



Dr.WEB

Enterprise Security Suite

Managing stations under Windows



© Doctor Web, 2020. All rights reserved

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

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

Trademarks

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

Disclaimer

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

Dr.Web Enterprise Security Suite. Managing stations under Windows
Version 11.0.2
Administrator Manual
5/13/2020

Doctor Web Head Office

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

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

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

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

Doctor Web

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

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

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

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

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



Table of Contents

Chapter 1. Introduction	5
1.1. About Manual	5
1.2. Conventions and Abbreviations	6
Chapter 2. Dr.Web Enterprise Security Suite	7
2.1. About Product	7
2.2. Workstations Protection	8
Chapter 3. Dr.Web for Windows	10
3.1. Dr.Web for Windows Components	10
3.2. Dr.Web for Windows Configuration	11
3.2.1. Scanner	12
3.2.2. SpIDer Guard	14
3.2.3. Office Control	17
3.2.4. Dr.Web Agent	25
3.2.5. Dr.Web for Microsoft Outlook	30
3.2.6. Preventive Protection	33
3.2.7. Dr.Web Firewall	37
3.2.8. Network Port Monitor	42
3.2.9. SpIDer Mail and SpIDer Gate	43
Appendix A. Technical support	50



Chapter 1. Introduction

1.1. About Manual

This manual is a part of the documentation package of the anti-virus network administrator and intended to provide detailed information on the organization of the complex anti-virus protection of corporate computers and mobile devices using Dr.Web Enterprise Security Suite.

The manual is meant for the anti-virus network administrator—the employee of organization who is responsible for the anti-virus protection of workstations and servers of this network.

The manual contains the information about centralized configuration of the anti-virus software of workstations which is provided by the anti-virus network administrator via Dr.Web Security Control Center. The manual describes the settings of Dr.Web for Windows anti-virus solution and features of the centralized configuration of the software.

To get additional information, please refer to the following manuals:

- **User Manual** of Dr.Web for Windows anti-virus solution contains the information about configuration of the anti-virus software provided on a station directly.
- **Administrator Documentation** of Dr.Web Enterprise Security Suite anti-virus network (includes **Administrator Manual**, **Installation Manual** and **Appendices**) contains the general information on installation and configuration of the anti-virus network and, particularly, on operation with Dr.Web Security Control Center.



Before reading these document, make sure you have the latest version of the manuals. The manuals are constantly updated and the current version can always be found at the official website of Doctor Web at <https://download.drweb.com/doc/>.



1.2. Conventions and Abbreviations

Conventions

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

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

Abbreviations

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

- DNS—Domain Name System,
- GUI—Graphical User Interface, a GUI version of a program—a version using a GUI,
- NAP—Network Access Protection,
- Dr.Web GUS—Dr.Web Global Update System
- OS—operating system.

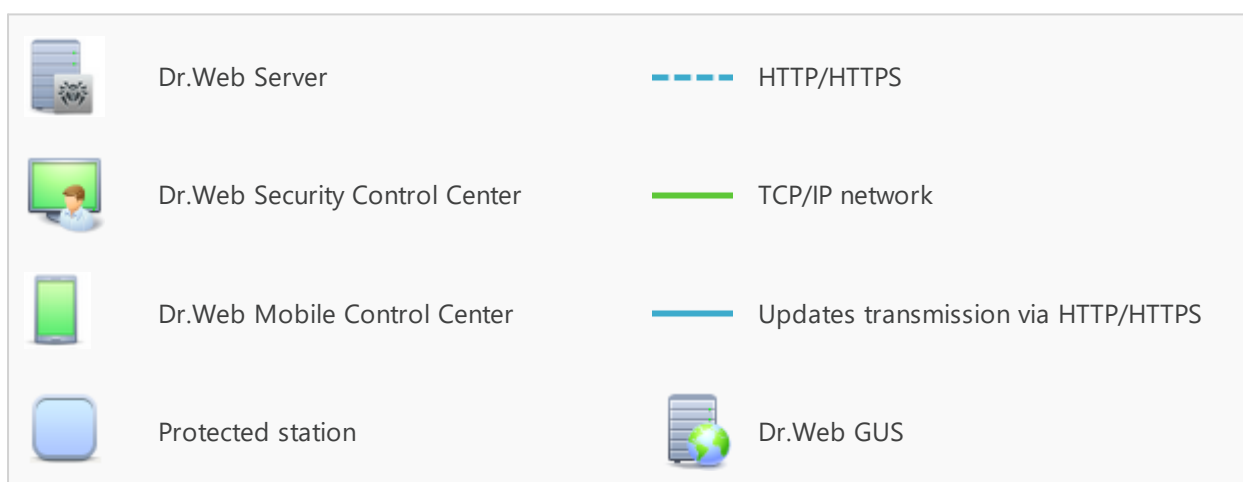
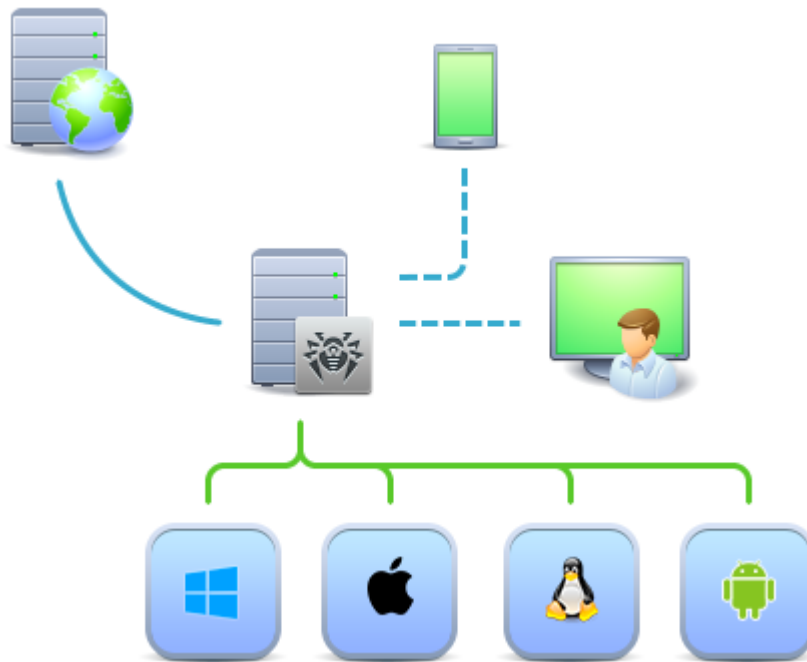


Chapter 2. Dr.Web Enterprise Security Suite

2.1. About Product

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

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



The logical structure of the anti-virus network



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

2.2. Workstations Protection

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



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

Anti-virus packages are installed on protected stations and are connected to Dr.Web Server. Each station is included in one or several groups registered on this Server. Stations and the 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 a mobile device. Installation may be implemented either by the administrator or by the user.
2. Remotely. Remote installation is available for stations under Windows OS only and performed in the Control Center through the LAN. Installation is implemented by an anti-virus network administrator. At this, user intervention is not required.



You can find detailed description of the anti-virus packages installation procedures on workstations in the Dr.Web Enterprise Security Suite **Installation Manual**.

Management

When connection with Dr.Web Server is established, the administrator is able to use the following functions implemented by the 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 the anti-virus scans and other tasks to execute on a station.
- Get scan statistics and other information on anti-virus components operation and on stations state.



- Start and stop anti-virus scans and etc.

Update

Dr.Web Server downloads updates and distributes them to connected stations. Thus, optimal threat 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 the Server is lost, the virus databases can be updated directly from the GUS.



