zip archive

1. Click **Import archive with repository files** on the toolbar.
2. In the opened window, in the **Select file** section, specify a zip archive containing repository files using the button.

   You can import only the zip archives generated during the export of one of the following repository object types:
   - The entire repository.
   - The entire product.
   - The entire revision of a product.

   The name of such archives contains the `repository_` prefix.
3. In the **Import settings** section, specify the following parameters:
   - **Add missing revisions only**—in this import mode, only the revisions missing from the current version of the repository will be added. Other revisions will remain unchanged.
   - **Replace entire repository**—in this import mode, the repository is fully replaced with the imported one.
   - Set the **Import configuration files** flag to import configuration files when importing the repository.
4. Click **Import** to start the import process.

10.11.6. Known hashes of threats

The **Known hashes of threats** section allows you to search the bulletin with known hashes of threats which is provided by the FinCERT organization and included in the 15-drwhashdb product.

The section is available only if the usage of bulletins of known threat hashes is licensed. You can check the license in the information on a license key that can be found in the License Manager section, the **Allowed lists of hash bulletins** parameter (the license in at least one of the license keys used by Dr.Web Server is sufficient).

Anti-virus protection level is not reduces if hash bulletins are not licensed. This license allows to notify the administrator that the detected threat is in the specialized bulletins of known hashes of threats.

The 15-drwhashdb product is managed in the **Administration > Detailed repository configuration > Known hashes of threats** section.

The table in this section contains the following data:

- **Threat hash**—known hash of threat.
- **Bulletin name**—FinCERT_IOC.

To search in the hash table fields, click  .

When a threat is detected on a station (by application control, preventive protection or scanning) and information about it is sent to the Dr.Web Server, the server checks its hash with the hash in the FinCERT list and, if it matches, marks it as present in the FinCERT bulletin. This information is available in the statistics tables with detected threats when the **Bulletin** column is enabled in the **Anti-Virus Network > Statistics** section.

The hash database is stored in a single hash-db file in the following folder:

- for Windows OS: `C:\Program Files\DrWeb Server\var\hash-db\<revision number>\hash.db`,
- for Linux OS: `/var/opt/drwcs/hash-db/<revision number>/hash.db`,
- for FreeBSD OS: `/var/drwcs/hash-db/<revision number>/hash.db`.

Notifications about detecting threats by known hashes

You can configure sending notifications about found matches with known threat hashes in the Notification Configuration section.

The following notifications are available:

- **Application Control blocked the process from the known hashes of threats list**,

- **Security threat detected by known hashes of threats**,
- **Scan error at threat detection by known hashes of threats**,
- **Report of Preventive protection on threats detection by known hashes of threats**.

Set the **Send notifications on events of neighbor Dr.Web Server at threat detection by known hashes** flag to send notifications to the administrator about the events received from the configuring child Dr.Web Server in case of security threat detection by known hashes of threats. If the flag is cleared, the administrator will receive notifications on events only on the own Dr.Web Server.

The flag is available only if the usage of bulletins of known threat hashes is licensed (the 15-drwhashdb repository product).

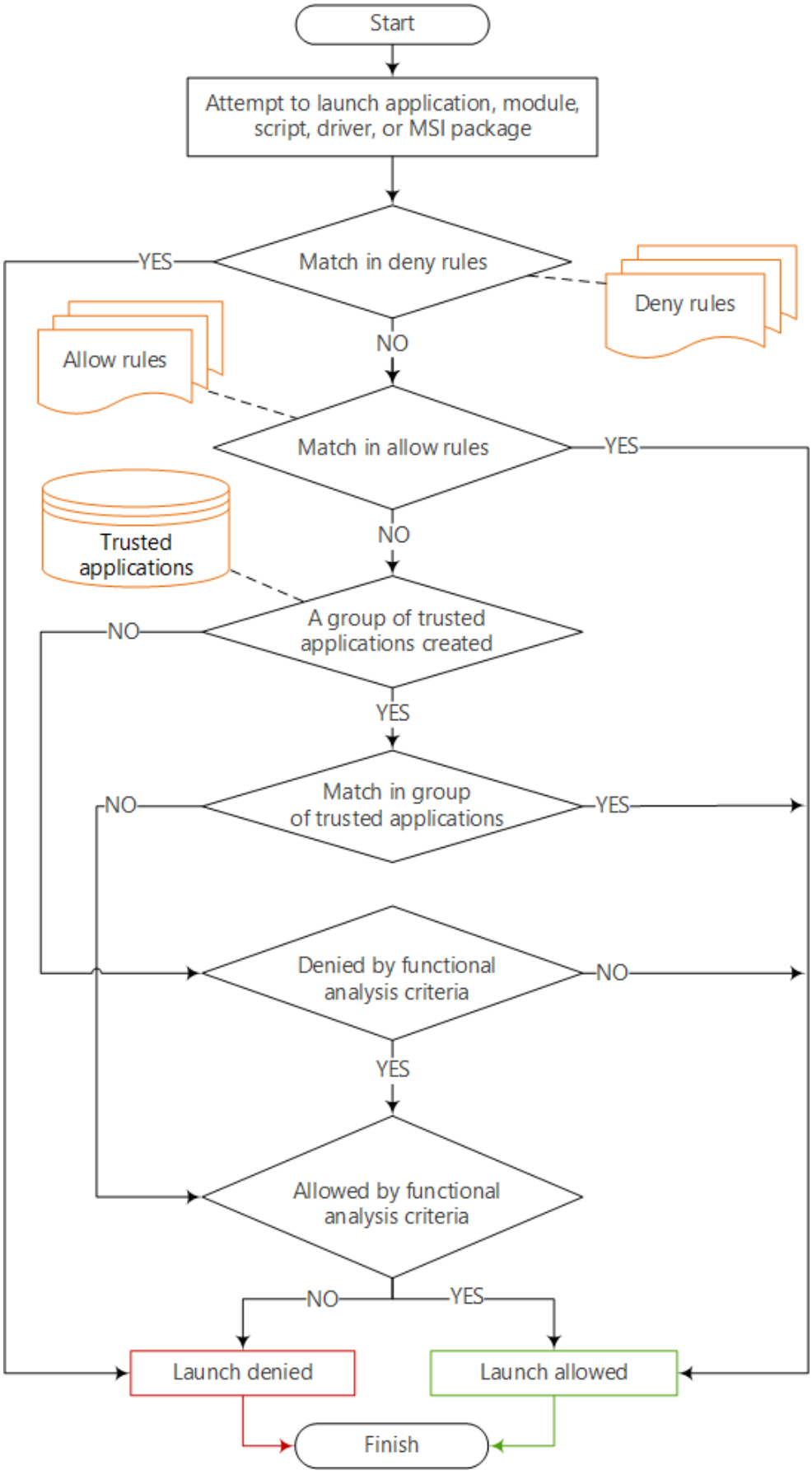
It is also possible to customize notifications via user hooks.

If you do not have a license for a product, the corresponding notifications are automatically turned off.

10.12. Application Control

Using the Application Control component, you can adjust which applications, modules, script interpreters, drivers and MSI packages to allow and which ones to prohibit launching on protected stations on the anti-virus network on which Dr.Web Agent for Windows is installed.

Schemes of Application Control operation is given below.



Basic tools of the Application Control:

- Profiles—the list of rules that determine which of the applications on the stations can be started and which are prohibited. Profiles are created by the administrator and are assigned to policies, stations and users, as well as groups of stations or users. Profiles define the operation mode on the Application Control.

  Profiles are configured in the network tree of the **Anti-virus network** section.
- Application lists:
  - Trusted Applications—the list of applications that is made according to the specified rules and is collected from the selected stations by decision of the administrator. When operating in the allow mode, running these applications will always be allowed. Specific groups of trusted applications are selected in the settings for each profile individually.
  - Application Catalog—the list of all applications installed on protected stations. The catalog is collected automatically in the background mode and cannot be changed by the administrator.

  Application lists are configured in the **Administration** section.
- Application Control Events—information on events detected on stations by the Application Control component.

  Application Control events are displayed in the **Anti-virus network** → **Statistic** section.

Basic operation modes of the Application Control:

- *Functional analysis*—the set of predefined rules by which applications are allowed or prohibited to be launched in accordance with the functions performed.
- *Allow mode*—means that on all monitored stations, only applications from the **Trusted applications** list and applications that comply with the allow rules are allowed to run. All other applications are blocked.
- *Deny mode*—means that on all monitored stations, only applications that comply with the deny rules are prohibited to run. All other applications are allowed.

Allow and deny modes can be enabled or disabled both together and separately.

Functional analysis must be always enabled. If all policies are disabled, applications launch is not controlled.

To configure Application Control

1. Create a new profile.
2. Assign stations, users, and groups to use the settings of created profile.
3. Configure the profile settings.

It is recommended to configure profiles operation in the test mode.

10.12.1. Test Mode

In order to make sure that configured profile or rule works correctly, you can use the *test mode*, which imitates Application Control actions. In this mode, applications are not actually blocked but all activity is getting logged (see Application Control Events), as if the profile or rule was working as usual. The test mode is convenient for easy configuration of Application Control by an administrator when deployed an enterprise network.

To enable test mode for a profile

1. In the **General** section of profile properties, set the flag **Enable profile** to start using a profile (disabled by default).
2. Set the flag **Switch profile to global test mode**.
3. Click **Save**.

A profile in test mode will have the icon in **Profiles** group of the anti-virus network tree. On workstations that have such profile assigned to them, no applications will be blocked based on specified functional analysis criteria, allow or deny rules. Instead, respective statistics will be logged in the **Anti-virus Network** → **Statistics** → **Application control events** section. This log keeps detailed information about each started application, which you can review and use to tailor profile settings for your needs.

Once you make sure that tested profile operates as you need, it needs to be switched from test mode to active mode. Active profile has the icon in **Profiles** group of the anti-virus network tree.

To disable test mode for a profile

1. In the **General** section of profile properties, clear the flag **Switch profile to global test mode**.
2. Click **Save**.

Test mode can also be used to check how specific allow or deny rules work in a profile, without switching the profile entirely.

To enable test mode for allow or deny rule in a profile

1. In the **Allow rules** or **Deny rules** section of profile properties, select the rule you created and would like to test.
2. In the opened rule settings, set the **Enable rule** and **Switch rule to test mode** flags.
3. Click **Save**.

In this mode, applications started on workstations *will be blocked* but only according to functional analysis criteria and the rules that were not switched to test mode. Allow and deny rules in test mode will work similarly to profiles in this mode, meaning that their settings have no impact on applications being blocked, but each imitated trigger of a rule gets into activity log in the **Application control events** section.

In contrast with profile test mode, there is no indication of any rules being in test mode on involved profile icon in the anti-virus network tree. Any active profile with rules in test mode would have the icon.

Once you make sure the rule you are testing works properly, it needs to be switched from test mode to active mode.

To disable test mode for allow or deny rule in a profile

1. In the **Allow rules** or **Deny rules** section of profile properties, select the rule you are testing.
2. In the opened rule settings, clear the **Switch rule to test mode** flag.
3. Click **Save**.

10.12.2. Trusted Applications

Trusted Applications Management

Trusted applications group (or applications white list) is a list of applications collected by the specified conditions from the selected station or station group. This applications will be allowed to run on all stations of the anti-virus network on which they are added to the profile of the Application Control component operating in the allow mode.

Collection of information required to form a group of trusted applications is a demanding procedure, which, based on specified conditions, can have a significant impact on involved computer's performance. In order to reduce load on anti-virus network workstations, information shall be collected using one or several *reference workstations*, i.e. computers deliberately assigned with this task. An ideal candidate for this job would be a computer with newly installed operating system, latest updates and all the required software.

To manage trusted applications on Dr.Web Servers collecting the information, open the **Administration** → **Application Control** → **Trusted applications** section.

The section table contains the list of all actual trusted applications groups.

The following control buttons are available on the toolbar:

Create trusted applications group

Reload creation of trusted applications group

Delete trusted applications group

To create a new trusted applications group

1. In the **Trusted applications** section, click **Create trusted applications group** on the toolbar.
2. In the **General** windows, specify the following settings:
   - **Group name**—the name of creating trusted applications group.
   - **Description**—optional arbitrary description of creating group.

   Click **Next**.
3. In the **Parameters for adding applications to trusted** window, configure the settings according to which applications at stations will be added to the creating group of trusted applications (at least one setting must be selected in each category):

   Set the **Set low priority for information collection process** flag if information for created group of trusted applications is collected on a workstation, whose system resources must not be fully occupied with this task.

   Enabling this parameter will help save the computer's resources required to collect information; however, it can significantly increase the time required to complete this operation.

   - **Search scope**—set the flags for the areas where the information on applications will be collected.

     You can specify several paths for the **Search by specified paths** option to search the applications. Use ";" as a separator.

   - **Type of hashes to add**—set the flags for objects whose hashes will be written into creating group of trusted applications.
   - **File categories**—set the flags for objects that will be considered during search.

   Click **Next**.
4. In the network tree, select stations and station groups to collect information on applications for the trusted list. To select several groups and stations, use CTRL and SHIFT.

   Set the **Do not consider nested groups** flag to collect information on stations only in the selected group. If the flsg is cleared, information will be collected on all stations in the selected group and its subgroups.
5. Click **Save**.
6. The collection of information about applications on the stations will start according to the settings specified. The process may take a long time to complete.

   Information on the state and updates of trusted application group you can find:
   - in the general table of the **Trusted applications** section,

- in the additional information on group that is opened when clicking the group row in the general table of the **Trusted applications**.

Information about applications is collected within a current session on involved workstation. If the collection process is not yet complete and the workstation shuts down or restarts, the whole operation will start from the beginning once the workstation is back on. Partially collected information about applications is not saved.

To start the update of trusted applications group

1. In the **Trusted applications** section table, set the flags for the groups you want to update.
2. Click **Reload creation of trusted applications group** on the toolbar.

To delete trusted applications group

1. In the **Trusted applications** section table, set the flags for the groups you want to delete.
2. Click **Delete trusted applications group** on the toolbar.
3. Applications of this group will be removed from the list of allowed to run at stations, and collecting applications for the list of trusted by conditions of this group will be stopped.

You cannot delete the group of trusted applications assigned to profiles of Application Control.

When you delete the trusted applications group, a new revision is created in the repository for the **Trusted applications** product, and it is propagated on the neighbor Dr.Web Servers. At this, the Control Application profiles for which this group is assigned on neighbor Dr.Web Servers may not function properly.

To remove information about applications on a certain station from the trusted applications group

1. In the **Trusted applications** section table, click the line with the applications group from which you want to remove the information about applications on station.
2. In the opened window, in the stations table, set the flags for stations for which you want to remove information about applications.
3. Click **Delete selected stations** on the toolbar.