The principle of stations operation in the Mobile mode is described in the Dr.Web Enterprise Security Suite **Administrator Manual**.



Chapter 3. Dr.Web for Windows

Dr.Web Agent provides multilevel protection of RAM, hard disks, and removable media against any kind of viruses, rootkits, Trojans, spyware, adware, hacktools, and all possible types of malicious objects from any external source.

Dr.Web uses a convenient and efficient procedure for updating virus databases and program components via the Internet.

Dr.Web can detect and remove unwanted programs (adware, dialers, jokes, riskware, and hacktools) from your computer. To detect unwanted programs and perform actions with the files contained in the programs, anti-virus components of Dr.Web are used.

3.1. Dr.Web for Windows Components

For stations under Windows OS, the following anti-virus components are provided:

Dr.Web Scanner, Dr.Web Agent Scanner

Scans a computer on user demand and according to the schedule. Also, the remote launch of the anti-virus scan of stations from the Control Center including rootkits check is supported.



You can find the description of Dr.Web Agent, Scanner settings and remote scan launch via the Control Center in the Dr.Web Enterprise Security Suite **Administrator Manual**.

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 the 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, XMPP (Jabber), and TLS (SSL) protocols. 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. Allows to control the integrity of important files from the accidental change or virus infecting and limit the access to unwanted information for employees.



Firewall

Protects computers from external unauthorized access and prevents leak of vital 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 in the specific folder.



You can find the description of how to manage Quarantine via the Control Center in the **Administrator Manual**.

Self-Protection

Protects files and folders of 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 Enterprise Security Suite is granted to Dr.Web processes only.

Preventive Protection

Prevents from 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 in case of detection of viral activity.

3.2. Dr.Web for Windows Configuration








To view or edit the configuration of the anti-virus components on the workstation:

1. Select the **Anti-virus network** item in the main menu of the Control Center.
2. In the hierarchical list of the opened window, click the name of a station under Windows OS or a group containing such stations.
3. In the **Configuration** section of the opened control menu, in the **Windows** subsection, select the necessary component.
4. A window with the component settings will be opened.

Managing settings of anti-virus components via the Control Center differs from managing settings directly via the corresponding components on station:

- to manage separate parameters, use the options located on the right from the corresponding settings:
 - ➔ **Reset to initial value**—restore the value that parameter had before editing (last saved value).
 - ➔ **Reset to default value**—set the default value for a parameter.
- to manage a set of parameters, use the options located on the toolbar:



-  **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.
-  **Propagate these settings to another object**—copy settings from this section to settings of other station, group or several groups and stations.
-  **Set inheritance of settings from primary group**—remove personal settings of a station and set inheritance of settings in this section from a primary group.
-  **Copy settings from a 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 stations settings considered personal.
-  **Export settings from this section to the file**—save all settings from 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 the file of a special format.

5. After settings changes were made via the Control Center, click **Save** to accept the changes. The settings will be passed to the stations. If the stations were offline when changes are made, the settings will be passed when stations connect to the Server.



Administrator may forbid editing settings on station for a user (see the **Permissions of Station Users** section in the Dr.Web Enterprise Security Suite **Administrator Manual**). At this, only administrator will be able to edit settings via the Control Center.

3.2.1. Scanner

3.2.1.1. General

On the **General** tab, you can configure general parameters of Dr.Web Scanner operation.

- The **Play sounds** option instructs Dr.Web Scanner to use sound alerts for every event. Option is disabled by default.
- The **Automatically apply actions to threats** option allows Dr.Web Scanner to apply specified actions to detected threats automatically. If this option is disabled, the user will be prompted to specify the action.
- The **Interrupt scanning when switching to battery mode** allows to interrupt scanning when switching to the battery mode. Option is disabled by default.

On this tab, you can set the maximum permissible percent of CPU consumption by Dr.Web Scanner. By default, 50% is set.



3.2.1.2. Actions

On the **Actions** page, you can select actions to apply to the threats detected by Dr.Web Scanner, depending on their type.

- **Cure, move to quarantine if not cured.** Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is moved to quarantine. The action is available only for objects infected with a known virus that can be cured except for the Trojan programs and files within complex objects.
- **Cure, delete if not cured.** Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is deleted. The action is available only for objects infected with a known virus that can be cured except for the Trojan programs and files within complex objects.
- **Move to quarantine.** This action moves a detected threat to a special folder that is isolated from the rest of the system.
- **Delete.** It is the most effective way to remove all types of threats. This action implies full deletion of a dangerous object.
- **Ignore.** No actions are applied to the object. Notifications are not displayed.



The default settings are optimal for most cases. Do not change them unnecessarily.

Curing of infected objects may require restart of the station. The following options are available:

- **Prompt restart**—prompts the user to restart the station.
- **Restart computer automatically**—allows to enable an automatic restart of the computer.



3.2.1.3. Exclusions

On the **Exclusions** tab, you can specify files and folders that will not be scanned by Dr.Web Scanner.

To configure the list of exclusions

1. To add a file or folder to the exclusion list, do one of the following:
 - To add a certain file or folder, enter its full path.
 - To exclude all files or folders with a particular name, enter the name without the path.
 - To exclude files or folders from scanning, enter the mask of their names. The mask defines template for an object definition. At that,
 - the asterisk (*) character replaces any, possibly empty, sequence of characters;
 - the question mark (?) replaces any character (one);



- other mask characters do not replace anything and mean that the name must contain a particular character in this place.
- 2. You can specify only one object in one field. To add one more object to the list, click .
- 3. To remove the object from the list of exclusions, click  next to the list item that corresponds to the object.

You can also disable scan of installation packages, archives, and email files. This option is enabled by default.

3.2.1.4. Log

Enable the **Detailed logging** option to log such events as updates, starts and stops of Dr.Web Scanner, detected threats, names of packers, and contents of scanned archives.



By default, size of a log file is restricted to 10 MB. If the log file size exceeds the limit, the content is reduced to:

- Specified size if the current session information does not exceed the limit.
- Size of the current session if the session information exceeds the limit.

If the **Detailed logging** option is enabled, operation of corresponding component is logged in the debug mode with maximal detailing. Limitations on the file size are disabled in this mode. This leads to significant increasing of the log file size. Also note, that the rotation of the log file is not performed (in all logging modes).

Debug logging mode decrease performance of Anti-virus and operating system of a station. It is recommended that you use this mode only when problems occur in component operation or on request of technical support service. It is not recommended to enable logging debug mode for extended period of time.



On the Control Center, the logging settings are specified separately for each component on the **Log** sections. On stations, logging settings are specified in the **Advanced** common section.

3.2.2. SpIDer Guard

3.2.2.1. General

The **General** tab allows you to configure settings to scan workstations and servers by SpIDer Guard.

1. Scan mode

- **Optimal** (enabled by default). In this mode, SpIDer Guard scans objects only in the following cases:



- For objects on hard drives, an attempt to execute a file, create a new file, or add a record to an existing file or boot sector.
 - For objects on removable media, an attempt to access file or boot sectors in any way (write, read, execute).
 - **Paranoid.** In this mode, SpIDer Guard scans all files and boot sectors on hard or network drives and removable media at any attempt to access them (create, write, read, execute). The Paranoid mode ensures maximum protection, but considerably reduces computer performance.
2. The **Use heuristic analysis** option allows SpIDer Guard to detect suspicious objects that are most likely to be infected with unknown viruses. By default, this option is enabled. If this option is disabled, only the signature analysis is used for scanning.
 3. The **Scan for rootkits** option allows to perform the background scanning of the operating system for complex threats and curing active infections when necessary. During the background rootkit scanning, files and folders specified on the **Exclusions** page are excluded from scanning.



Disabling of SpIDer Guard does not affect background rootkit scanning. If the option is enabled, background scanning is performed regardless of whether SpIDer Guard is running or not.

Additional tasks

This setting group allows you to enable scan of certain types of objects and to **Block autoruns from removable media**. In any mode (optimal or paranoid), objects on network drives and removable media are scanned only if the corresponding options are enabled.

3.2.2.2. Actions

On the **Actions** page, you can select actions to be applied to threats detected by SpIDer Guard, depending on their type.

- **Cure, move to quarantine if not cured.** Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is moved to quarantine. The action is available only for objects infected with a known virus that can be cured except for the Trojan programs and files within complex objects.
- **Cure, delete if not cured.** Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is deleted. The action is available only for objects infected with a known virus that can be cured except for the Trojan programs and files within complex objects.
- **Move to quarantine.** This action moves a detected threat to a special folder that is isolated from the rest of the system.
- **Delete.** It is the most effective way to remove all types of threats. This action implies full deletion of a dangerous object.



- **Ignore.** No actions are applied to the object. Notifications are not displayed.



The default settings are optimal for most cases. Do not change them unnecessarily.

3.2.2.3. Exclusions



On the **Exclusions** tab, you can specify folders and files to be excluded from the SpIDer Guard scans.

The **Exclude system files from the scan** option instructs to exclude from the scan system files, which are included in the internal list of the SpIDer Guard component. This list is composed for each Windows OS version according to recommendations from the Microsoft® company on using the antivirus software.

If the option is enabled, the following options are available:

- **Exclude Prefetcher DB files** option instructs to exclude from scanning database files of the Prefetcher system component.
- **Exclude Windows search DB files** option instructs to exclude from scanning database files of Windows OS search service.

To configure the list of exclusions

1. To add a file, a folder, or a process to the exclusion list, do one of the following:
 - To add an existing object, enter its name without the path.
 - To exclude all objects with a particular name, specify the name in the entry field. It is not necessary to specify a path to the object.
 - To exclude specific objects, specify the mask of their names to in the entry field. The mask defines a template for an object definition. At that:
 - the asterisk (*) character replaces any, possibly empty, sequence of characters;
 - the question mark (?) replaces any character (one);
 - other mask characters do not replace anything and mean that the name must contain a particular character in this place.
2. You can specify only one object in one field. To add one more object to the list, click .
3. To remove the object from the list of exclusions, click  next to the list item that corresponds the object.

3.2.2.4. Log

Enable the **Detailed logging** option to log such events as updates, starts and stops of SpIDer Guard, detected threats, names of packers, and contents of scanned archives.



It is recommended that you use this mode to determine the most frequent objects scanned by SplDer Guard. If necessary, you can add these objects to the list of [exclusions](#) in order to increase the computer performance.



By default, size of a log file is restricted to 10 MB. If the log file size exceeds the limit, the content is reduced to:

- Specified size if the current session information does not exceed the limit.
- Size of the current session if the session information exceeds the limit.

If the **Detailed logging** option is enabled, operation of corresponding component is logged in the debug mode with maximal detailing. Limitations on the file size are disabled in this mode. This leads to significant increasing of the log file size. Also note, that the rotation of the log file is not performed (in all logging modes).

Debug logging mode decrease performance of Anti-virus and operating system of a station. It is recommended that you use this mode only when problems occur in component operation or on request of technical support service. It is not recommended to enable logging debug mode for extended period of time.



On the Control Center, the logging settings are specified separately for each component on the **Log** sections. On stations, logging settings are specified in the **Advanced** common section.

3.2.3. Office Control

3.2.3.1. General

On the **General** page, you can configure and restrict access to local file system resources:

- Enable the **Block data transfer over network** option to block data transfer over local networks and the Internet. Note that data transfer is blocked via network protocols NetBIOS and HTTP/HTTPS. Data transfer via the ICMP protocol is allowed.
- Enable the **Block sending tasks to a printer** option to forbid printer usage from users computers.
- Enable the **Check connected USB devices for BadUSB-vulnerability** option to verify all devices identified as a keyboard.
- Enable the **Control access to the protected objects** option to edit the list of the blocked [buses](#) and device [classes](#).

Device blocking

You can restrict access to the specified busses and device classes. You can also configure the [white list](#) of devices.



Device classes are all devices that perform the same functions (e.g., printing devices). Device buses are communication subsystems for transferring data between functional units of the computer (for example, the USB bus).

This function allows to block one or several device classes on all the buses. You can also block all the devices connected to one or several buses.



Use Windows Device Manager if you do not know which class corresponds to your device or which bus corresponds to a certain device class.



1. In Windows Device Manager, find the necessary device. If necessary, expand items of the specified device types.

The item that corresponds to the device is its device class (for example, flash drives correspond to the **Disk drives** class).




2. Select the necessary device, open the context menu, and click **Properties**.
3. On the **Details** tab, in the **Property** drop-down list, select **Parent**.
4. In the **Value** field, a string containing *Bus\Device UID* is specified.

For example, the value for a flash drive is *USB\VID_1EAB&PID_0501\03421*, where USB is a bus that corresponds to the device class.

To configure the list of the blocked device classes

1. Make sure that the **Control access to the protected objects** option is enabled.
2. In the **Device classes** section, click  to add a device to the **Blocked classes** list.
3. In the opened window, select all the device classes you want to block. To do that, set the **Block** flag next to the corresponding item in the list.
4. Click **Save**.
5. To remove a device from the list, select the corresponding item in the list and click .
6. To add other devices, repeat steps 1 and 2.


To configure the list of the blocked buses

1. Make sure that the **Control access to the protected objects** option is enabled.
2. In the **Device buses** section, click  to add a device to the **Blocked buses** list.
3. Select device buses you want to block from the drop-down list.
4. Select the classes you want to disable on this device bus. To block the bus entirely, select all classes.
5. Click **Save**.
6. To remove a device from the list, select the corresponding item in the list and click .
7. To edit the list of classes disabled on this device bus, select the necessary device bus in the **Blocked buses** list and click .
8. To add other devices, repeat steps 1 and 2.



Example

If you want to block all flash drives,

1. Make sure that the **Control access to the protected objects** option is enabled.
2. In the **Device buses** section, click .
3. Select the **USB devices** bus from the drop-down list.
4. Select the **Disk drives** class that will be blocked on this bus.
5. Click **Save**.

If you want to allow access to a certain device, add it to the [white list](#).



Note that stations will not be connected to Dr.Web Server if the following options are enabled:

- **Block data transfer over network.**
- **Control access to the protected objects > Device classes > Network adapters.**

These options block all network interaction for stations. At this, you cannot use Control Center to change settings remotely either.


3.2.3.2. User-Defined

3.2.3.2.1. User-Defined

On the **User-defined** page, you can allow station users to access websites, local directories and files. You can also set time limits on using the Internet and computer.

The parameters of Office Control are applied to all users of the computer where Dr.Web Agent is installed. By default, access to the Internet and to local resources is not restricted to any of the accounts; no time limits are set.

Structure of station users

- The structure of station users is displayed as a tree that includes user groups and individual users. By default, **Administrators**, **Guests** and **Users** groups are set.
- All the existing user groups are available after the station is connected to the Server.
- If Active Directory service is used in your LAN, you can add its individual users. To do that, click  and set the search parameters in the **Search of users on LDAP server** window. Selected users will be added to the **Active Directory** group.

Types of user settings

- *General*—general settings for the **Users** root group. They are used by default.