When removing all stations, the trusted applications group will be deleted.

Trusted Applications Repository

When configuring the allow mode for the Application Control profile, the trusted applications group are selected from the list of groups available in the repository for the **Trusted applications** product.

If your anti-virus network running several Dr.Web Servers under interserver connection, to facilitate the collection of information, it is possible to distribute the load between your Dr.Web Servers as follows:

- Administrator collects information from protected stations on one of Dr.Web Servers. Information automatically placed into the Dr.Web Server repository in the **Trusted applications** product and propagated via interserver connection according to the specified settings.

  Information on trusted applications may be collected on several Dr.Web Servers of the network, but network segments served by these Dr.Web Servers must be isolated from each other.
- Other Dr.Web Servers get the **Trusted applications** product update via interserver connection according to the specified settings. You do not need to configure trusted applications collecting on these Dr.Web Servers, because revisions of the product received from the neighbor Dr.Web Server will be placed in the repository.

The **Trusted applications** product is not updated from GUS. This product is propagated only between neighbor Dr.Web Servers via interserver connection.

Before collecting Trusted applications, define which Dr.Web Servers will collect information and send it to neighbor Dr.Web Servers, and which—receive it via interserver connection. Depending on this, you must configure corresponding settings on each of the Dr.Web Servers.

To configure Dr.Web Servers collecting and sending trusted applications

1. Open the **Administration** section.
2. Go to the **Detailed repository configuration** → **Trusted applications** section.
3. On the **Synchronization** tab, clear the **Prevent sending updates to neighbor Dr.Web Servers** flag and set the **Prevent receiving updates from neighbor Dr.Web Servers** flag.
4. Click **Save**.
5. Go to the **Administration** → **Application Control** → **Trusted applications** section and configure collecting of trusted applications as described below.
6. New revision of the **Trusted applications** product is written to the repository after receiving information from all stations specified in the settings for collecting group of trusted applications. After writing the product revision to the repository, it is propagated via interserver connection to the neighbor Dr.Web Servers.

To configure Dr.Web Servers receiving trusted applications

1. Open the **Administration** section.
2. Go to the **Detailed repository configuration** → **Trusted applications** section.
3. On the **Synchronization** tab, clear the **Prevent receiving updates from neighbor Dr.Web Servers** flag.

   If Dr.Web Server should send the **Trusted applications** product to other Dr.Web Servers via interserver connection, also clear the **Prevent sending updates to neighbor Dr.Web Servers** flag.
4. Click **Save**.

10.12.3. Application Catalog

To view applications catalog, open the **Administration** → **Application Control** → **Applications catalog** section.

Application catalog contains information on applications installed on protected stations under Windows OS connected to Dr.Web Server.

The catalog is collecting automatically in the background mode and cannot be changed by the administrator after collecting. Information on each application is sent by Dr.Web Agent to Dr.Web Server once at first activity of this application.

The catalog can be used for the following needs:

- Get information on installed applications on the network stations.
- Create deny and allow rules. Using of the catalog simplifies the process of the rules creation, since all information on application is filled automatically based on data about the selected known application.

Filling Application Catalog

To activate sending the information for the application catalog from the stations

1. In the **Anti-virus network** section in the network tree, select station or station group with Application Control installed from which you want to receive information on applications installed.
2. In the control menu, select **Windows** → **Dr.Web Agent** if you selected a group, or **Dr.Web Agent** if you selected a station.
3. On the **General** tab, set the **Track Application Control events** flag to track all processes activity at stations detected by Application Control and send events to Dr.Web Server. If there is no connection with Dr.Web Server, events are collected and sent upon connect. If the

flag is cleared, only processes blockings can be sent (depending on the settings in the Dr.Web Server configuration).

4. Click **Save**.

To activate collecting the information for the application catalog at Dr.Web Server

1. Open the **Administration** → **Dr.Web Server configuration** section.
2. Go to the **Statistics** tab and set one of the following options:
   - **Application Control statistics on processes activity** to receive and write information on any activity of all processes: either allowed or prohibited to launch by Application Control. Setting this option will enable registration of applications in the catalog, as long as at least one profile is created and assigned, with one or several categories of functional analysis criteria selected.
     Before creating the profiles and assigning them to stations of anti-virus network, all applications are allowed to be launched.
   - **Application Control statistics on processes blocking** to receive and write information on activity of all processes prohibited to launch by Application Control. For this option, applications will be written to the catalog only after creating profiles by the settings of which application launch will be blocked, and assigning these profiles on stations of anti-virus network.

   The **Application Control statistics on processes activity** flag may significantly increase resource intensity of statistics collecting over all anti-virus network.

3. Click **Save**.
4. Restart Dr.Web Server.
5. After restarting, Dr.Web Server starts collecting statistics according to the specified settings on applications launch received from all stations with Application Control installed.

Creating Rules from Application Catalog

To create a new rule basing on the data from the application catalog

1. In the **Application catalog** section, select a row with the application for which you want to create the rule for controlling the launch.
2. The table row click opens the window with information on the selected application.
3. Click **Create rule**.
4. The window for creation of a new rule will be opened. Specify the following settings:
   a) In the **Profile name** drop-down list, select the Application Control profile for which the rule will be created.
   b) In the **Rule name** filed, specify the name of creating rule.
   c) For the **Rule type** option, select the type of creating rule: deny or allow.

d) For the **Operation mode** option, select the operation mode of the creating rule (corresponds the **Switch rule to test mode** flag at rule creation in a profile):
If you want to check the rule operation, select the **Test** option. Applications will not be controlled at stations, but the activity log will be written as for enabled settings. Application launch and block results based on a rule in test mode will be displayed in the Application Control Events section.
With the **Active** option, the rule operates in active mode and blocks applications at stations by specified rule settings (see also modes of profiles operation).

e) In the **Prohibit the launch of applications on the following criteria/Allow the launch of applications on the following criteria** section (depending on the rule type selected at step 4c), the fields will be automatically specified in accordance with the applications on the base of which the rule is creating. If necessary, you can edit the settings.

5. Click **Save**. The rule will be created in the specified profile of the Application Control.

10.13. Additional Features

10.13.1. Database Management

The **Database management** section allows to perform direct maintenance of the database with which Dr.Web Server is operated.

The **General** section contains the following parameters:

- The **Last DB maintenance** field—the date of last execution of the database maintenance commands from this section.
- The list of commands to maintain the database which includes:
  - Commands similar to the tasks from Setting Dr.Web Server Schedule. The names of commands correspond to the names of tasks in the **Action** section of the Dr.Web Server schedule (description of corresponding schedule tasks is given in the Tasks types and their parameters table).
  - The **Analyse database** command. It is designed to optimize the Dr.Web Server database using the `analyze` command.
  - The **Purge non-activated stations** command. It is designed to delete accounts of stations that were created in the anti-virus network but have never been connected to Dr.Web Server. Specify the period after which the unused station accounts should be purged. You can view the list of unused station accounts in the hierarchical list of the anti-virus network, in the **Status** → **New** group.

To execute database maintenance commands

1. In the commands list, set the flags for the commands you want to execute.

   If necessary, change the time periods for the database purging commands, after which stored information is confirmed outdated and should be removed from Dr.Web Server.

2. Click **Apply now**. All selected commands will be executed immediately.

For postponed or/and periodic automatic execution of these commands (except **Analyse database**), use Dr.Web Server Task Scheduler.

To manage database use the following buttons on the toolbar:

 Import,

 Export.

Database Export

To save the database information into a file

1. Click  **Export** on the toolbar.
2. In the export settings configuration window, select one of the following variants:
   - **Export entire database** to save all information from the database into a gz archive. Exported XML file is similar to the database export file which is obtained when running the Dr.Web Server executable file from the command line with the `modexecdb database-export-xml` switch. This export file can be imported when running the Dr.Web Server executable file from the command line with the `modexecdb database-import` switch. These commands are described in details in the **Appendices** document, G3.3. Database Commands.
   - **Export information on stations and groups** to save information about the objects of the anti-virus network into a zip archive. In the result of this command execution, all information on groups of stations and stations accounts of the anti-virus network served by this Dr.Web Server, is save into the file of a specific format. Export file contains the following information about stations: properties, component configuration, permissions, update restriction settings, schedule, list of installable components, statistics, information on deleted stations; about groups: properties, component configuration, permissions, update restriction settings, schedule, list of installable components, parent group ID. The export file can later be imported via the **Database management** section.
     - In the **Anti-virus network** tree, you can select one or several user groups. In this case, export will contain information only on selected groups and on stations for which the selected groups are primary. If no group is selected, export will contain information on all stations and user groups of the anti-virus network.
3. Click **Export**.
4. Specify the path to save the archive with the database according to the web browser settings in which the Control Center is opened.

When exporting a large amount of data, the duration of export may exceed the session time. If the session expires before the export is completed, the export process will be terminated automatically and the export data file will not be generated.

Database Import

You can use the import procedure of the database containing information on the objects of anti-virus network, to transfer the information either on the new Dr.Web Server or on the Dr.Web Server that is already operating into anti-virus network, particularly to merge the lists of served stations of two Dr.Web Servers.

All imported stations will be able to connect to Dr.Web Server on which you perform the import. When you performing the import, please note that you must have corresponding number of available licenses to connect imported stations. E.g., if necessary, in the License Manager section, add the license key from Dr.Web Server, from which the information about stations had been imported.

To load the database from a file

1. Click  **Import** on the toolbar.
2. In the import window, specify the zip archive with the database file. To select the file, you can use the  button.

   You can import only those zip archives that have been obtained during the export of the database for the **Export information on stations and groups** option.
3. Click **Import** to start the import process.
4. If during import, there are stations or/and groups with the same identifiers which are included both into imported data and into the current Dr.Web Server database, the **Collisions** section opens to configure actions on duplicated objects.

   Groups and stations lists are presented in separated tables.

   For corresponding objects table, in the **Groups import mode** or **Stations import mode** drop-down list, select one of the collision resolving option:

   - **Save import data for all**—delete all information on duplicated objects from the current Dr.Web Server database and overwrite it with the information from the imported database. The action is applied simultaneously to all duplicated objects in this table.
   - **Save current data for all**—save all information on duplicated objects from the current Dr.Web Server database. Information on duplicated objects from the imported database will be ignored. The action is applied simultaneously to all duplicated objects in this table.
   - **Select manually**—specify the action for each duplicated objects manually. In this mode, the list of duplicated objects become editable. Set the options for those objects, which will be saved.

   Click **Save**.

10.13.2. Dr.Web Server Statistics

Via the Control Center, you can view the statistics on Dr.Web Server operating on the level of system resources usage of a computer on which Dr.Web Server is installed and also network interaction with anti-virus network components and external resources such as GUS.

To view Dr.Web Server operation statistics

1. Select the **Administrating** item in the main menu of the Control Center.
2. In the opened window, select the **Dr.Web Server statistics** item of the control menu.
3. In the opened window, the following statistic data sections are presented:
   - **Customer activity**—data on number of served clients, which are connected to this Dr.Web Server: Dr.Web Agents, neighbor Dr.Web Servers and Dr.Web Agent installers.
   - **Network traffic**—parameters of incoming and outgoing network traffic for exchanging data with Dr.Web Server.
   - **System resources usage**—usage parameters of system resources of the computer on which Dr.Web Server is installed.
   - **Microsoft NAP**—NAP Validator operation parameters.
   - **Database usage**—parameters of the Dr.Web Server database accessing.
   - **File cache usage**—parameters of accessing the file cache of the computer on which Dr.Web Server is installed.
   - **DNS cache usage**—parameters of accessing the cache which stores queries to DNS servers on the computer on which Dr.Web Server is installed.
   - **Alerts**—parameters of the administrative notifications subsystem operation.
   - **Repository**—parameters of data exchange between the Dr.Web Server repository and GUS servers.
   - **Web statistics**—parameters of sending infection statistics to Doctor Web company servers.
   - **Web server statistics**—parameters of usage of the Web server.
   - **Cluster**—parameters of accessing via the interserver synchronization protocol in Dr.Web Server cluster system for multiserver network configuration.
   - **Multicast updates transfer**—parameters of data exchange at multicast updates transmission on workstations via the multicast protocol.
4. To view statistic data of specific section, click the section name.
5. In the opened list, the section parameters with dynamic counters of values are given.
6. At the statistic section opening, the graphical representation for each parameter changes is enabled. At this:
   - To disable graphical representation, click the section name. When graphical representation is disabled, the digital value of parameters still dynamically refreshes.

- To enable graphical representation of the data repeatedly, click the section name ones more.
- The names of the sections and their parameters for which the graphical representation is enabled, are marked with the bold font.

7. To adjust the data refresh frequency, select the desired period in the **Refresh rate** drop-down list on the toolbar. A new period will be automatically applied to both digital and graphical data.
8. On mouse hover over the graphical data, the selected point digital value is displayed as the following:
   - **Abs**—parameter absolute value.
   - **Delta**—incrementation of the parameter value relative to its previous value according to the data refresh rate.
9. To hide the section parameters, click the arrow on the left of the section name. When the section parameters are hidden, the graphical statistic data is cleared and on the parameters opening, the drawing starts from the beginning.

10.13.3. Backups

The **Backups** section allows to view as files and folders and also save locally contents of Dr.Web Server critical data backup copies.

During backup, the following objects are saved: repository settings, configuration files, encryption keys, certificates, embedded database backup.

Dr.Web Server critical data backup copies are saved in the following cases:

- As a result of the **Back up critical Dr.Web Server data** task execution according to the Dr.Web Server schedule.
- As a result of back up when running the Dr.Web Server executable file from the command line with the backup switch. This command is described in details in the **Appendices** document, G3.5. Backup of Dr.Web Server Critical Data.

View Information on Backups

To view information on the backup, select the object related to the necessary backup in the hierarchical tree. Backups are placed in the tree according to the directories of their storage: the default folder (`var/opt/drwcs/backup` for Dr.Web Server under Unix-like systems and `C:\DrWeb Backup` for Dr.Web Server under Windows OS)

- for Dr.Web Server under Linux: `/var/opt/drwcs/backup`,
- for Dr.Web Server under FreeBSD: `/var/drwcs/backup`,
- for Dr.Web Server under Windows: `C:\DrWeb Backup`,
- all paths to backup storage specified in the Dr.Web Server schedule tasks.

If there is a blank field specified in tasks of Dr.Web Server under Windows OS, the following folder will be used by default: `C:\Program Files\DrWeb Server\var\backup`. Only the backups stored inside the Dr.Web Server folder will be available for view.

If you change the directory for storing the backup in an already created task, the previously created directory will not be displayed in the web interface. In this case, you need to create a new task for the new directory.

When selecting backup directories or files, the properties panel with the following information on the object is opened: **Type**, **Size** (for separate file only), **Created on** and **Modification date**.