- *Inherited*—root group settings that are inherited from the **Users** root group in case settings for user groups and individual users are not specified. At this, user settings section is empty.
- *Personal*—personal settings for user groups and individual users that are not inherited from the root group.
 - a) To specify personal settings, select the corresponding user group or individual user in the tree structure and click **Specify settings**. Root group settings are copied from the root group. You can edit them if necessary.
 - b) In case personal settings are specified, you can remove them. To do this, select an existing user group or an individual user and click . At this, root group settings will be used.

Web filtering

- Select the **No restrictions** mode to allow access to all websites. This mode is enabled by default.
- Select the **Block by categories** mode to add categories to the black and while lists manually to block or allow access to the resources regardless of other restrictions.
- Select the **Block all except websites from the white list** mode to deny access to all web resources except for those in the white list.

In any mode except for the **No restrictions** one, you can enable the **Enable safe search** option to manage results of the search engines. This option allows to exclude unwanted resources from search results.

Black and White Lists

You can create lists of websites to block or allow access to the resources regardless of other settings. By default, both lists are empty. If required, you can add addresses to the black and white lists.

To configure domain addresses lists

1. Enter a domain name or a part of a domain name for the website in the **White list** or **Black list** field depending on whether you want to allow or block access to it:
 - a) To add a certain website, enter its URL (for example, `www.example.com`). This allows access to all webpages located on this website.
 - b) To allow access to websites whose URL contains a certain text, enter this text in the input field. For example, if you enter `example`, then the access to `example.com`, `example.test.com`, `test.com/example`, `test.example222.ru`, and others will be granted.
 - c) To allow access to websites within a particular domain, enter the domain name with a period (.) character, for example, `.com`. This allows access to all webpages located on this domain.



If the domain name includes a forward slash (/), the substring before the slash is considered a domain name, while the substring after the slash is considered a part of address for the websites that you want to access within this domain. For example, if you enter `example.com/test`, such webpages as `example.com/test11`, `template.example.com/test22`, and so on will be processed.

- d) To add certain websites to the exclusions, enter the mask of their names. Masks will be added in the `mask://... format`.



A mask denotes the common part of object names, at that:

- The asterisk (*) character replaces any, possibly empty, sequence of characters.
- The question mark (?) replaces any, including an empty, character (one).

Examples:

- `mask://*.com/` or `.com`—enable opening of all the domain .com websites;
- `mask://mail`—enable opening of all websites whose names contain the word “mail”;
- `mask://??? .com`—enable opening of all the domain .com websites, whose names consist of three characters or less.

Your input may be unified. For example: the `http://www.example.com` address will be transformed into `www.example.com`.

2. To add one more object to the list, click .
3. To remove the address from the list, click  next to the list item that corresponds the address.
4. To add other devices, repeat steps 1 and 2.




If traffic is encrypted (HTTPS websites), black and white lists can include domain addresses only (for example, `https://example.com`).

You can configure access to individual pages of the domain for unencrypted traffic only (HTTP websites) (for example, `http://example.com/test`).


Folders and files

Enable the **Protect folders and files** option to block access to all resources listed below.

To configure the list of protected files and folders

1. To add an object, enter the path in the corresponding field.
2. Select limitation mode:
 - a) **Read-only**—an added object will be read only.
 - b) **Blocked**—to block access to the specified object completely.
3. You can specify only one object in one field. To add one more object to the list, click .





4. To remove an object from the list, click  next to the list item that corresponds the object.
5. To disable all limitations for all objects in the list, disable the **Protect folders and files option**.

Time limits

You can set restrictions on time the user can spend on the Internet or work on the computer. By default, no time limits on the computer and Internet use are set.

To set time limits for a particular profile

1. To add a new profile to the list, click .
2. In the **New profile** window, enter a profile name.
3. Click **Save**.
4. To remove a profile from the list, select the corresponding item in the list and click .
5. If necessary, repeat steps 1 and 2 to add other profiles.
6. Configure the limitation mode using the table of time limits.

How to use the table of time limits

Using the table, you can specify hours and days of the week when users are allowed to use the computer or access the Internet. The restriction is set to every 30 minutes of every weekday.

Color	Limitation mode	Mode description
White	No restrictions	Access to the Internet and computer are allowed in the specified period. This mode is set by default.
Blue	Block Internet access	Access to all web resources is blocked in the specified period. Once the limitation period starts, the access to all websites is blocked.
Red	Block all	Access to the computer is blocked in the specified period. Once the limitation period starts, the user is logged off.



To restrict access to the Internet

Select days of the week and hours when the user is *restricted from accessing the Internet* and then mark the corresponding timeslots blue:

- To mark one timeslot, click it once.
- To mark several adjacent timeslots, click the first slot once and select the rest of required squares while holding down the mouse button.

To restrict access to the computer

Select days of the week and time when the user is *restricted from using the computer*, and then mark the corresponding timeslots red.

- To mark one timeslot, click it twice.
- To mark several adjacent timeslots, click the first slot twice and select the rest of required squares while holding down the mouse button.

3.2.3.2.2. White List

If you have [restricted access](#) to some device classes or buses, you can allow access to certain devices by adding them to the white list.

You can allow access to any types of devices, including removable media (USB flash, floppy, CD/DVD, ZIP drives, etc.), keyboards, printers, LAN adapters and so on. You can also add a certain device to the white list to exclude it from the scan for BadUSB vulnerability.

You can allow access to devices for all users, user groups and individual users.

To configure the general white list

1. Select the **Users** root group.
2. Enable the **Allow access for devices from the white list** option. The access for devices from the general white list is allowed to all users with Dr.Web for OS Window installed.



The option is available for the **Users** root group only. In case the access for devices from the white list is allowed, you can configure users white lists.


3. [Configure](#) the white list.

To configure the users white list

1. Select the necessary user group or an individual user (see [Types of user settings](#)).
2. Open the **White list** section.
3. [Configure](#) the white list.




To configure the white list of devices for users and groups of users

1. To add a device to the list, click .
2. In the **Add devices to the white list** window, use the following options:
 - Select a device in the **Previously connected devices** field and transfer it to the **Devices for adding to the white list** field using the arrow.




You can add the selected element to the **Previously connected devices** field either as a device, or as a mask. The mask allows to exclude the device that generates new ID every time it connects to the station.

- Specify the device ID manually in the corresponding field and click .




Previously connected devices list is available for individual users only.

Previously connected devices list is available after the station is connected to the Server.

3. Click **Save**.
4. To configure access rules for devices with file systems, enable the **Read** option to browse the device and the **Write** option to change it. The rules for devices with file systems can be specified for user groups and individual users only.
5. To remove a device from the list, select the corresponding item in the list and click .
6. To add other devices, repeat steps 1 and 2.

To configure the white list of devices for groups of stations


1. Select the corresponding group of stations.
2. Open the **White list** section.
3. To add a device to the list, click .
4. In the **Add devices to the white list** window, select a station. The list of devices previously connected to this station opens.
5. Select a device in the **Previously connected devices** field and transfer it into the **Devices for adding to the white list** field using the arrow. Device ID will appear in the **Specify the device ID manually** field.



You can add the selected element to the **Previously connected devices** field either as a device, or as a mask. The mask allows to exclude the device that generates new ID every time it connects to the station.

6. Click .
7. Click **Save**.



- To configure access rules for devices with file systems, enable the **Read** option to browse the device and the **Write** option to change it. The rules for devices with file systems can be specified for user groups and individual users only.
- To remove a device from the list, select the corresponding item in the list and click .