Manage Backups

To manage backups, use the following buttons on the toolbar:

 **Backup**—back up the Dr.Web Server critical data.

 **Export**—save the backup of selected object to the computer on which the Control Center is opened.

 **Delete selected objects**—delete objects selected in the tree without possibility to restore.

Backup Export

To save the backup locally

1. In the hierarchical tree, select the necessary backups (to select entire backup, it is enough to select in the tree the folder that corresponds to this backup), or separate files from the backup composition. To select several objects, use CTRL or SHIFT.

   Please note the general type of exported objects during the export:

   a) Zip archives of the backups are saved for the following selected objects:
      - One or several entire backups (when selecting folders which correspond to the backups).
      - Several separate files from the backups composition.

   b) Separate files from the backups composition. If only one file have been selected for the export, it will be saved as it is without archiving.

2. Click  **Export** on the toolbar.
3. Specify the path to save selected objects according to the web browser settings in which the Control Center is opened.

Back up

To back up the Dr.Web Server critical data, click **Backup** on the toolbar. The data will be saved into gz archive. Backup files are similar to files which are obtained when running the Dr.Web Server executable file from the command line with the backup switch.

This command is described in details in the **Appendices** document, G3.5. Backup of Dr.Web Server Critical Data.

10.13.4. Utilities

The set of available utilities depends on the Dr.Web Server repository settings. To enable or disable receiving updates from GUS of the utilities available in this section, refer the **Administration → General repository configuration → Dr.Web installation packages →** Dr.Web administrative utilities section.

In the **Utilities** section, you can download additional utilities to use with Dr.Web Enterprise Security Suite:

- **Dr.Web Agent for UNIX remote installation utility**

  The utility lets you remotely install Dr.Web Agent on workstations running Unix-like OS.

- **Dr.Web Agent for Windows remote installation utility**

  The utility lets you remotely install Dr.Web Agent on workstations running Windows OS.

- **Dr.Web Mobile Control Center**

  Serves for administrating the anti-virus network based on Dr.Web Enterprise Security Suite. Designed for installation and operation on mobile devices under iOS and Android OS.

- **Dr.Web utility for collecting information on a system**

  The utility is designed to generate the report on the state of a system and all installed software, including Dr.Web anti-virus solutions for protected stations and Dr.Web Server software. The report archive can be used for diagnostics by the anti-virus network administrator, as well as for sending to the technical support service of Doctor Web company.

- **Dr.Web Server remote diagnostics utility**

  Allows remotely connect to Dr.Web Server for basic controlling and viewing the operation statistics. Graphical version of the utility is available for Windows OS only. See also Dr.Web Server Remote Access.

- **Dr.Web Server remote scriptable diagnostics utility**

  Allows remotely connect to Dr.Web Server for basic controlling and viewing the operation statistics. This version of the utility is adapted for use in scripts. See also Dr.Web Server Remote Access.

- **Digital keys and certificates generation utility**

  Allows to generate encryption keys and digital certificates as well as perform and verify digital signatures of files. The utility is an important tool for ensuring the security of connections between components of the anti-virus network.

- Dr.Web Repository Loader

  Serves to download Dr.Web Enterprise Security Suite products from the Global Update System. Graphical version of Dr.Web Repository Loader is available for Windows OS only.

- **Dr.Web for Windows removal utility**

  An emergency tool for removing incorrect or damaged installations of Dr.Web Agents for Windows software in cases when standard removal tools are not available or will not work. The utility is not designed to be used as the main Dr.Web software uninstallation tool.

To get information on command line switches to use the utilities, please refer the **Appendices** document, the **G7. Utilities** section.

10.13.5. Enterprise products

Availability of products depends on the Dr.Web Server repository settings. To enable or disable updates from GUS for specific products in this section, proceed to the **Administration → General repository configuration → Dr.Web installation packages →** Dr.Web enterprise products section.

In the **Enterprise products** section, you can download installation packages for different software products used in the Dr.Web Enterprise Security Suite anti-virus network:

- **Dr.Web Mobile Security Suite (Android)**

  A package to install Dr.Web Agent for Android on protected workstations.

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

  A package to install Dr.Web Mail Security Suite (IBM Lotus Domino Windows) on an enterprise mail server.

- **Dr.Web Desktop Security Suite (Linux)**

  A package to install Dr.Web Agent for Linux on protected workstations.

- **Dr.Web Desktop Security Suite (macOS)**

  A package to install Dr.Web Agent for macOS on protected workstations.

- **Dr.Web Server Security Suite (macOS)**

  A package to install Dr.Web Agent for macOS on protected servers.

- **Dr.Web Mail Security Suite (Microsoft Exchange Server)**

  A package to install Dr.Web Mail Security Suite (Microsoft Exchange Server) on an enterprise mail server.

- **Dr.Web Gateway Security Suite (Unix)**

  A package to install Dr.Web Gateway Security Suite (Unix) on an enterprise web gateway or a proxy server.

- **Dr.Web Mail Security Suite (Unix)**

  A package to install Dr.Web Mail Security Suite (Unix) on an enterprise mail server.

- **Dr.Web Server Security Suite (Unix)**

  A package to install Dr.Web Server Security Suite (Unix) on an enterprise file server.

- **Dr.Web Proxy Server**

  A package to install Dr.Web Proxy Server on a computer within the enterprise anti-virus network that is used as a proxy server.

- **Dr.Web Scanning Server**

  A package to install Dr.Web Scanning Server designed for processing anti-virus scanning requests from virtual machines in virtual environments.

- **Dr.Web NAP Validator**

  A package to install Dr.Web NAP Validator on a computer within the enterprise anti-virus network that is used as a network access protection server.

- **Dr.Web Agent for Active Directory**

  A tool for Dr.Web Agent installation via Active Directory.

- **Dr.Web Agent full installer**

  A package for a complete installation of both Dr.Web Agent for Windows and the anti-virus package on protected workstations.

- **Utility to change attributes for Active Directory objects**

  A tool for object attribute editing for authentication via Active Directory.

- **Utility for Active Directory scheme modification**

  A tool to make a new object class and describe its attributes for authentication via Active Directory.

10.14. Peculiarities of a Network with Several Dr.Web Servers

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

The connections between Dr.Web Servers can have an hierarchical structure, which allows optimally distribute the load between Dr.Web Servers.

To exchange information between Dr.Web Servers a special *interserver synchronization protocol* is used.

Features provided by interserver synchronization protocol:

- Distributing updates between Dr.Web Servers within anti-virus network.
- Immediate transmission of updates as soon as they are received from Dr.Web GUS servers.
- Transmitting statistic information on protection station states between connected Servers.
- Transmitting licenses for protected stations between neighbor Dr.Web Servers.

10.14.1. Building a Network with Several Dr.Web Servers

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

Dr.Web Enterprise Security Suite allows to connect such anti-virus networks by transferring data between Dr.Web Servers.

Dr.Web Server can send to another Dr.Web Server

- software and virus database updates (only one of them is to receive updates from Dr.Web GUS servers);
- information on events related to threats, statistics, etc.;
- licenses for protected stations (you can configure licenses propagation between Dr.Web Servers in the License Manager).

Dr.Web Enterprise Security Suite provides for two types of connections between Dr.Web Servers:

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

An example of a multi-server structure is presented in Figure 10-1.

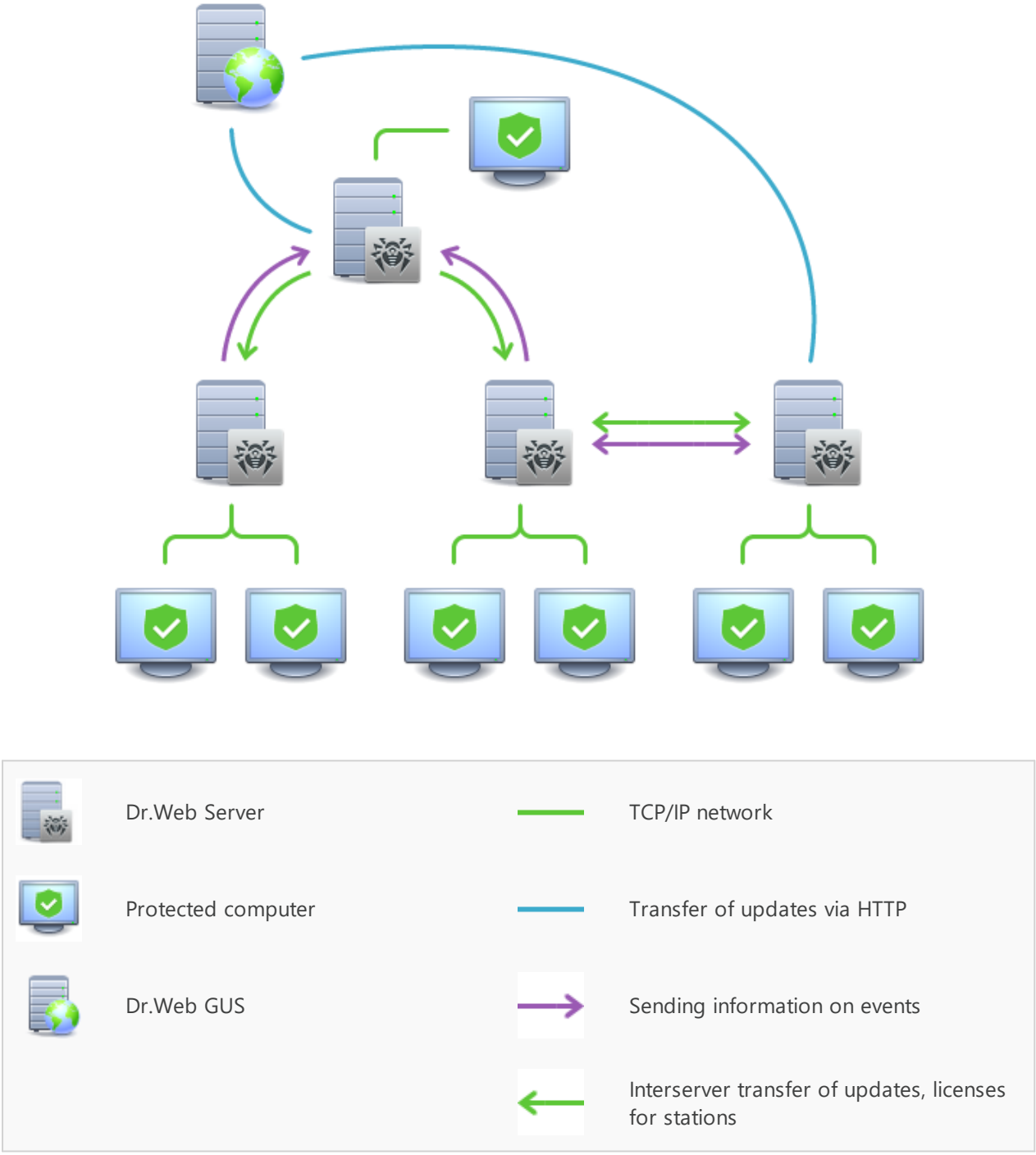


Figure 10-1. A multi-server network

Some advantages of the anti-virus network with several Dr.Web Servers:

1. Receiving of updates from Dr.Web GUS servers by one principle Dr.Web Server and their subsequent distribution to other Dr.Web Servers directly or through intermediates.

Dr.Web Servers that receive updates from the superior Dr.Web Server, do not receive updates from GUS even if such task is set in the schedule.

Still, in case the parent Dr.Web Server is inaccessible, it is recommended to keep the task for updating from the GUS on subordinate Dr.Web Servers. This allows Dr.Web Agents which are connected to the subordinate Dr.Web Server to receive updated virus databases and program modules (see also p. General Repository Configuration).

In the task for updating from GUS on the superior Dr.Web Server propagating updates, you must set up the receiving updates of the Dr.Web Server software for all operating systems installed on all subordinate Dr.Web Servers, which receive updates from this superior Dr.Web Server (see p. General Repository Configuration).

2. Distribution of workstations between several Dr.Web Servers, decreasing the load on each of them.
3. Consolidation of data from several Dr.Web Servers on one Dr.Web Server; the possibility to view all the data through Dr.Web Security Control Center connected to such Dr.Web Server.

   Dr.Web Enterprise Security Suite anti-virus monitors and prevents the creation of cyclic data flows.

4. Available licenses for protected stations can be donated to the neighbor Dr.Web Server. At this, the license key itself remains at the disposal of the distributing Dr.Web Server, available licenses are propagated to a neighbor Dr.Web Server for a specified time period and after it has expired, the licenses are revoked.

10.14.2. Setting Connections between Several Dr.Web Servers

To use several Dr.Web Servers in an anti-virus network, you should set up connections between these Dr.Web Servers.

It is recommended to make a plan of the anti-virus network structure first. All data flows, connections of the "peer to peer" and "parent-child" types should be indicated. Then, each Dr.Web Server included into the network connections with any "neighboring" Dr.Web Servers ("neighbors" have at least one dataflow between them) should be set up. After that, for each Dr.Web Server included into the network, you should set up connections with "neighboring" Dr.Web Servers ("neighbors" have at least one data flow between them).

If interserver connections between Dr.Web Servers are configured, several new features are added to administrator login area in the main menu.

Example of configuring of a connection between Parent and Child Dr.Web Servers

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

1. Make sure that both Dr.Web Servers operate normally.
2. To each of Dr.Web Servers give "meaningful" names, as it will help prevent mistakes while connecting and administering Dr.Web Servers. You can change the names through Dr.Web Security Control Center menu: **Administration** → **Dr.Web Server configuration** on the **General** tab in the **Name** field. In this example we name the parent Dr.Web Server `MAIN`, and the child Dr.Web Server—`AUXILIARY`.

   > Names specified at cofiguring will be automatically replaced with the computer names after connecting Dr.Web Servers.

3. On both Dr.Web Servers, enable the server protocol. To do this, on Dr.Web Security Control Center **Administration** menu, select **Dr.Web Server configuration**. On the **Modules** tab, set the **Dr.Web Server protocol** flag (see Modules).
4. Restart both Dr.Web Servers.
5. Via Dr.Web Security Control Center of the child Dr.Web Server (`AUXILIARY`), add the parent Dr.Web Server (`MAIN`) to the list of neighbor Dr.Web Servers.

   To do this, select **Anti-virus Network** item in the main menu. A window with the hierarchical list of the anti-virus network will be opened. To add a Dr.Web Server to the list, click the **Add a network object** → **Create neighbor** on the toolbar.