3.2.4. Dr.Web Agent

3.2.4.1. General

On the **General** tab, you can set the following parameters of the Agent:

- In the **Task Scheduler startup delay (min.)** field, specify the time interval between the start of the OS and the execution of the startup scan task, if it was scheduled for the Agent. The 1 minute delay is set by default. Set the 0 value to perform the scan task without any delay, i.e. immediately after the start of the OS.
- In the **Period of statistics sending (min.)** field, specify the value of the time interval in minutes for the Agent to send to the Server all statistics data, collected by the SpIDer Guard, SpIDer Mail and SpIDer Gate components at the station. Specify the 0 value to disable statistics sending.
- In the **Interval of virus databases relevance** field, specify the time interval during which the virus databases installed on stations are considered up-to-date. The start of the interval is the moment of virus databases creation. During specified period, notifications about out-of-date virus databases are not displayed.
- In the **Language** drop-down list, specify the language for the Agent and Dr.Web Anti-virus components interface at the station or group of stations.
- Set the **Enable Microsoft Network Access Protection** flag to enable station state monitoring using *Microsoft® Network Access Protection (NAP)* technology. This enables the *System Health Agent (SHA)* which is automatically installed in a workstation with Dr.Web Agent software.
- Set the **Allow quarantine remote control** flag to enable remote control of workstations Quarantine from the Server.



The **Allow quarantine remote control** option is available if in the **Administration** → **Dr.Web Server configuration** → **Statistics** tab, the **Quarantine state** flag is set.

- Set the **Collect information about stations** flag to enable collecting information about software and hardware at the stations. When the flag is set, in the **Period of collecting information about stations (min.)** drop-down list, select period in minutes of sending actual information on hardware and software by Agent from station to the Server.
- Set the **Synchronize time** flag to enable system time synchronization on the Agent computer with the time on the computer with Dr.Web Server installed.
- Set the **Block changing of system date and time** flag to prevent manual and automatic change of the system date and time as well as of the time zone except for the time synchronization with Dr.Web Server (which is set by the **Synchronize time** flag).



- Set the **Block user activity emulation** flag to prevent any changes in the Dr.Web operation, except for those made manually by the user. This option allows to prevent any automatic changes in the Dr.Web operation, including execution of scripts that emulate user interaction with Dr.Web and are launched by the user.
- Set the **Enable hardware virtualization** flag to take full advantage of the computer resources, which makes detection and curing of threats easier and enhances self-protection of Dr.Web. To enable this option, restart of the station is required.



Hardware virtualization works only if the station hardware and operating system support hardware virtualization.

Enabling this option may cause a conflict with some third-party software.

If problems occur, disable this option.

32-bit platforms do not support hardware virtualization.

3.2.4.2. Mobility

On the **Mobility** tab, you can specify parameters of the [Mobile Mode](#) of the Agent:

- In the **Update period** field, specify the time interval between the anti-virus software updates on station using GUS servers.
In the **Manual** mode, automatic updates are disabled. In this case, to receive the latest virus databases, the user must launch the update in the Agent settings on the station.
- Set the **Use proxy server** flag to use an HTTP proxy server to receive updates from the Internet. This will make the fields to set a proxy server available.

Updating Mobile Dr.Web Agents

If the user's computer has no connection to Dr.Web Server for a long time, to receive updates in time from the Dr.Web GUS, it is recommended that you set the Agent mobile mode of operation on the station.

In the mobile mode, the Agent tries to connect to the Server three times and, if failed, performs an HTTP update. The Agent tries continuously to find the Server at interval of about a minute.



The mobile mode will be available in the Agent settings if the mobile mode has been allowed in the Control Center, in the **Anti-virus Network** → **Permissions** → **Windows** → **General** → **Run in mobile mode** section.



When the Agent is functioning in the mobile mode, the Agent is not connected to Dr.Web Server. All changes made for this workstation at the Server, will take effect once the Agent mobile mode is switched off and the connection with the Server is re-established.



In the mobile mode only virus databases are updated.

Description of the mobile mode configuration at the Agent side is given in the **User Manual** of Dr.Web Agent for Windows.

3.2.4.3. Log

On the **Log** tab, you can specify logging parameters of Agent and some Dr.Web Anti-virus components:

- The **Agent log verbosity level** parameter determines the level of detail of Agent logging (the `dwservice.log` and `es-service.log` files).
- The **Engine log verbosity level** parameter determines the level of detail of engine logging (engine logging data is written into the system log file).
- The **Update log verbosity level** parameter determines the level of detail of Dr.Web updating module logging (the `dwupdater.log` file).
- Enable the **Create memory dumps at scan errors** option to create memory dumps in case of scan errors. It is recommended that you enable this setting for Dr.Web operation errors analysis.
- Enable the **Set limitations on the Agent log file** option to limit the number of log files, their size or the time of writing log data into each file.
 - **Maximum number of files**—maximum number of log files (including the current and the archived) that will be stored.
 - Enable the **Archive log files** option to archive old log files at rotation.
 - **Log rotation mode**—rotation mode of the operation log. Select one of the following values:
 - **rotation by size** sets the limit on the size of each log file.
Maximum size of each file—maximum allowed size of each log file. When the current file reaches the specified size, it is archived with the corresponding change of its name, and a new log file is created.
 - **rotation by time** sets the time limit on writing log data into each file.
Maximum time to write the file—maximum time of writing log data into each file. When the time reaches the specified duration, the file is archived with the corresponding change of its name, and a new log file is created.

3.2.4.4. Interface

On the **Interface** tab, you can specify the parameters of the Agent interface:

- Set the **Show icon in taskbar** flag to display Agent icon in the taskbar. If icon is disabled, user cannot view and edit settings of Agent and the anti-virus package.



- Set the **Show reboot request on components update** flag to display a request on station reboot if the station received updates of anti-virus components which require reboot to be applied. If the flag is cleared, request is not displayed at the station and the automatic reboot is not performed. Statistics of a station received by the Control Center, contains notification on the need of station reboot. Information on a state that requires reboot is displayed in the **State** table. Administrator is able to reboot a station from the Control Center if necessary.



The **Show reboot request on components update** flag does not affect on displaying reboot requests which are required to complete the cure of detected threats or changing the state of hardware virtualization. These requests are always displayed.

To select the type of events which a user will receive, set the corresponding flags:

- **Critical notifications**—receive only critical notifications on the following events:
 - connections waiting for Firewall to reply are detected;
 - login (identifier) of the station and password are already used for connection to the Server.

The notification shows, if the user has administrator privileges.

- **Threat notifications**—receive only notifications about threats. This type of notification includes messages about threats detection by one of the anti-virus software components.
- **Major notifications**—receive only important notifications on the following events:
 - time limit set for working on the computer is about to expire;
 - access to a device is blocked;
 - access to a protected object is blocked by Preventive Protection;
 - attempt to change system date and time is blocked;
 - virus databases are out-of-date (when operating in Mobile mode).
- **Minor notifications**—receive only minor notifications on the following events:
 - successful update;
 - update failures;
 - time limit set for Internet use is about to expire;
 - URL is blocked by Office Control;
 - URL is blocked by SpIDer Gate;
 - access to the protected object is blocked by Office Control;
 - scan of a station is run by administrator from the Control Center;
 - scan of a station is run according to a central schedule;
 - scan of a station is finished.

If you want messages of all groups to be sent, set all the four flags. Otherwise only message of the specified groups will be displayed.



Notifications on the following issues are not included in any of the specified groups and are always displayed to a user:

- priority updates installed and restart is required;
- to finish neutralizing threats, restart the computer;
- to enable or disable the hypervisor, restart the computer;
- request for allowing a process to modify an object;
- messages sent by the administrator from the Control Center;
- USB device (keyboard) connected/blocked within protection from BadUSB vulnerability.

In the **Additional** subsection, you can specify the following settings:

- Set the **Do not show notifications in full-screen mode** flag to disable popup notifications if any program is running in full-screen mode.
- Set the **Display Firewall notifications on separate desktop in full-screen mode** flag to display Dr.Web Firewall notifications on a separate desktop, i.e. on top of running full-screen application. It is recommended that you enable this option to avoid blocking network connections which are used by this full screen mode application without a possibility to enable them when the Dr.Web Firewall request is received.

3.2.4.5. Events

Dr.Web Agent sends to the Server the information about the following events:

- Program starts and stops
- Threat detection
- Task Scheduler assignments completion
- [Device blocking](#)

The information is sent to the Server the moment the event occurred. In case events sending is prohibited, the information is accumulated in the database. The information will be sent to the Server when event sending is allowed.

To change the events sending mode, enable the **Restrict events sending** option. By default, events sending is prohibited.

In the table, you can specify the restriction mode according to colors below the table:

- White—**No restrictions**
- Red—**Data transfer is prohibited:** events sending is blocked completely

The restriction is set to every 30 minutes of every weekday.

To change the access restriction mode, click on the corresponding table block. The color of boxes changes cyclically according to the color scheme below the table. You can also select several timeslots using the drag-and-drop method.



3.2.5. Dr.Web for Microsoft Outlook

3.2.5.1. General

- The **Enable the check** option allows to activate the Dr.Web for Microsoft Outlook plug-in.
- The **Check archives** option allows to enable or disable the check of attached archived files.

3.2.5.2. Actions

On the **Actions** tab, you can select actions to be applied to threats detected by Dr.Web for Microsoft Outlook, depending on their type.

- **Cure.** Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, the action from the **Incurable** list is applied. The action is available only for objects infected with a known virus that can be cured except for Trojan programs and files within complex objects.
- **Move to quarantine.** This action moves a detected threat to a special folder that is isolated from the rest of the system.
- **Delete.** It is the most effective way to remove all types of threats. This action implies full deletion of a dangerous object.
- **Ignore.** No actions are applied to the object. Notifications are not displayed.



The default settings are optimal for most cases. Do not change them unnecessarily.

3.2.5.3. Log

Enable the **Detailed logging** option to log read/write errors or errors occurred while scanning archives or password-protected files, parameters of such program components as scanner, core, virus databases, and messages on core failures.



By default, size of a log file is restricted to 10 MB. If the log file size exceeds the limit, the content is reduced to:

- Specified size if the current session information does not exceed the limit.
- Size of the current session if the session information exceeds the limit.

If the **Detailed logging** option is enabled, operation of corresponding component is logged in the debug mode with maximal detailing. Limitations on the file size are disabled in this mode. This leads to significant increasing of the log file size. Also note, that the rotation of the log file is not performed (in all logging modes).

Debug logging mode decrease performance of Anti-virus and operating system of a station. It is recommended that you use this mode only when problems occur in component





operation or on request of technical support service. It is not recommended to enable logging debug mode for extended period of time.



On the Control Center, the logging settings are specified separately for each component on the **Log** sections. On stations, logging settings are specified in the **Advanced** common section.

3.2.5.4. Anti-Spam

To configure spam filter operation settings

- Enable the **Check mail for spam** option to enable the spam filter.
- You can enable addition of special text to the spam message header by enabling the **Add a prefix to headers of spam messages option**. Type the text to add in the **Prefix** field. The default prefix is *****SPAM*****.
- The checked messages can be marked as read in email options. For that purpose, enable the **Mark as read option**. By default, this option is enabled.
- You can also configure white and black lists of email addresses and domains for email filtration.
 - a) Specify an address in the corresponding field. Rules for specifying addresses are listed below.
 - b) You can specify only one email address in one field. To add one more address to the list, click .
 - c) To remove the address from the list, click  next to the list item that corresponds the address.

Black list

If the sender's address is on the black list, the message will be automatically regarded as spam.

- To add a specific sender to the list, enter the full email address (for example, `spam@spam.com`). All messages, received from this address, will be automatically regarded as spam.
- Each list item can contain only one email address or email address mask.
- To add a group of sender addresses, enter the mask that determines their names. The mask defines a template for an object definition. It may contain regular characters from email addresses and a special asterisk character (*), which replaces any (including an empty one) sequence of characters.

For example, the following variations are possible:

▫ `mailbox@domain.com`



- *box@domain.com
- mailbox@dom*
- *box@dom*



The asterisk (*) can be specified at the start or at the end of an address only.

The 'at' sign (@) is mandatory.

- To regard messages sent from any email address within a domain as spam, use an asterisk character (*) instead of the user name in the address. For example, if you enter *@spam.com, all messages from addresses within the spam.com domain will be regarded as spam automatically.
- To regard messages sent from an email address with a certain user name from any domain as spam, enter an asterisk character (*) instead of the domain name in the address. For example, if you enter john@*, all messages from all senders with the john mailbox name will be regarded as spam automatically.
- Addresses from the recipient domain are not processed. For example, if the recipient mailbox (your mailbox) is in the mail.com domain, then messages from the mail.com domain will not be processed with the anti-spam filter.

White List

If the sender's address is added to the white list, the email will not be checked on spam. However, if the domain names in the receiver's and sender's addresses are similar, and this domain name is specified in the white list using the (*) character, this message is checked for spam.

- To add a specific sender to the list, enter the full email address (for example, mail@example.net). This ensures delivery of all messages from this sender with no spam check.
- Each list item can contain only one email address or email address mask.
- To add a group of sender addresses, enter the mask that determines their names. The mask defines a template for an object definition. It may contain regular characters from email addresses and a special asterisk character (*), which replaces any (including an empty one) sequence of characters.

For example, the following variations are possible:

- mailbox@domain.com
- *box@domain.com
- mailbox@dom*
- *box@dom*



The asterisk (*) can be specified at the start or at the end of an address only.

The 'at' sign (@) is mandatory.

- To ensure the delivery of messages sent from any email address within a certain domain, use an asterisk (*) instead of the user name in the address. For example, if you enter *@example.net, messages from all senders within the example.net domain will be delivered without check.
- To regard messages sent from an email address with a certain user name from any domain as spam, enter an asterisk character (*) instead of the domain name in the address. For example, if you enter john@*, all messages from all senders with the john mailbox name will be regarded as spam automatically.

3.2.6. Preventive Protection

On the **Preventive Protection** tab, you can configure Dr.Web reaction to actions of other programs that can compromise workstation security. Also, you can select a level of protection against exploits.

At that, you can configure a separate protection mode for particular applications or configure a general mode whose settings will be applied to all other processes.

Block WSL

Set the **Block WSL** flag to block Windows Subsystem for Linux on stations with Dr.Web Agent installed.



The option is relevant for Windows 10 only.

Exploit Prevention

In the **Exploit prevention** section, you can configure the blocking of malicious programs that use vulnerabilities of well-known applications. From the corresponding drop-down list, select the required level of protection.

Protection level	Description
Prevent unauthorized code from running	If an attempt of a malicious object to exploit software vulnerabilities to get access to critical regions of the operating system is detected, it will be blocked automatically.



Protection level	Description
Interactive learning mode	If an attempt of a malicious object to exploit software vulnerabilities to get access to critical regions of the operating system is detected, Dr.Web will display an appropriate message. Read the information and select a suitable action.
Allow unauthorized code to be executed	If an attempt of a malicious object to exploit software vulnerabilities to get access to critical regions of the operating system is detected, it will be allowed automatically.

Level of Suspicious Activity Blocking

In the **Level of suspicious activity blocking** section, you can configure a general protection mode whose settings will be applied to all processes if the personal mode from the section [below](#) is not specified. You can also protect user data from unwanted changes.

Select one of protection levels that anti-virus provides:

- **Paranoid**—maximal protection level when you need total control of access to critical Windows OS objects.