   A window with connection settings between the current and a new Dr.Web Server will be opened. Specify the following parameters:

   - **Type** of creating neighbor is **Parent**.
   - **Name**—the name of the parent Dr.Web Server (`MAIN`).
   - **Password***—an arbitrary password to access the parent Dr.Web Server.
   - **Own certificates of Dr.Web Server**—the list of SSL certificates of configuring Dr.Web Server. Click and select the `drwcsd-certificate.pem` certificate file of the current Dr.Web Server. To add one more certificate, click and add the certificate to a new field.
   - **Certificates of neighbor Dr.Web Server***—the list of SSL certificates of connecting parent Dr.Web Server. Click and select the `drwcsd-certificate.pem` certificate file of the parent Dr.Web Server. To add one more certificate, click and add the certificate to a new field.
   - **Address***—the network address of the parent Dr.Web Server and the connection port. Use the following format: *<Server_address>*:*<port>*.

   You can browse the list of Dr.Web Servers, available in the network. To do this:

   a) Click the arrow on the right of the **Address** field.

b) In the opened window, specify networks in the following format: with a hyphen (for example, `10.4.0.1-10.4.0.10`), separated by a comma with a whitespace (for example, `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`), with a network prefix (for example, `10.4.0.0/24`).

c) Click  to browse the network for available Dr.Web Servers.

d) Select the Dr.Web Server in the list of available Dr.Web Servers. Its address will be set to the Address field to create connection.

- **URL of Dr.Web Security Control Center**—you can specify the address of a start web page for Dr.Web Security Control Center of the main Dr.Web Server (see Dr.Web Security Control Center).
- In the **Connection parameters** drop-down lists, specify the type of creating neighbor Dr.Web Servers connection.
- In the **Encryption** and **Compression** drop-down lists, specify parameters of traffic encryption and compression between connecting Dr.Web Servers (see Traffic Encryption and Compression).
- **Automatic renewal period of donated licenses**—time period for which licenses are donated from the key on this Dr.Web Server. After this period, the donated licenses are automatically renewed for the same period. Automatic renewal is performed till the expiration of the license propagation period. The option is used if the main Dr.Web Server donates licenses to the current Dr.Web Server.
- **Interval for preliminary renewal of accepted licenses**—the setting is not used in creating a parent Dr.Web Server.
- **License synchronization period**—interval for synchronizing information about donating licenses between Dr.Web Servers.
- Flags in **Licenses**, **Updates** and **Events** sections are set according to parent-child type of connection and cannot be changed:
  - parent Dr.Web Server sends licenses to child Dr.Web Servers;
  - parent Dr.Web Server sends updates to child Dr.Web Servers;
  - parent Dr.Web Server receives information about events from child Dr.Web Servers.
- Configure administrator notification:
  - Set the **Send notifications on events of neighbor Dr.Web Server** flag to send notifications to the administrator about the events received from the configuring child Dr.Web Server. If the flag is cleared, the administrator will receive notifications on events only on the own Dr.Web Server. You can configure sending of certain notifications in the Notification Configuration section.
  - Set the **Send notifications on events of neighbor Dr.Web Server at threat detection by known hashes** flag to send notifications to the administrator about the events received from the configuring child Dr.Web Server in case of security threat detection by known hashes of threats. If the flag is cleared, the administrator will receive notifications on events only on the own Dr.Web Server. You can configure sending of certain notifications in the Notification Configuration section.
    The flag is available only if the usage of bulletins of known threat hashes is licensed.

You can check the license in the information on a license key that can be found in the License Manager section, the **Allowed lists of hash bulletins** parameter (the license in at least one of the license keys used by the Dr.Web Server is sufficient).

- Set the **Synchronize data on hardware and software installed on stations via interserver connections** flag to send collected data about hardware, software, and Windows OS updates installed on connected stations to the child Dr.Web Server you are configuring. The data will be sent immediately once the created neighbor Dr.Web Server is connected, and it will be updated should there be any changes in stations' hardware or software in future.
  This kind of statistics is collected only from the stations protected by Dr.Web Agent for Windows and only after the corresponding option is enabled in the Dr.Web Server and Dr.Web Agent configuration, as described in the Hardware and Software on Stations under Windows OS section.

Enabling these options may significantly increase the number of received notifications.

When configuring peer Dr.Web Servers, these options are available only if the **Receive** flag is set in the **Events** section.

The following notifications are available about events on the neighbor Dr.Web Server: **Security threat detected**, **Report of Preventive protection**, **Scan error**, **Scan statistics**.

The following separate notifications are provided about event on the neighbor Dr.Web Server in case of security threat detection by known hashes of threats: **Security threat detected by known hashes of threats**, **Scan error at threat detection by known hashes of threats**, **Report of Preventive protection on threat detection by known hashes of threats**.

- In the **Update restrictions** → **Events** section, you can configure the schedule of events transmission from the current Dr.Web Server to the parent one (editing of the **Update restrictions** table is the same as editing schedule table in the Update Restrictions for Workstations section).

Click **Save**.

As a result, the Parent Dr.Web Server (MAIN) will be included to the **Parents** and **Offline** folders (see Figure 10-2).

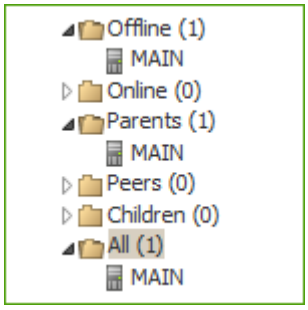


Figure 10-2.

6. Open Dr.Web Security Control Center of the parent Dr.Web Server (`MAIN`) and add the child Dr.Web Server (`AUXILIARY`) to the list of neighbor Dr.Web Servers.

   To do this, select **Neighborhood** item in the main menu. A window with the hierarchical list of the anti-virus network will be opened. To add a Dr.Web Server to the list, click the **Add a network object** → **Create neighbor** on the toolbar.

   A window with connection settings between the current and a new Dr.Web Server will be opened. Specify the following parameters:

   - **Type** of creating neighbor is **Child**.
   - **Name**—the name of the child Dr.Web Server (`AUXILIARY`).
   - **Password***—type the same password as at step **5**.
   - **Own certificates of Dr.Web Server**—the list of SSL certificates of configuring Dr.Web Server. Click and select the `drwcsd-certificate.pem` certificate file of the current Dr.Web Server. To add one more certificate, click and add the certificate to a new field.
   - **Certificates of neighbor Dr.Web Server***—the list of SSL certificates of connecting child Dr.Web Server. Click and select the `drwcsd-certificate.pem` certificate file of the child Dr.Web Server. To add one more certificate, click and add the certificate to a new field.
   - **URL of Dr.Web Security Control Center**—you can specify the address of a start web page for Dr.Web Security Control Center of the child Dr.Web Server (see Dr.Web Security Control Center).
   - In the **Connection parameters** drop-down lists, specify the type of creating neighbor Dr.Web Servers connection.
   - In the **Encryption** and **Compression** drop-down lists, specify parameters of traffic encryption and compression between connecting Dr.Web Servers (see Traffic Encryption and Compression).
   - **Automatic renewal period of donated licenses**—the setting is not used in creating a connection to a child Dr.Web Server.
   - **Interval for preliminary renewal of accepted licenses**—time interval before the expiration of the licenses automatic renewal period, from which this Dr.Web Server requests the preliminary automatic renewal of these licenses. The option is used if the child Dr.Web Server receives licenses from the current Dr.Web Server.
   - **License synchronization period**—the setting is not used in creating a connection to a child Dr.Web Server.
   - Flags in **Licenses**, **Updates** and **Events** sections are set according to *parent-child* type of connection and cannot be changed:
     - child Dr.Web Server receives licenses from the main Dr.Web Server;
     - child Dr.Web Server receives updates from the main Dr.Web Server;
     - child Dr.Web Server send information about events to the main Dr.Web Server.
   - The following options are disabled and cannot be changed because the child Dr.Web Server does not receive events from the main Dr.Web Server: **Send notifications on**

events of neighbor Dr.Web Server, **Send notifications on events of neighbor Dr.Web Server at threat detection by known hashes** and **Synchronize data on hardware and software installed on stations via interserver connections**.

- In the **Update restrictions** → **Updates** section, you can configure the schedule of updates transmission from the current Dr.Web Server to the child one (editing of the **Update restrictions** table is the same as editing schedule table in the Update Restrictions for Workstations section).

Click **Save**.

As a result, the child Dr.Web Server (AUXILIARY) will be included to the **Children** and **Offline** folders (see Figure 10-3).

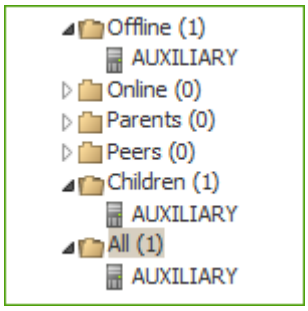


Figure 10-3.

7. Wait until the connection between Dr.Web Servers is established (usually it takes not more than a minute). Press f5 from time to time to update the Dr.Web Server list. After Dr.Web Servers have been connected, the child Dr.Web Server (AUXILIARY) will move from the **Offline** folder to the **Online** folder (see Figure 10-4).

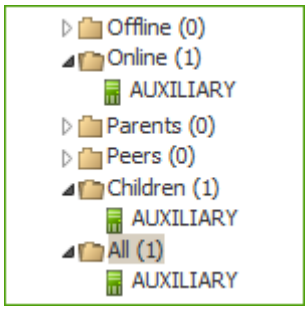


Figure 10-4.

8. Open Dr.Web Security Control Center of the child Dr.Web Server (AUXILIARY) to make sure that the parent Dr.Web Server (MAIN) is connected to the child Dr.Web Server (AUXILIARY) (see Figure 10-5).

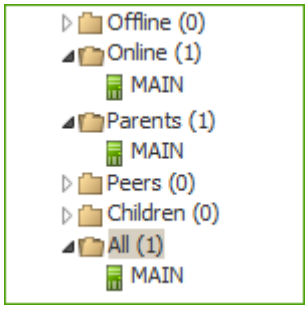


Figure 10-5.

You may not connect several Dr.Web Servers with the same pare of parameters: password and the SSL certificate.

For peer to peer connections between Dr.Web Servers, it is recommended to set Dr.Web Server address in the settings for one of them only. It will not take effect on the Dr.Web Servers interconnection, but allows to avoid messages like **Link with the same key id is already activated** in the Dr.Web Servers log files.

However, specifying the address of the connected Dr.Web Server on one side is mandatory.

Connection between two Dr.Web Servers can be failed because of the following reasons:

- Network problems.
- Wrong address of the parent Dr.Web Server was set during connection setup.
- Wrong certificates at one of connecting Dr.Web Servers.
- Wrong access password at one of connecting Dr.Web Servers (passwords on connecting Dr.Web Servers do not match).

If you need to establish a new interserver connection between Dr.Web Servers of 10 and 13 versions, perform the following additional actions:

1. When creating a connection, specify the public key of Dr.Web Server v.13 on Dr.Web Server v.10.
2. Generate certificate from the private key of Dr.Web Server v.10 using the `drwsign` utility (the `gencert` command) from Dr.Web Server v.13 kit (see the **Appendices** document, G7.1. Digital keys and certificates generation utility). Specify this certificate when creating a connection on Dr.Web Server v.13.

10.14.3. Using an Anti-Virus Network with Several Dr.Web Servers

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

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

The administrator can receive consolidated data about important events on network segments linked to any Dr.Web Server via interserver connections.

To view information on events on all Dr.Web Servers linked to the current Dr.Web Server

1. Select **Anti-virus Network** item in the main menu of the Control Center. In the anti-virus network tree, in the **Neighbors** group, select the neighbor Dr.Web Server information of which you want to view.
2. In the control menu, select **General** → **Hardware and software**, to view the statistics on hardware and software on protected stations connected to the selected neighbor Dr.Web Server.

   Information given in this section, is the same as the information in the sections for stations connected to your Dr.Web Server (see Hardware and Software on Stations under Windows OS).
3. To view statistics on anti-virus components operation on protected stations connected to the selected neighbor Dr.Web Server, select corresponding item in the **Statistics** section of the control menu.

   Information given in this section, is the same as the information in the sections for stations connected to your Dr.Web Server (see Statistics).

10.14.4. Dr.Web Server Cluster

For information on updating Dr.Web Servers within a cluster, see Updating Dr.Web Servers in a Cluster.

For information on restoring a cluster node after a Dr.Web Server fatal failure, see **Appendices**, the Restoring a Dr.Web Server Cluster Node

When creating a Dr.Web Server cluster in the anti-virus network, follow the directions below:

1. Configuration files

`webmin.conf`—does not require unification on all cluster servers.

`drwcsd.conf`—a number of settings require unification:

- Available only in the configuration file:

Parameters	Values
`<passwd-salt value=''/>` Cryptographic salt value to encrypt the administrator password in the database	the same

Parameters	Values
`<id value=''/>` Unique Dr.Web Server identifier from license key	different

- Can be changed from the Control Center (**Dr.Web Server Configuration**):

Tabs	Parameters	Values
General	**Dr.Web Server name**	empty or different
	Dr.Web Server language, **Number of parallel requests from clients**, **Number of backups for the Dr.Web Server versions**	irrelevant
	other	the same
Traffic	**Updates and Installations**	the same
Network	**DNS**, **Proxy**	irrelevant
	Transport: **Encryption**, **Compression**; settings related to the **Multicasting** mode	the same
	Transport: other	irrelevant
	Email, **Cluster**, **Download**	the same
	Multicast updates	recommended to leave it on one server of the cluster and turn it off on the other servers
Statistics, **Security**, **Cache**, **Modules**, **Licenses**	all	the same
Location, **Log**	all	irrelevant
Database	**Number of connections**, **Restore corrupted image automatically**	irrelevant
	other	the same

2. The same Dr.Web Server name

For all Dr.Web Servers, the same DNS name of Dr.Web Server must be specified to be used for generating Dr.Web Agent installation files for the anti-virus network stations.

This name is specified via the Control Center: **Administration** → **Dr.Web Server configuration** → **Network** tab → Download tab → **Dr.Web Server address** field. Settings of

this section are stored in the `download.conf` configuration file (description of the file is given in the **Appendices** document, F3. Download.conf Configuration File).

3. Cluster usage setup

On the network DNS server, the common cluster name must be registered for each Dr.Web Server and a load balancing method must be set.

For automatic application of settings in a Dr.Web Server cluster, the cluster protocol must be used.

To configure the cluster protocol, open the **Administration** → **Dr.Web Server configuration** menu in the Control Center of each Dr.Web Server and specify the following settings:

a) To enable the cluster protocol, on the Modules tab, set the **Dr.Web Servers cluster protocol** flag.

b) To configure parameters for interaction of Dr.Web Servers within a cluster, specify the corresponding parameters on the Cluster tab.