Using this mode may lead to compatibility problems with legitimate software that uses the protected registry branches.

- **Medium**—protection level at high risk of computer getting infected. In this mode, the access to the critical objects that can be potentially used by malicious software is additionally blocked.
- **Optimal**—protection level that disables automatic changes of system objects, modification of which explicitly signifies a malicious attempt to damage the operating system.
- **User-defined**—protection level that is set by a user (the Server administrator) and based on settings specified in the table below.

To specify custom settings of preventive protection level, set the flags in the table of this section to one of the following positions:

- a) **Allow**—always allow actions with this object or from this object.
- b) **Ask**—prompt the dialog box for setting necessary action by the user for the specific object.
- c) **Block**—always deny actions with this object or from this object.

If you change table settings when one of the preinstalled levels in the **Level of suspicious activity blocking** section is set, it automatically changes to **User-defined**.

You can create several independent user-defined profiles.

To add a new user-defined profile, click . In the opened window, specify the name of a new profile and click **Save**.



To delete user-defined profile that you had created, select it in the **Level of suspicious activity** blocking list and click . You are not allowed to delete predefined profiles.

Preventive protection settings allow to monitor the following objects:

- **Integrity of running applications**—detect processes that inject their code into running applications that may compromise computer security. Processes that are added to the exclusion list of the SplDer Guard component are not monitored.
- **Integrity of users files**—detect processes that modify user files with the known algorithm which indicates that the process may compromise computer security. Processes that are added to the exclusion list of the SplDer Guard component are not monitored. To protect your data from unauthorized modifications, it is recommended that you set the creation of protected copies for important files.
- **HOSTS file**—the operating system uses this file for simplifying access to the Internet. Changes to this file may indicate virus infection or other malicious program.
- **Low level disk access**—block applications from writing on disks by sectors avoiding the file system.
- **Drivers loading**—block applications from loading new or unknown drivers.

Other options control access to critical Windows OS objects and allow protection of the following registry branches from modification (in the system profile as well as in all user profiles).

Protected registry branches

Option	Registry branch
Image File Execution Options	Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
User Drivers	Software\Microsoft\Windows NT\CurrentVersion\Drivers32 Software\Microsoft\Windows NT\CurrentVersion\Userinstallable.drivers
Winlogon parameters	Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL
Winlogon notifiers	Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify
Windows shell autorun	Software\Microsoft\Windows NT\CurrentVersion\Windows, Applnit_DLLs, LoadApplnit_DLLs, Load, Run, IconServiceLib
Executable files associations	Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (keys) Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (keys)



Option	Registry branch
Software Restriction Policies	Software\Policies\Microsoft\Windows\Safer
Internet Explorer plug-ins (BHO)	Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
Program autorun	Software\Microsoft\Windows\CurrentVersion\Run Software\Microsoft\Windows\CurrentVersion\RunOnce Software\Microsoft\Windows\CurrentVersion\RunOnceEx Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup Software\Microsoft\Windows\CurrentVersion\RunOnceEx\Setup Software\Microsoft\Windows\CurrentVersion\RunServices Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
Policy autorun	Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
Safe mode configuration	SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal SYSTEM\ControlSetXXX\Control\SafeBoot\Network
Session Manager parameters	System\ControlSetXXX\Control\Session Manager\SubSystems, Windows
System services	System\CurrentControlSet\XXX\Services



If any problems occur during installation of important Microsoft updates or installation and operation of programs (including defragmentation programs), disable the corresponding options in this group.



Personal Parameters of Access

In the **List of applications with personal parameters of access to the protected objects** section, you can configure the separate protection mode for particular applications. To all other processes, the settings specified in the section [above](#) will be applied.

To Edit a Rule

1. To add one more rule, click .
 - a) To configure the added rule, click next to this rule.



- b) In the opened window, specify the path to the application executable file on a protected workstation.
 - c) Look through default settings and, if necessary, edit them.
 - d) Click **Save**.
2. To edit an existing rule, click  to the necessary rule and perform the steps from the units 1.a) - 1.d).
 3. To delete an existing rule, click  next to the necessary rule.

3.2.7. Dr.Web Firewall



In case the station user is allowed to configure **Dr.Web Firewall**, settings are displayed as personal.

3.2.7.1. Application Filter



The majority of **Application filter** options are set on station only, see **Dr.Web for Windows. User Manual**.

Application level filtering helps you to control access of various applications and processes to network resources as well as to enable or disable applications to run other processes. You can create rules for both system and user applications.

To set operation mode

Select one of the following operation modes:

- [Allow unknown connections](#)—free access mode, when all unknown applications are permitted to access networks.
- [Block unknown connections](#)—restricted access mode, when all unknown connections are blocked. For known connections, Firewall applies the appropriate rules.
- [Interactive learning mode](#)—learning mode, when the user is provided with full control over Firewall reaction.
- [Allow connections for trusted applications](#)—an access mode, when all trusted applications are allowed to access network resources, for all other applications, a warning is displayed. You can set an application rule via such warning (set by default).

Allow unknown connections

In this mode, Firewall allows all unknown applications for which filtering rules have not been set to access network resources, including the Internet. No notification on access attempt is displayed by Firewall.



Block unknown connections

In this mode, Firewall automatically blocks all unknown connections to network resources, including the Internet.

When a user application or the operating system attempts to connect to a network, Firewall checks whether filtering rules have been created for the application. If there are no filtering rules, Firewall blocks network access for the application without displaying any notifications to the user. If filtering rules for the application are set, Firewall processes the connection according to the specified actions.

Interactive learning mode

In this mode, you have total control over the Firewall reaction to the detection of unknown connections. Thus, the program is trained while you work on your computer.

When a user application or an operating system attempts to connect to a network, Firewall checks whether filtering rules have been created for the application. If no filtering rules have been set, you are prompted to select a temporary solution or to create a rule to be applied each time this type of connection is detected.

Allow connections for trusted applications

This mode is set by default.

In this mode, all trusted applications are allowed to access network resources, including the Internet. Among trusted applications are system applications, applications with Microsoft certificate, and applications from Dr.Web list of trusted applications. Rules for such applications are not displayed in the rule list. For other applications, Firewall prompts you to allow or block the unknown connection manually, as well as create a new rule for it.

When a user application or an operating system attempts to connect to a network, Firewall checks whether filtering rules have been created for the application. If no filtering rules have been set, you are prompted to select a temporary solution or to create a rule to be applied each time this type of connection is detected.

The **Allow local connections** option allows all applications on your computer to interconnect (i.e., allow unlimited connections between applications installed on your computer). For this type of connection, no rules are applied. Disable this option to apply filtering rules to connections carried out both through the network and within your computer.

3.2.7.2. Packet Filter



By default, packet filter is disabled on the Server. When a station connects to the Server, packet filtering settings specified on the Server are set on the station. Thus, packet filter will be disabled even if it was enabled and configured on the station.



By default, packet filter is disabled on Dr.Web Agent provided with Enterprise Security Suite 11.0.2. At that, if Agent has already been installed with a previous version, than packet filter will be disabled during the update. If not, Agent is installed with disabled packet filter by default.

Packet filtering allows you to control access to network regardless of what program initiates the connection. These rules are applied to all network packets transmitted through a network interface of your computer.