For example:

- **Multicast group**: `232.0.0.1`
- **Port**: `11111`
- **Interface**: `0.0.0.0`

In this example, transports for all interfaces are configured for all Dr.Web Servers of a cluster. In other cases, e.g., if one of the networks is external for the cluster and Dr.Web Agents connect from it, and the second network is internal for the cluster, the cluster protocol should be used only for interfaces of the internal network. In this case, the following addresses must be set as interfaces: `192.168.1.1`, ..., `192.168.1.N`.

After configuring the necessary parameters, click **Save** and restart the Dr.Web Servers.

4. The same database

To be able to work with a common database, all Dr.Web Servers must be the same version.

All Dr.Web Servers within one cluster must use the same external database.

As in the case of database use outside of a cluster, each of Dr.Web Servers calls the database independently and all Dr.Web Server data is stored separately. Wherever relevant, a Dr.Web Server only gets database records for its ID, which is unique for each Dr.Web Server. Usage of the same database allows Dr.Web Servers to communicate with Dr.Web Agents that were initially registered on other Dr.Web Servers of a cluster.

When creating a Dr.Web Server cluster with the same database, please consider the following points:

- The database may be installed either separately from all Dr.Web Servers or on one of the computers on which Dr.Web Server of a cluster is installed.

- The database must be created before the installation of the first Dr.Web Server of a cluster or before the connection of the first Dr.Web Server to the database.
- When adding new hosts to the cluster (except the first Dr.Web Server), it is not recommended to set the common database which is used in this cluster during the Dr.Web Server installation. Otherwise, it may cause deletion of the information already stored into the database. It is recommended to install Dr.Web Servers with the embedded database at first and to switch them to the common external database after the installation.
  You can switch Dr.Web Servers to the external database via the Control Center: in the **Administration** → **Dr.Web Server configuration** → on the Database tab or via the `drwcsd.conf` Dr.Web Server configuration file.
- Except for the first Dr.Web Server of a cluster, it is not recommended to add Dr.Web Servers already operating within an anti-virus network with another external or embedded database to a cluster. It will cause the loss of data, such as information on stations, statistics, settings (except the settings stored in the configuration files), because data is completely erased from the database during the import. In this case, only some settings can be imported.
- By default, after installation or upgrade of Dr.Web Servers from previous versions, a cryptographic salt value is randomly generated in the configuration file (`drwcsd.conf`) to encrypt the administrator password stored in the database. To prevent any authentication issues, make sure to manually set the same salt value on every Dr.Web Server included in the cluster. See the required configuration parameter in the **Appendices** document, F1. Dr.Web Server Configuration File.

5. **The same version of the repository**

   On all Dr.Web Servers of a cluster, repositories must contain updates of the same version.

   You can reach this requirement by one of the following ways:

   - Update all Dr.Web Servers of a cluster from the GUS simultaneously. In this case, all Dr.Web Servers contain the latest version of updates. All Dr.Web Servers repositories can also be configured to update from a local update zone (GUS mirror) which will distribute the same confirmed version of product updates, or the latest version if the GUS mirror is created.
   - You can create a hybrid structure that combines both a cluster of Dr.Web Servers and a hierarchical structure based on interserver connections. In this case one Dr.Web Server (may be either a Dr.Web Server within a cluster or not included into a cluster) is assigned as a parent and receives updates from the GUS. The other Dr.Web Servers of the cluster are the child hosts and receive updates from the parent Dr.Web Server via the interserver connections.

   If Dr.Web Servers of a cluster are configured to receive updates from the local zone or from the parent Dr.Web Server, it is necessary to monitor the functionality of this zone or the parent Dr.Web Server. If a host that distributes updates stops functioning, it is necessary to reconfigure one of the other Dr.Web Servers to operate as a parent Dr.Web Server or create a new update zone for receiving updates from the GUS correspondingly.

6. **Distribution of station licenses**

   To distribute licenses between Dr.Web Servers of a cluster, you can use the following approaches:

   a) Do not configure a hierarchical structure of Dr.Web Servers within the cluster. It is enough to add a license key (or several keys) on one of the Dr.Web Servers of a cluster. Information on this license key will be added to the common database. Thus, the license key will be used by all Dr.Web Servers of the cluster simultaneously. The total number of licenses stored in the common database must correspond to the total number of stations served by all Dr.Web Servers of the cluster.

   To use a license key on all Dr.Web Servers of a cluster instead of only on the one on which the key was added, the other Dr.Web Servers of a cluster must be restarted after the key is added.

   b) Create a hybrid structure that combines both a cluster of Dr.Web Servers and a hierarchical structure based on interserver connections. This kind of structure is useful if Dr.Web Agents are serviced by Dr.Web Servers that are both included into the cluster and outside the cluster. In this case, the necessary number of licenses is propagated from a license key via the interserver connection directly during server operation:

   - From Dr.Web Server outside the cluster to one of the Dr.Web Servers of the cluster. Propagated licenses are used by all Dr.Web Servers of the cluster as described in step **a)**.
   - From one of the Dr.Web Servers of the cluster (i.e. from the key used by all Dr.Web Servers of the cluster) to a Dr.Web Server outside the cluster.

   The administrator of the anti-virus network should manually configure propagation of a necessary number of licenses for a necessary time period (for more details, see Donating Licenses via Interserver Connections).

   For example, you can configure a hierarchical structure of Dr.Web Servers and allocate the parent Dr.Web Server (may be either a Dr.Web Server within a cluster or not included into a cluster) which will propagate both repository updates and licenses from a license file.

7. **Tasks in the Dr.Web Server schedule**

   To avoid duplicates in queries to the database, make sure to execute the following tasks from the Dr.Web Server schedule only on one of Dr.Web Servers: **Purge old records**, **Back up critical Dr.Web Server data**, **Purge old stations**, **Purge unsent events**. For example, execute them on the Dr.Web Server located on the same computer as the common external database, or on the most powerful computer of a cluster if the configurations of the Dr.Web Servers are different and the database is located on a separate computer.

Chapter 11: Updating Dr.Web Enterprise Security Suite Software and Its Components

This chapter describes how to update Dr.Web Enterprise Security Suite components. The update is performed while the product is in use; this procedure cannot be used to upgrade to a newer version.

The procedure for upgrading the product and its components to a newer version is described in the **Installation Manual**, see Chapter 7: Upgrading Dr.Web Enterprise Security Suite Software and Its Components.

Before updating Dr.Web Enterprise Security Suite and its components, it is strongly recommended to ensure the validity of the TCP/IP protocol settings to provide the internet connection. Particularly, the DNS service must be enabled and properly configured.

Before updating the software it is recommended to configure the repository including access to Dr.Web GUS (see General Repository Configuration).

11.1. Updating Dr.Web Server and Restoring it from Backup

The Control Center provides the following capabilities for managing the Dr.Web Server software:

- Updating the Dr.Web Server software to one of the available versions downloaded from GUS and stored in the Dr.Web Server repository. The settings for updating the repository from GUS are described in section Administration of Dr.Web Server Repository.
- Rolling back the Dr.Web Server software to the saved backup. Dr.Web Server backups are created automatically when updating to a newer version in the **Dr.Web Server Updates** section (step 4 in the procedure below).

Dr.Web Server can be also upgraded using the Dr.Web Server distribution kit. The procedure is described in the **Installation Manual**, section Administration of Dr.Web Server Repository or Upgrading Dr.Web Server for Unix-like OS.

Not all Dr.Web Server updates have the distribution kit file. Some of them can be installed via the Control Center only.

After upgrading Dr.Web Server under Unix-like OS using the Control Center, the Dr.Web Server version in the OS package manager will not change.

Managing Dr.Web Server software

1. Select the **Administration** item in the main menu of the Control Center, in the window that opens, select **Dr.Web Server** in the control menu.
2. To open the Dr.Web Server version list, click the **View list of versions** link.
3. This opens the **Dr.Web Server Updates** section with the list of available updates and backups of Dr.Web Server.
   - The **Current version** section contains the version of Dr.Web Server currently in use. The **Change list** section contains the brief list of new features and the list of errors that have been resolved in this version compared to the previous update version.
   - The **Available updates** section contains the list of updates for this Dr.Web Server downloaded from GUS. The **Change list** section contains a brief list of new features and a list of errors resolved in each update.
     For the initial version of Dr.Web Server, installed from the installation package, in the **Change list** is empty.
   - The **Backups** section contains the list of backup copies which are stored for this Dr.Web Server. The **Date** section contains the information on the date of the backup.
4. *To update* the Dr.Web Server software, select the check box next to the necessary version of Dr.Web Server in the **Available updates** list and click **Apply**.

   You can update only to a later version of Dr.Web Server in relation to the version currently in use.

   During the Dr.Web Server update, the current version is saved as a backup (placed to the **Backups** section), and version to which update is performed, is moved from the **Available updates** to the **Current version** section.

   Backup copies are saved in the following folder:

   `var → update → backup →` *<old_version>-<new_version>*

   During the update, the `var → dwupdater.log` log file is created or modified.
5. *To rollback* the Dr.Web Server software to a saved backup copy, select the check box next to the required version of Dr.Web Server in the **Backups** list and click **Apply**. During the rollback of the Dr.Web Server software, the applied backup copy is placed in the **Current version** section.
6. *To restore* the integrity of Dr.Web Server and roll back to the state of current revision click the **Restore Server** button.
   The integrity of the server software will be restored without saving a backup copy, updating the database and configuration files. If this revision is absent in the repository, recovery is impossible.

11.2. Updating Dr.Web Servers in a Cluster

There are two ways to update Dr.Web Servers within a cluster:

Using installation packages

In this case, it is required to stop all Dr.Web Servers and update them one by one.

The procedure is described in the **Installation Manual**, section Chapter 7: Upgrading Dr.Web Enterprise Security Suite Software and Its Components

Using Control Center

This method involves removing the nodes from the cluster, switching them over to the embedded DB and updating them one by one. After updating all the nodes, connect them back to the common cluster. To do this:

1. Remove all Dr.Web Servers from the cluster except the one that will update the cluster DB: on all Dr.Web Servers in the cluster except one, navigate to **Administration** → **Dr.Web Server configuration** → **Modules** tab and clear the **Dr.Web Servers cluster protocol** check box. Click the **Save** button and restart the station.
2. Switch over the Dr.Web Servers that were removed from the cluster to another DB, for example, the embedded one: go to **Administration** → **Dr.Web Server configuration** → **Database** tab and select **SQLite3** from the **Database** drop-down list. For more information about connecting to a database, see the Database section.
3. Disable Dr.Web Agent connections to these Dr.Web Servers: go to **Administration** → **Dr.Web Server configuration** → **Modules** tab and clear the **Dr.Web Agent protocol** check box. Click the **Save** button and restart the station.
4. Stop all the Dr.Web Servers that were removed from the cluster.
5. Update the Dr.Web Server hosting the cluster DB.
6. Start and update the remaining Dr.Web Servers one by one via the Control Center. After updating the last server, switch them back to the cluster DB: go to **Administration** → **Dr.Web Server Configuration** → **Database** tab and select the cluster DB in the **Database** drop-down list. For more information about connecting to a database, see the Database section.
7. Allow Dr.Web Agent connections: go to **Administration** → **Dr.Web Server configuration** → **Modules** tab and set the **Dr.Web Agent protocol** check box. Click the **Save** button and restart the station.
8. Add the Dr.Web Servers back to the cluster: go to **Administration** → **Dr.Web Server configuration** → **Modules** tab and set the **Dr.Web Servers cluster protocol** check box. Click the **Save** button and restart the station.

If there are many Dr.Web Servers and updating them may take a long time, it is possible to update only some of them and create a separate cluster with them in it while the rest are updated to maintain continuous operation.

The procedure is described in the Updating Dr.Web Server and Restoring it from Backup section.

11.3. Manual Update of Dr.Web Server Repository

To view the repository status or update anti-virus network components

1. Select the **Administration** item in the main menu of the Control Center and click **Repository state** in the control menu of the opened window.
2. In the opened window you can view the list of products in the repository, the date of the currently used revision, the date of the last downloaded revision, and the status of the products.

   The **State** column displays the status of the products in the Dr.Web Server repository at the time of the last update.

3. To manage the repository contents, use the following buttons:
   - Click the **Check for updates** button to check whether updates for all of the products are available on the GUS servers. If the checked component is outdated, it will be updated automatically during the check.
   - To save the log of repository updates, click one of the following buttons on the toolbar:
     - **Save data in CSV file**,
     - **Save data in HTML file**,
     - **Save data in XML file**,
     - **Save data in PDF file**.
   - Click **Reload repository from disk**, to reload the current version of the repository from disk.

   At startup, Dr.Web Server loads the repository contents to memory. If during the Dr.Web Server operation the administrator changed the contents without using the Control Center, for example, when updating the repository using an external utility or manually, reload the repository to enable the use of its downloaded version.

11.4. Scheduled Update of Dr.Web Server Repository

You can configure a task schedule on Dr.Web Server for regular software updates (for more details about the schedule, see section Setting Dr.Web Server Schedule).

Configuring the schedule for updating the Dr.Web Server repository

1. Select **Administration** in the main menu and then navigate to **Dr.Web Server Task Scheduler** in the control menu. The list of Dr.Web Server current tasks will open.
2. To add a new task, click **Create task** on the toolbar. The Task editor window will open.
3. On the **General** tab, specify the following parameters:
   - In the **Name** field, specify the name of the task that will be displayed in the schedule list.
   - Select the **Enable execution** check box, to enable the execution of the task. If the check box is cleared, the task remains on the list but will not be executed.
   - Select the **Critical task** check box to perform an out-of-sequence launch of the task if its scheduled execution has been skipped for any reason. The Scheduler rechecks the task list every minute and launches the skipped critical task if it was found. If the task has been skipped several times, it will be run only once.
   - If the **Run the task asynchronously** check box is cleared, the task will be added to the general queue of Scheduler tasks that are executed sequentially. Select the check box to run this task in parallel out of sequence.
4. On the **Action** tab, specify the following parameters:
   - From the **Action** drop-down list, select the **Update repository** task type.
   - In the **Product** list, select the check boxes next to the repository products which will be updated by this task.
   - Select the **Update license keys** to activate the automatic license key update procedure during the repository update. Detailed information is given in the Automatic License Renewal section.
5. On the **Time** tab, specify the following parameters:
   - In the **Period** drop-down list, select the task launch mode and set the time according to the specified periodicity:
   - Select the **Disable after the first execution** check box to execute the task only once at the specified time. If the check box is cleared, the task will be executed multiple times according to the specified periodicity.
6. Click **Save** to create a new task with the specified parameters.

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

If Dr.Web Server is not connected to the internet to receive repository updates from GUS servers, the following update configurations are possible:

- If you have another Dr.Web Server in the network that is connected to the internet to receive updates, configure the inter-server connection with this Dr.Web Server as peep-to-peer or as parent-child where the Dr.Web Server not connected to the internet will be a child. In this

case, the Dr.Web Server not connected to the internet will automatically receive all updates from the parent Dr.Web Server.

The configuration of inter-server connections is described in the Peculiarities of a Network with Several Dr.Web Servers section.

- If you cannot configure automatic update from another Dr.Web Server via inter-server connection, you can update the repository of the disconnected Dr.Web Server manually:
  - If you have another Dr.Web Server in the network that is connected to the internet to receive updates, transfer the repository contents from the updated Dr.Web Server manually, as described in the Copying Repository from Another Dr.Web Server section.
  - If you cannot connect any of Dr.Web Servers to the internet to receive updates, you can download the repository from GUS without using the Dr.Web Server software. To do this, use the standard Dr.Web Repository Loader utility included in the repository.

GUI version of Dr.Web Repository Loader utility is available for Windows OS only and can be downloaded in the following ways:

- from https://download.drweb.com. After entering the serial number and selecting the product type, the **Download Wizard** table opens where you can select the required Dr.Web repository loader.
- via the Control Center, in the **Administration** → **Utilities** section. The utility is located in the `webmin\utilities` folder of the Dr.Web Server installation folder (executable file is `drweb-reploader-gui-windows-<bitness>.exe`). If it is missing, download it by following the instruction.

A console version of the utility is also available.

11.5.1. Copying Repository from Another Dr.Web Server

If Dr.Web Server is not connected to the internet, its repository can be updated manually by copying the repository of another updated Dr.Web Server.

This method is not intended for upgrading Dr.Web Server to a new version.

Deploying the repository updates from another Dr.Web Server

1. Update the repository of Dr.Web Server connected to the internet from the **Administration** → Repository State section of the Control Center.
2. Export the repository or its part (the required products) from the Repository Content section of the Control Center. You should export only whose types of objects that are supported to be imported.
3. Copy the archive with the exported repository to the computer with the Dr.Web Server to be updated.

   Import the downloaded repository to Dr.Web Server via the Control Center in the **Administration** → Repository Content section.

If you use specific repository settings such as frozen revisions or if you update Dr.Web Agents only from the specified revision (not from the latest), then you should enable the **Add missing revisions only** option and disable the **Import configuration files** option when importing the repository.

11.5.2. Dr.Web Repository Loader

If you cannot connect any of Dr.Web Servers to the internet, you can download the repository from GUS without using the Dr.Web Server software. To do this, use the standard Dr.Web Repository Loader utility.

Features

- To download the repository from GUS, you need a license key of Dr.Web Enterprise Security Suite or its MD5 hash which you can view in the **Administration** → **License Manager** section of in the Control Center.
- You can launch Dr.Web Repository Loader in the following modes:
  - graphical version of the utility (under Windows OS only),
  - console version of the utility.
- You can use a proxy server when downloading the repository from the GUS.

The composition of the repository products is described in the Administration of Dr.Web Server Repository section.

If the version of Dr.Web Server is changed, the list of products available for download will also change. Please click the **Update list** button in the list of products and ensure that all required products are selected.

Possible Uses

Download and manual replacement

1. Download the Dr.Web Server repository from GUS using the Dr.Web Repository Loader utility.

   When downloading, create an archive of the repository:

   a) When using the graphical utility: select the **Load repository** mode and select the **Archive repository** check box in the main utility window.

   b) When using the console utility: use the `--archive` switch.
2. Copy the archive with the exported repository to the computer with Dr.Web Server to be updated.

Import the downloaded repository to Dr.Web Server via the Control Center from the **Administration** → Repository Content section.

If you use specific repository settings such as frozen revisions or if you update Dr.Web Agents only from the specified revision (not from the latest), then you should enable the **Add missing revisions only** option and disable the **Import configuration files** option when importing the repository.

Create the repository mirror on a local network server

1. Download the Dr.Web Server repository from GUS using the Dr.Web Repository Loader utility.

   When downloading, set the **Synchronize update mirror** option in the main utility window.
2. Upload the downloaded repository to your LAN web server that will be used to propagate repository updates.
3. In the **Administration** → General Repository Configuration section, configure Dr.Web Server to receive updates from your local mirror and not from Dr.Web GUS. The protocol for downloading updates depends on the type of the server in step 2: HTTP/HTTPS for web server, FTP/FTPS for FTP server, etc. The exception is the FILE protocol—it cannot be used on network (see below).

Create the repository mirror on Dr.Web Server

1. Download the Dr.Web Server repository from GUS using the Dr.Web Repository Loader utility.

   When downloading, set the **Synchronize update mirror** option in the main utility window.
2. Put the downloaded mirror in any folder on the computer where Dr.Web Server is installed.
3. In the **Administration** → General Repository Configuration section, configure receiving the updates via the FILE protocol.

   In the **Base URI** field, specify the local path to the mirror folder. The **List of Dr.Web Global Update System Servers** parameter is not used.

Make sure that the mirror is located in the folder named `13.00`. Note that the path in the **Base URI** field must be specified up to this folder, not including the folder itself.

11.5.2.1. GUI Utility

The GUI version of the Dr.Web Repository Loader utility is available for Windows OS and can be downloaded from the Control Center, in the **Administration** → **Utilities** section. You can run this utility version on any computer running Windows OS with internet access.

The utility is located in the `webmin\utilities` folder of the Dr.Web Server installation directory. The executable file is `drweb-reploader-gui-windows-<bitness>.exe`.

Downloading the repository using the GUI version of Dr.Web Repository Loader

1. Run the GUI version of the Dr.Web Repository Loader utility.
2. In the main window of the utility, specify the following parameters:
   a) **License key or MD5 of the key**—specify Dr.Web license key file. Click **Browse** and select the active license key file. Instead of a license key you can specify only the MD5 hash of a license key, which you can view in the Control Center in the **Administration** → **License Manager** section.
   b) **Downloading folder**—specify the folder for downloading the repository.
   c) In the **Mode** list, select one of the following update loading modes:
      - **Load repository**—the repository is downloaded in the Dr.Web Server repository format. The downloaded files can be directly imported via the Control Center as the Dr.Web Server repository updates.
      - **Synchronize update mirror**—the repository is downloaded in the GUS updates zone format. The downloaded files can be placed on the update mirror in your local network. Further, Dr.Web Servers can be configured to receive updates directly from this update mirror containing the latest version of the repository but not from the GUS servers.
   d) Select the **Archive** check box in the **Administrating** → Repository Content section to pack downloaded repository into a zip archive automatically. This option allows you to have a prepared archive file ready to be imported to Dr.Web Server via the Control Center.
3. If you want to change the additional settings for GUS connections and update downloads, click **Additional settings**. The opened settings window displays the following tabs:
   a) On the **Products** tab, you can change the list of products to be downloaded. The opened settings window displays the list of all repository products available for download from the GUS:
      - To update the list of products currently available on the GUS, click **Update**.
      - Select the check boxes next to the products that you want to download from the GUS or select the check box at the top of the table to select all products from the list.
   b) On the **Dr.Web GUS** tab, you can configure the parameters of update servers:
      - GUS servers are listed in the order in which the utility contacts them when downloading the repository. To change the order of the GUS servers, use the **Up** and **Down** buttons.
      - To add a GUS server to the list of servers used for updates, specify the address of the GUS server under the list of servers and click **Add**.
      - To remove a GUS server from the list of used servers, select the server you want to remove and click **Remove**.
      - In the **Base URI** field, specify a GUS server folder where updates for Dr.Web products are located.

- From the **Protocol** drop-down list, select the type of protocol to be used to deliver the updates from update servers. For all protocols, the updates are downloaded according to the settings of the GUS server list.
- From the **Allowed certificates** drop-down list, select the type of SSL certificates that will be accepted automatically. This option is used only for secure protocols that support encryption.
- **Login** and **Password**—user credentials to authenticate on the update server, if the update server requires authorization.
- Select the **Use CDN** check box to allow the repository to be downloaded from the GUS via a Content Delivery Network.

c) On the **Proxy Server** tab, you can specify parameters for connecting to the GUS via the proxy server:

- **Proxy server address** and **Port**—the network address and the port number of the proxy server to be used.
- **Login** and **Password**—authorization parameters on the proxy server if the proxy server requires authorization.

d) On the **Scheduler** tab, you can configure the schedule to receive updates periodically. The schedule is launched by the the Task Scheduler component of the Windows OS. In this case, you do not have to launch the utility manually, the repository is downloaded automatically according to the specified time slots.

e) On the **Log** tab, you can configure the parameters of update download log.

Click **OK** to apply the changes and return to the main widow of Dr.Web Repository Loader.

4. After configuring all parameters, click **Download** in the main window of Dr.Web Repository Loader to initiate a connection to the GUS and download the repository.

11.5.2.2. Console Utility

The following versions of the Dr.Web Repository Loader console utility are provided:

Executable file	Location	Description
`drweb-reploader-<OS>-<bitness>`	Control Center, the **Administration** → **Utilities** section	Standalone version of the utility. Can be launched from any directory or on any computer with the appropriate operating system.
	The `webmin/utilities` directory of Dr.Web Server	
`drwreploader`	The `bin` directory of Dr.Web Server	The version of the utility depends on server libraries. It can only be launched from its installation directory.

Command line switches for the console version of the Repository Loader utility are described in the **Appendices**, section G7.5. Dr.Web Repository Loader.

11.6. Update Restrictions for Workstations

Using the Dr.Web Security Control Center you can configure the bandwidth limits for the network traffic during the delivery of updates from Dr.Web Server to Dr.Web Agents on protected workstations in specific time slots.

For more details see Workstation Traffic Limitations.

The update bandwidth restrictions are not applied to the installation of new components and also to the updates initiated by the administrator using the **Restore failed components** toolbar option.

Configuring the station update mode

1. Select the **Anti-virus network** item in the main menu, in the window that opens click the name of a station or group in the hierarchical list. Select **Update restrictions** in the control menu.
2. From the **Update restriction** drop-down list, select the type of restriction:
   - **Update all products**—do not restrict the distribution of updates to stations.
   - **Forbid all updates**—forbid the distribution of all updates to stations during the time slots specified in the **Stations update timetable** table below.
   - **Update only bases**—forbid the distribution of updates only for program modules during the time slots specified in the **Stations update timetable** table below. Virus databases will be updated normally, without any changes.
3. Select the **Reduce the severity of virus databases aging** check box to reduce the severity statues for stations with outdated virus databases. If the check box is selected, the stations with outdated virus databases will be marked in the anti-virus network with the icon, and in the **Status** section, the stations will have **Low** severity. If the check box is cleared, the stations with outdated virus databases will be marked in the anti-virus network with the icon (if the **Settings of tree view → Show station states severity** option on the toolbar is enabled), and in the **Status** section, the stations will have **Maximal** or **High** severity. Description of a similar setting of the Dr.Web Agent (**Virus database relevance period**) is given in the **Administrator Manual on managing stations under Windows** (section **Dr.Web Agent → General**).
4. In the **Interval of revisions relevance** field, specify the time interval during which revisions of the products installed on stations will be considered relevant when new revisions appear in the Dr.Web Server repository.
5. Select the **Receive the latest updates** check box to transmit all component updates to the stations regardless of the limitations specified in the Detailed Repository Configuration section.

   If the check box is cleared, the station will receive only the updates for which the revision is marked as **Current** in the **Detailed repository configuration** section.

6. Select the **Allow revisions downgrade** check box to allow downgrading the versions of the anti-virus components on stations from the Dr.Web Server repository according to the distribution settings.

   See also Downgrade Product Revision.

7. Select the **Limit updates traffic** check box to limit the bandwidth for delivering the updates from Dr.Web Server to Dr.Web Agents.

   If the check box is cleared, updates for Dr.Web Agents will be delivered without limiting the network traffic bandwidth.

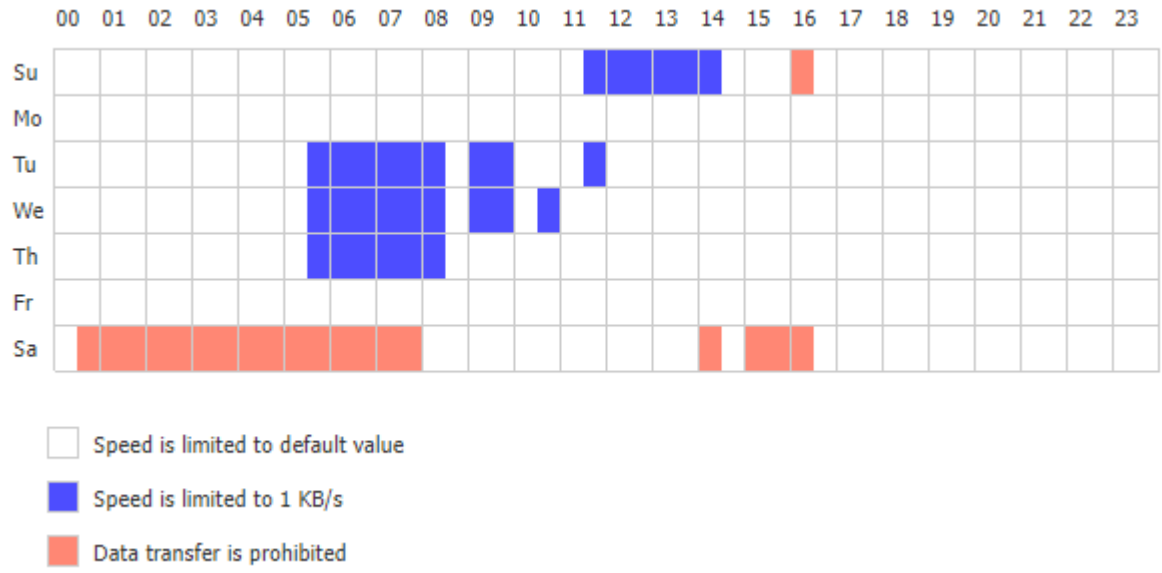
   If the check box is selected, specify the following fields:

   - In the **Default speed** field, specify the default value of the maximum bandwidth for update delivery, if no other limitations are set (empty white cells in the schedule table). The default speed value is also applied for periods when data transfer is prohibited but the update process has already started (see below).
   - In the **Maximal transmission speed (KB/s)** field, specify the value of maximum speed for update delivery. In this case, the updates will be delivered within the specified bandwidth of the aggregate network traffic used for updating all Dr.Web Agents.
     It is allowed to configure up to five bandwidth limits for update delivery. To add a bandwidth limit, click +. To remove the limit, click − next to the limit you want to remove.

   The values of the **Default speed** and **Maximal transmission speed (KB/s)** fields must meet the following restrictions:

   - The value 0 cannot be set. The minimum allowed limit value is 1 KB/s.
   - An empty value (the field is not set) cancels all limitations on update traffic for the corresponding time period.

   In the schedule table, you can set the data transfer restrictions separately for each 30 minutes of each day of the week.



To change the type of data transfer restriction, click the corresponding block in the table. You can also select several time blocks using drag and drop.

The color of the cells changes cyclically according to the legend below the table.

The delivery of updates cannot be initiated in the periods marked with the **Data transfer is prohibited** color. If the update transfer has been already under way at the beginning of this period, it will not be stopped, however the maximum transfer rate will be set to the value indicated in the **Default speed** field.

8. After editing is complete, click **Save** to accept changes.

The following options are also available in the toolbar to manage the parameters of this section:

 **Reset all parameters to initial values**—restore the values that all parameters in this section had before the current edit (most recent saved values).

 **Reset all parameters to default values**—restore the default values of all parameters in this section.

 **Propagate these settings to another object**—copy settings from this section to the settings of another station, group or multiple groups and workstations.

 **Inherit settings from policy or primary group**—remove custom settings of a station and set inheritance of settings in this section from a primary group.

 **Copy settings from policy or primary group and set them as personal**—copy settings of this section from a primary group and set them for selected stations. Inheritance is not set and station settings are considered custom.

 **Export settings from this section to the file**—save all settings in this section to a file of a special format.

 **Import settings to this section from the file** —replace all settings in this section with settings from a file of a special format.

11.7. Updating Dr.Web Agents in Mobile Mode

If a user computer, laptop or mobile device hasn't connected to Dr.Web Server for a long time, it is recommended that you set Dr.Web Agent on the station to *mobile mode*, to ensure that it receives timely updates from Dr.Web GUS.

The mobile mode is available in the Dr.Web Agent settings if it is allowed in the Control Center, in **Anti-virus Network** → **Permissions** → <*operating_system*> → **General** → **Change Dr.Web Agent configuration** (for Windows OS) or **Run in mobile mode** (for other operating systems).

In the mobile mode, Dr.Web Agent tries to connect to Dr.Web Server three times and, if unsuccessful, performs an update from the GUS. Dr.Web Agent keeps trying to find Dr.Web Server, once in several minutes.

In the mobile mode, Dr.Web Agent is disconnected from Dr.Web Server. All changes made to the settings of such a station on Dr.Web Server will take effect only after the mobile mode is switched off for this Dr.Web Agent and it is reconnected to Dr.Web Server.

In the mobile mode, only virus databases are updated.

In the mobile mode, the Dr.Web Agent operation is not limited in time, but the virus databases are updated from GUS only until the expiration date of the station license key. The information about the license key is saved by Dr.Web Agent the last time it connected to Dr.Web Server (the license key itself is stored on Dr.Web Server).

See the description of the Dr.Web Agent mobile mode settings in the **User Manual**.

Chapter 12: Configuring the Additional Components

12.1. Dr.Web Proxy Server

The anti-virus network can consist of one or several Dr.Web Proxy Servers.

The main function of Dr.Web Proxy Server is to establish a connection between Dr.Web Server and Dr.Web Agents in cases when it is impossible to ensure direct access (for example, if Dr.Web Server and Dr.Web Agents are located in separate networks with no packet routing between them).

Installing Dr.Web Proxy Server on a computer in the anti-virus network allows using it 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.

General Functions

Dr.Web Proxy Server performs the following functions:

1. Listens to the network and manages connections according to the specified protocol and port.
2. Performs protocol translation (supported protocols: TCP/IP).
3. Transfers the data between Dr.Web Server and Dr.Web Agents according to Dr.Web Proxy Server settings.
4. Caches Dr.Web Agent and anti-virus package updates delivered by Dr.Web Server. Using Dr.Web Proxy Server cache for update delivery has the following advantages:
   - reduction of network traffic,
   - reduction of delivery time for Dr.Web Agent updates.
5. Encrypts the traffic between Dr.Web Servers and Dr.Web Agents.

It is possible to create a hierarchy of Dr.Web Proxy Servers.

The diagram of the anti-virus network when using Dr.Web Proxy Server is shown in the figure 12-1.

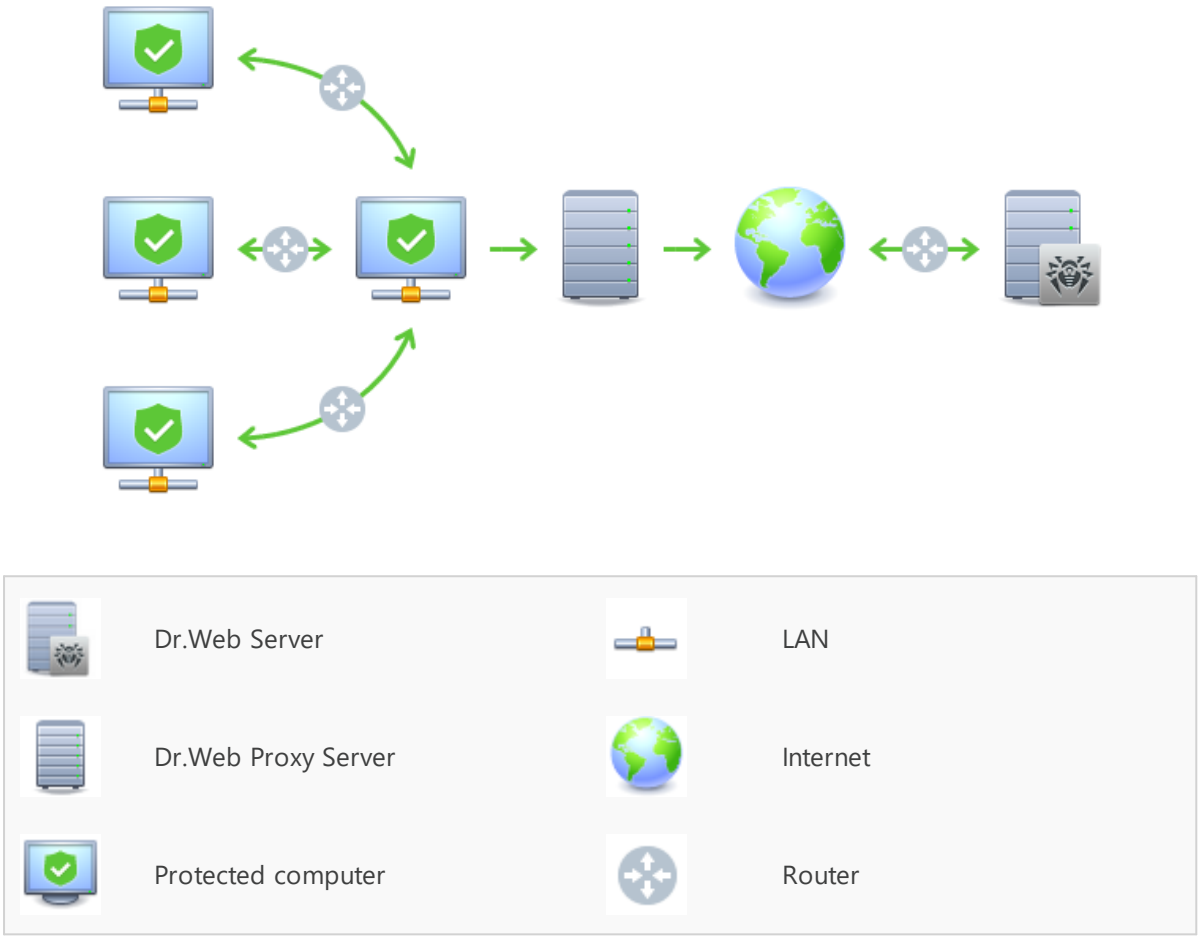


Figure 12-1. Diagram of the anti-virus network when using Dr.Web Proxy Server

Principle of Operation

When using Dr.Web Proxy Server, the following operations are performed:

1. If the Dr.Web Server address is not specified in Dr.Web Agent, Dr.Web Agent sends a multicast request according to the network protocol.
2. If Dr.Web Proxy Server is configured to be discoverable as Dr.Web Server (`discovery="yes"`), a message is sent to Dr.Web Agent indicating the presence of an available Dr.Web Proxy Server.
3. Dr.Web Agent sets the parameters received from Dr.Web Proxy Server as parameters of Dr.Web Server. Further interaction is transparent to Dr.Web Agent.
4. Dr.Web Proxy Server listens on the specified ports for incoming connections via the specified protocols according to the configuration file.
5. For each incoming connection from Dr.Web Agent (or Dr.Web Server) Dr.Web Proxy Server establishes a connection to Dr.Web Server (or Dr.Web Agent).

The forwarding algorithm for the list of Dr.Web Servers

1. Dr.Web Proxy Server loads the list of Dr.Web Servers from the `drwcsd-proxy.conf` configuration file into RAM (see the **Appendices**, F4. Dr.Web Proxy Server Configuration File).
2. Dr.Web Agent connects to Dr.Web Proxy Server.
3. Dr.Web Proxy Server forwards Dr.Web Agent traffic to the first Dr.Web Server from the list of Dr.Web Servers loaded into RAM.
4. Dr.Web Proxy Server rotates the list in RAM and moves Dr.Web Server from the first position to the end of list.

   Dr.Web Proxy Server does not save the changed order of Dr.Web Servers in its configuration file. After Dr.Web Proxy Server is restarted, the list of Dr.Web Servers will be loaded into RAM in the original version, which is stored in the configuration file.

5. When the next Dr.Web Agent connects to Dr.Web Proxy Server, the process is repeated from step 2.
6. If Dr.Web Server is disconnected from the anti-virus network (for example, it goes offline or is unavailable due to denial of service), Dr.Web Agent connects to Dr.Web Proxy Server again, and the process is repeated from step 2.

   Network scanner launched from an external network (in relation to Dr.Web Agents) will not be able to detect the installed Dr.Web Agents.

   If a replacement option is selected in the **Replace station name** drop-down list on the General tab in Dr.Web Server configuration and a Dr.Web Proxy Server is used in the anti-virus network, then all stations connected to Dr.Web Server via Dr.Web Proxy Server display the name of the computer with Dr.Web Proxy Server installed instead of their own names.

Traffic Encryption and Compression

Dr.Web Proxy Server supports traffic compression. Transferred data is processed regardless of whether the traffic is compressed or not.

Dr.Web Proxy Server supports traffic encryption. To support the encryption, Dr.Web Proxy Server must connect to Dr.Web Server (see the **Installation Manual**, section Connecting Dr.Web Proxy Server to Dr.Web Server) and sign its certificate with the certificate and private key of Dr.Web Server. Traffic encryption between Dr.Web Server and Dr.Web Proxy Server is performed using the Dr.Web Server certificate; the traffic encryption between Dr.Web Agents and Dr.Web Proxy Server is performed using Dr.Web Proxy Server certificate signed with the Dr.Web Server certificate and private key.

Caching

Dr.Web Proxy Server supports traffic caching.

Products are cached according to their revisions. Each revision is stored in its own directory. A directory of a newer revision contains *hard links* to the unchanged files from previous revisions as well as the actual changed files. Thus, the files for each version are stored on a hard drive in a single copy, and all directories of newer revisions contain only links to unchanged files.

Depending on the settings specified in the configuration file, the following actions are performed if caching is enabled:

- Outdated revisions are deleted periodically. By default—once an hour.
- Only the latest revisions are stored. All other, earlier revisions are considered outdated and are deleted. By default, the last 3 revisions are stored.
- Unused *memory mapped* files are periodically unloaded. By default—every 10 minutes.

Settings

Dr.Web Proxy Server does not have a GUI. You can configure it in one of the following ways:

1. Remotely using the Control Center if Dr.Web Proxy Server is connected to Dr.Web Server (see Remote Configuration of Dr.Web Proxy Server).
2. Locally using the configuration file. The format of Dr.Web Proxy Server configuration file is described in the **Appendices**, section F4. Dr.Web Proxy Server Configuration File.

Only users with administrative privileges on the computer can manage Dr.Web Proxy Server settings (edit the configuration file).

For proper operation of Dr.Web Proxy Server on a Linux OS after a reboot, you must edit system network configuration without NetworkManager.

Starting and Stopping

On Windows, Dr.Web Proxy Server can be started or stopped using standard tools.

- By entering commands in the command line interpreter:
  - to start the Dr.Web Proxy Server service, enter `net start drwcsd-proxy`;
  - to stop the Dr.Web Proxy Server service, enter `net stop drwcsd-proxy`.
- Using Service Manager snap-in. Select `drwcsd-proxy` on the list of services and choose the required action.

To start and stop Dr.Web Proxy Server on a Unix-like OS, use the `start` and `stop` commands with scripts created during the installation of Dr.Web Proxy Server (see the **Installation Manual**, section Installing Dr.Web Proxy Server).

To start Dr.Web Proxy-server on both Windows OS and Unix-like OS, you can run the `drwcsd-proxy` executable file with the appropriate switches (see the **Appendices**, section G5. Dr.Web Proxy Server).

12.1.1. Remote Configuration of Dr.Web Proxy Server

After connecting Dr.Web Proxy Server to Dr.Web Server, you can configure Dr.Web Proxy Server remotely using the Control Center.

Detailed information on connection settings and about quick connection using the command line is given in the **Installation Manual**, section Connecting Dr.Web Proxy Server to Dr.Web Server.

Dr.Web Proxy Server can accept settings only from a specific set of connected Dr.Web Servers that are marked as managing. If none of the Dr.Web Servers is marked as managing, then the Proxy Server connects to all Dr.Web Servers by rotation until it finds the first valid (not empty) configuration.

If a Dr.Web Server is marked as non-managing (the **Managing Dr.Web Server** parameter is set to **No**), Dr.Web Proxy Server cannot receive any settings from it. It also means that later on, this Dr.Web Server cannot be set as managing for the Dr.Web Proxy Server remotely. In this case you need to change the `<forward to="" master="">` parameter value in the Dr.Web Proxy Server configuration file manually (see **Appendices**, F4. Dr.Web Proxy Server Configuration File).

Specifying Dr.Web Proxy Server settings

1. Select the Anti-virus network item in the main menu of the Control Center. In the window that opens, click the name of Dr.Web Proxy Server or the **Proxies** group and its subgroups in the hierarchical list.
2. Select **Dr.Web Proxy Server** in the opened control menu. The Settings section opens.
3. On the **Certificate** tab, you can set the list of Dr.Web Server certificates. You must set all certificates of all Dr.Web Servers to which Dr.Web Proxy Server 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 of settings and to support the traffic encryption between Dr.Web Server and Dr.Web Proxy Server.
   - Dr.Web Proxy Server certificate is signed with the Dr.Web Server certificate and private key (the procedure is performed automatically on Dr.Web Server after the connection is established, and does not require any administrator intervention) and is required to

connect Dr.Web Agents and to support the traffic encryption between Dr.Web Agents and Dr.Web Proxy Server.

4. On the **Listen** tab, you can specify the parameters of traffic receiving and forwarding by Dr.Web Proxy Server.

If you are using unified network listening settings, you can specify one set of settings for all client connections, and a different set of settings for each Dr.Web Server.

To add another set of settings, click  .

To remove a set of settings, click  next to the set you want to remove.

For each set you can specify the following Dr.Web Proxy Server operation parameters separately:

a) In the listening settings section:

- In the **Address to listen** field, specify an IP address that Dr.Web Proxy Server will "listen" on. Inputting `0.0.0.0` instructs to "listen" on all interfaces.

Addresses should be specified in the network address format described in the **Appendices**, section. Appendix D. The 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 Discovery flag to enable discovery mode. This mode allows clients to discover an available Dr.Web Proxy Server during multicast requests.
- Set the **Multicasting** flag so that Dr.Web Proxy Server responds to multicast requests sent to Dr.Web Server.
- In the Multicast group field, specify the IP address of a multicast group to which Dr.Web Proxy Server should belong. The specified interface will be listened to by the Proxy Server for interaction with clients during active Dr.Web Servers searches. If you leave this field blank, Dr.Web Proxy Server will not be included in any multicast group. The default multicast group to which Dr.Web Server is included is `231.0.0.1`.

b) In the **Settings for connection with clients** section:

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

c) In the **Settings for connection with Dr.Web Servers** section, you can specify the list of Dr.Web Servers to which the traffic will be forwarded.

The order of Dr.Web Servers in the list defines the order of client traffic redirection and the order of connection of Dr.Web Proxy Server to Dr.Web Servers for receiving the settings. To change the Dr.Web Server order, drag the required lines with the mouse.

To manage Dr.Web Servers, use the buttons on the toolbar of the Dr.Web Server list:

edit the connection settings for the selected Dr.Web Server.

add the connection settings for the selected Dr.Web Server.

remove the connection settings for the selected Dr.Web Server.

The window where you can edit and add the connection settings for a Dr.Web Server provides the following options:

- In the **Managing Dr.Web Server** drop-down list, select one of the following options to set the Dr.Web Server in the managing role:
  Yes—the managing role is explicitly assigned to Dr.Web Server. You can assign managing roles to any number of Dr.Web Servers; Dr.Web Proxy Server connects to all the managing Dr.Web Servers in the order they are listed in the settings until it gets the first valid (not empty) configuration.
  No—the managing role will not be assigned to Dr.Web Server under any circumstances. You can also choose not to assign the managing role to any Dr.Web Servers. In this case, Dr.Web Proxy Server parameters (including the assignment of managing Dr.Web Servers) can be configured only locally via Dr.Web Proxy Server configuration file (see **Appendices**, F4. Dr.Web Proxy Server Configuration File).
  Possible—Dr.Web Server will assume the managing role only if there are no explicit managing Dr.Web Servers (those for which the value of this option is **Yes**).
- In the **Redirection address** field, specify the address of Dr.Web Server to which the connections established by Dr.Web Proxy Server will be forwarded. It is recommended that you use Dr.Web Server name in the FQDN format as the Dr.Web Server address.

If the **Redirection address** field is not specified or the `udp/` value is set, Dr.Web Proxy Server will use the detection service to find Dr.Web Server by sending multicast requests (see step 9).

Addresses should be specified in the network address format described in the **Appendices**, section. 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 data traffic between Dr.Web Proxy Server and specified Dr.Web Server. Select the compression level (from 1 to 9) in the **Compression level** field.

In the table, you can specify the traffic limitation settings in the same way as the Dr.Web Server settings given in the Updates and Installations sections.

5. On the **Cache** tab, specify the following Dr.Web Proxy Server caching settings:

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

- In the **Revisions deleting interval (min)** field, specify the interval at which old revisions should be deleted from the cache if their number exceeds the maximum number of revisions that should remain. The value is set in minutes. The default value is 60 minutes.

- In the **Number of revisions to remain** field, specify the maximum number of each product revisions to remain in the cache after the purge. By default, the last 3 revisions are kept, and the older revisions are deleted.

- In the **Unload interval of unused files (min)** field, specify the time interval in minutes for unloading unused files from the memory. The default value is 10 minutes.
- Set the **Use proactive caching** flag to load new revisions for the selected products from Dr.Web Server to Dr.Web Proxy Server according to the schedule below. During this period, revisions will be loaded to Dr.Web Proxy Server as soon as Dr.Web Server receives them from GUS. If the flag is cleared, new revisions will be downloaded to Dr.Web Proxy Server only when Dr.Web Agent requests them from Dr.Web Server.
  - In the list below, set the flags for the products you want to synchronize.
  - In the **Repository synchronization timetable** section, specify the schedule for loading the updates for the selected products.
    To change the type of data transfer limitations, click the corresponding table cell. Also, you can select several time cells using drag and drop.
    The color of the cells changes cyclically according to the legend below the table: data transfer can be either allowed without limitations or prohibited.

6. On the **Events** tab, specify the following parameters of event delivery:

- Set the **Cache events** flag to cache events received from Dr.Web Agents. In this case, the events will be sent to Dr.Web Server every 15 minutes for the period of time specified in the schedule below. If caching is disabled, events will be sent to Dr.Web Server immediately after they are received by Dr.Web Proxy Server.
- In the **Events sending timetable** section, specify the schedule for sending events received from Dr.Web Agents.
  To change the type of data transfer limitations, click the corresponding table cell. Also, you can select several time cells using drag and drop.
  The color of the cells changes cyclically according to the legend below the table: event transmission can be allowed without limitations or prohibited.

7. On the **Dump** tab, specify the following settings:

- Set the **Create memory dumps** flag to create memory dumps if critical errors occur in Dr.Web Proxy Server operation.
- In the **Maximum number of dumps** field, specify the maximum number of memory dumps. When the specified value is reached, the oldest dumps are deleted when new dumps are created. Memory dumps setup is available for Windows OS only.

8. On the **DNS** tab, you can configure the parameters of DNS server usage. The settings are similar to the DNS settings for Dr.Web Server.

9. On the **Discovery** tab, you can configure the settings for saving responses to multicast requests when searching for Dr.Web Servers for redirecting clients (see step 4c).

- **For positive responses, sec.**—the time (in seconds) for storing the list of Dr.Web Servers that responded to the multicast request during Dr.Web Server look-up. After the specified period of time, the request is sent again.

- **For negative responses, sec.**—the time (in seconds) for storing the information that none of Dr.Web Servers has responded to the multicast request. After the specified period of time, the request is sent again.

10. On the **Updates** tab, you can configure the parameters of Dr.Web Proxy Server automatic software update from Dr.Web Server:

- Set the **Enable automatic update** flag to download for Dr.Web Server and install new Dr.Web Proxy Server revisions automatically. The update schedule depends on Dr.Web Proxy Server proactive caching settings (see step 5):
  a) If Dr.Web Proxy Server is not included in the list for proactive caching (even if caching is not used), then Dr.Web Proxy Server updates will be downloaded and installed according to the automatic update schedule.
  b) If Dr.Web Proxy Server is included on the proactive caching list, Dr.Web 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 update schedule.
- In the **Automatic update schedule** section, specify the schedule according to which the automatic updates will be performed.
  To change the type of data transfer limitations, click the corresponding table cell. Also, you can select several time cells using drag and drop.
  The color of the cells changes cyclically according to the legend below the table: update delivery can be either allowed without traffic limitations or forbidden.

11. On the **Log** tab, you can select the verbosity level of the Dr.Web Proxy Server log. The following options are available:

- **Critical error**—messages on critical operation errors only;
- **Error**—messages on operation errors;
- **Warning**—warnings on errors;
- **Notification**—important information messages;
- **Information**—information messages;
- **Trace (0–3)**—event tracing with varying detail levels (**Trace3** being the most detailed);
- **Debug (0–3)**—debug messages with varying detail levels (**Debug3** being the most detailed);
- **All**—all messages (equivalent to **Debug3**).

12. When you are finished editing, click **Save**.

12.2. NAP Validator

Overview

Microsoft Network Access Protection (NAP) is a policy enforcement platform built into Windows OSs that allows you to better protect network assets by enforcing compliance with system health requirements.

With NAP, you can create customized health requirement policies to validate the health of computers in the following cases:

- before allowing access or communication,
- automatically update compliant computers to ensure ongoing compliance,
- adapt computers to meet established requirements.

For a detailed description of the NAP technology see Microsoft Docs.

NAP in Dr.Web Enterprise Security Suite

Dr.Web Enterprise Security Suite allows you to use the NAP technology to check health of Dr.Web anti-virus software on protected workstations.

The following tools are used for health validation

- A NAP health policy server installed and configured in the network.
- Dr.Web NAP Validator which is an implementation of NAP System Help Validator (SHV) using Dr.Web custom policy extensions. This component is installed on the computer where the NAP server is located.
- System Health Agents (SHAs) which are automatically installed on the workstations during the installation of Dr.Web Agents.
- Dr.Web Server which acts as the NAP remediation server and ensures the health of anti-virus software on workstations.

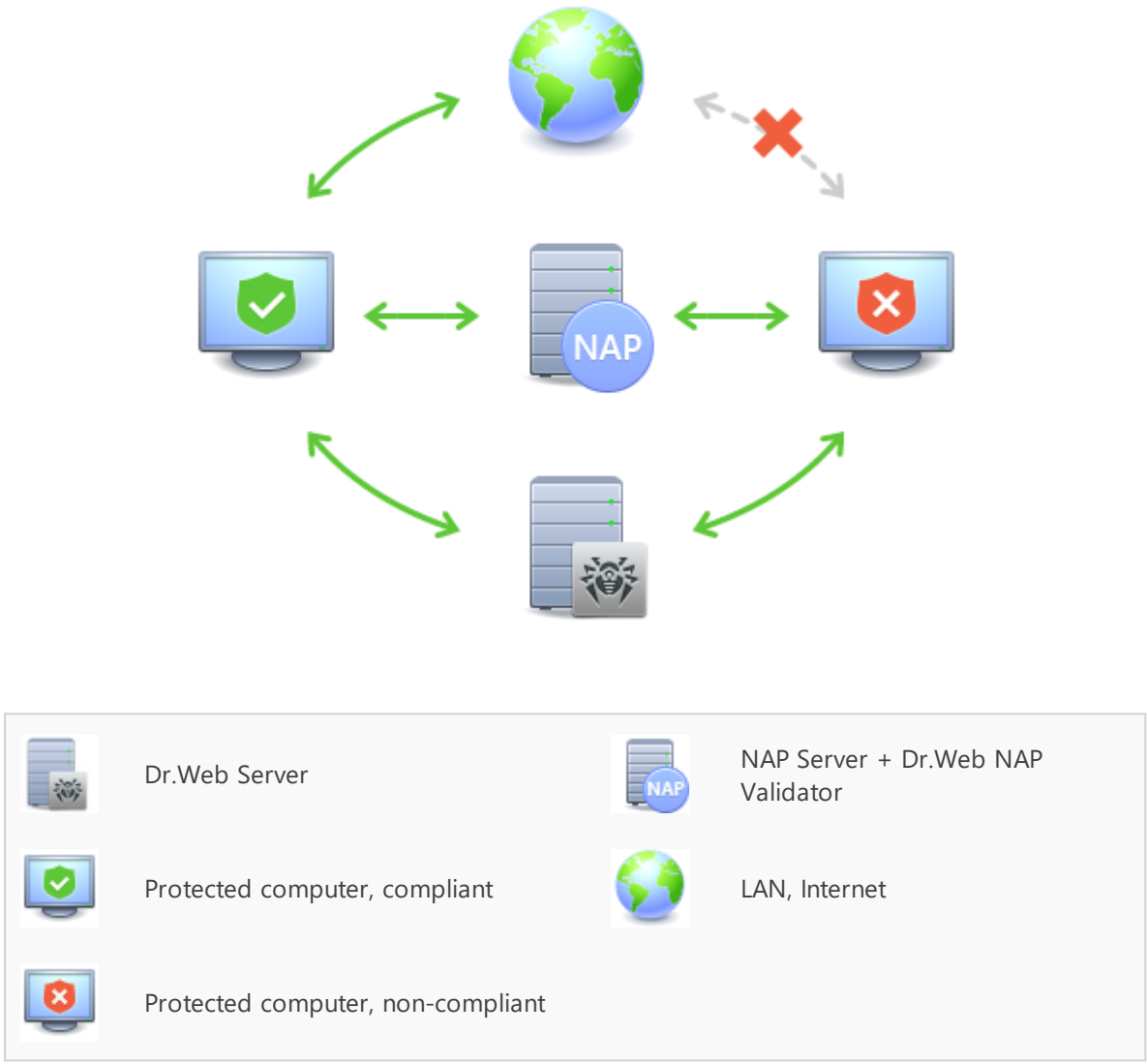


Figure 12-2. Diagram of the anti-virus network when using NAP

Workstation Validation Procedure

1. Validation is activated when you configure the appropriate settings of Dr.Web Agent.
2. The SHA connects to Dr.Web NAP Validator installed on the NAP server.
3. Dr.Web NAP Validator determines the compliance of workstations with the health requirement policies as described below. To determine health compliance, NAP Validator checks the status of anti-virus software on a workstation against the corresponding health requirement policies, and then classifies the workstation in one of the following ways:
   - Workstations that meet the health policy requirements are considered compliant and allowed unlimited access and communication on the network.
   - Workstations that do not meet at least one requirement of the health policy are considered non-compliant and their access is limited to Dr.Web Server only. Dr.Web

Server allows non-compliant workstations to update the system with the necessary anti-virus settings. After the update, the workstations are validated again.

Health Policy Requirements

1. Dr.Web Agent must be started and running.
2. Dr.Web virus databases must be up-to-date, that is the databases on the workstation must have the same version as those on Dr.Web Server.

Configuring NAP Validator

After installing Dr.Web NAP Validator (see the **Installation Manual**, section Installing NAP Validator) on the computer where a NAP server is located, you should perform the following actions:

1. Open the NAP server configuration component by running the `nps.msc` command.
2. In the **Policies** section, select **Health Policies**.
3. In the window that opens, open the properties of the following elements:
   - **NAP DHCP Compliant**. In the settings windows, set the **Dr.Web System Health Validator** flag which specifies the use of the Dr.Web NAP Validator component policies. To classify workstations as compliant only if all health policy requirements are met, select **Client passed all SHV checks** from the drop-down list.
   - **NAP DHCP Noncompliant**. In the settings windows, set the **Dr.Web System Health Validator** flag which specifies the use of the Dr.Web NAP Validator component policies. To classify workstations as non-compliant if any of the health policy requirements are not met, select **Client failed one or more SHV checks** from the drop-down list.