To configure packet filtering settings, select the following options:

Option	Description
Enable packet filter	Select this check box to enable and configure filtering packets for known network interfaces. If the flag is cleared, you will be allowed to configure the access to network resources only for specific applications.
Enable dynamic packet filtering	Select this check box to filter packets according to the state of existing TCP connections. Firewall will block packets that do not match the TCP protocol specification. This option helps to protect your computer from DoS (denial-of-service) attacks, resource scanning, data injection and other malicious operations. It is also recommended that you select this check box when using protocols with complicated algorithms of data transfer (FTP, SIP, and so on.) Clear the check box to filter packets regardless of the TCP session state.
Process fragmented IP packets	Select this check box to ensure correct processing of large amounts of data. The maximum transmission unit (MTU) may vary for different networks, therefore large IP packets may be fragmented. When this option is enabled, the rule selected for the first fragment of a large IP packet is applied to all other fragments. Clear this check box to process fragmented packets independently.

Packet filter rules

Dr.Web Firewall uses the following predefined rule sets:

- **Default Rule**—rules that identify common network configurations and widespread attacks (this rule set is used by default for new network interfaces).
- **Allow All**—all packets are passed through.
- **Block All**—all packets are blocked. At that, the Agent—Server connection is blocked.



For the fast switching between filtering modes, you can create custom sets of filtering rules.

- To set an existing set of rules by default, select it in the list and click ✓;
- To edit an existing set of rules, select it in the list and click ✎;
- To copy an existing set of rules, select it in the list and click 📄.
- To remove an existing set of rules, select it in the list and click 🗑️.

To create a new set of rules

1. In the **Rule sets** window, click +.
2. Enter the name of a new rule set.
3. Click **Save**. The **Creating a new rule** form appears.
4. Configure the necessary rule [parameters](#).




In case parameters of the rule is not saved, a new rule set is not created.

To configure a new rule

1. In the **Rule sets** window, select the rule set that you want to add.
2. In the **Rules** window, click + to create a new rule. This opens a rule creation window for packet filters.
3. Configure the following parameters:

Parameter	Description
Rule name	The name of the created/edited rule.
Description	The rule description.
Action	The action for Firewall to perform when a packet is intercepted: <ul style="list-style-type: none">• Allow packets—passes the packet through.• Block packets—blocks the packet.
Direction	The direction of the connection: <ul style="list-style-type: none">• Inbound—the rule is applied when a packet is received from the network.• Outbound—the rule is applied when a packet is sent into the network from your computer.• Any—the rule is applied regardless of packet transfer direction.
Logging	The logging mode for the rule. This parameter defines which information should be stored in the log: <ul style="list-style-type: none">• Disabled—no information is logged.



Parameter	Description
	<ul style="list-style-type: none">• Headers only—log the packet header only.• Entire packet—log the whole packet.
Criterion	Filtering criterion. For example, transport or network protocol. To add a filtering criterion, select the necessary criterion from the Criteria list and transfer it to the left field using the arrow. You can add any number of filtering criteria. For certain criteria, there are additional parameters available. To delete a criterion, select it in the list and click  .



If you do not add any criterion, the rule will allow or block all packets depending on the setting specified in the **Action** field.



Some filtering criteria are not compatible with the others. When you add/delete a criterion, only criteria that are compatible with the existing ones are shown in the **Criteria** list.

4. When the editing is over, click **Save** to save the changes.



The packet should meet all the criteria of the rule in order for the rule action to be applied to the packet.

To edit a rule

1. In the **Rule sets** window, select the rule set that you want to edit.
2. In the **Rules** window, select the rule from the list.
3. Click . This opens a rule modification window.
4. Configure the rule [parameters](#).
5. When the editing is over, click **Save** to save the changes.
6. To remove a rule, select it from the list and click .

Network interfaces



This setting is available after selecting the station only.

In the **Network interfaces** section, you can select a rule set to be used for filtering packets transmitted through a certain network interface.

To set rule sets for network interfaces, select the appropriate rule set for the required interface. If the appropriate rule set does not exist, you can [create](#) a new set of packet filtering rules.



3.2.7.3. Log

Enable the **Detailed logging** option to log data on network packets (pcap logs).



By default, size of a log file is restricted to 10 MB. If the log file size exceeds the limit, the content is reduced to:

- Specified size if the current session information does not exceed the limit.
- Size of the current session if the session information exceeds the limit.

If the **Detailed logging** option is enabled, operation of corresponding component is logged in the debug mode with maximal detailing. Limitations on the file size are disabled in this mode. This leads to significant increasing of the log file size. Also note, that the rotation of the log file is not performed (in all logging modes).

Debug logging mode decrease performance of Anti-virus and operating system of a station. It is recommended that you use this mode only when problems occur in component operation or on request of technical support service. It is not recommended to enable logging debug mode for extended period of time.



On the Control Center, the logging settings are specified separately for each component on the **Log** sections. On stations, logging settings are specified in the **Advanced** common section.

3.2.8. Network Port Monitor



The **Network port monitor** options are set on the Server only. They are not available to the station users.

Network port monitor checks ports used by TCP transport protocols. The intercepted connection is analyzed and, according to the traffic content, protocol type is defined. The necessary settings are used depending on the protocol type. Email protocols are scanned in accordance with the [Spider Mail](#) settings, others in accordance with the [SpIDer Gate](#) and [Office Control](#) settings.

- **SpIDer Mail** intercepts data exchange between mail clients and mail servers made via POP3, SMTP, IMAP4, or NNTP (IMAP4 stands for IMAPv4rev1) protocols, detects and neutralizes threats before the mail is transmitted to the Server.
- **SpIDer Gate** checks incoming HTTP traffic and blocks all malicious objects (in case default settings are used). HTTP protocol is used by web browsers, download managers, and other applications which exchange data with web servers, i.e. work with the Internet.
- **Office Control** restricts users to access websites in accordance with the [Web filtering](#) and [Black and White lists](#) options.




In case **Network port monitor** scans a specific port, **SplDer Mail** and **SplDer Gate** do not check applications or processes that use this port if they are added to the [Excluded applications list](#).

In case **Network port monitor** scans ports used by HTTP protocols, **SplDer Gate** does not check websites that are added to the **Office Control White list**.

By default, **Network port monitor** checks the inbound and outbound traffic on all the ports. Enable the **Check traffic only on specified ports** option to check the traffic on the ports specified in the **Ports** list.

By default, numbers of ports used by email and HTTP protocols are specified in the **Ports list**.

- To add a new port to the list, click .
- To remove a port from the list, click  next to the list item that corresponds the port.

3.2.9. SplDer Mail and SplDer Gate

3.2.9.1. SplDer Mail

3.2.9.1.1. General

On the **General** tab, you can select actions to apply to threats detected by SplDer Mail, depending on their type.

- **Cure, move to quarantine if not cured.** Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is moved to quarantine. The action is available only for objects infected with a known virus that can be cured except for the Trojan programs and files within complex objects.
- **Cure, delete if not cured.** Instructs to restore the original state of the object before infection. If the object is incurable, or the attempt of curing fails, this object is deleted. The action is available only for objects infected with a known virus that can be cured except for the Trojan programs and files within complex objects.
- **Move to quarantine.** This action moves a detected threat to a special folder that is isolated from the rest of the system.
- **Delete.** It is the most effective way to remove all types of threats. This action implies full deletion of a dangerous object.
- **Ignore.** No actions are applied to the object. Notifications are not displayed.



The default settings are optimal for most cases. Do not change them unnecessarily.



Scan options

The following settings allow you to configure additional email scanning parameters:

- **Use heuristic analysis.** In this mode, special methods are used to detect suspicious objects in emails that are most likely to be infected with unknown viruses. Disable this option to not use the heuristic analysis.
- **Check installation packages.** It instructs to check installation package files. This option is disabled by default.

Scanning optimization options

You can set the condition under which SpIDer Mail should acknowledge complex messages, whose scan is time consuming, as unchecked. To do that, enable the **Message scan timeout (sec.)** option and set the maximum email scanning time. After the expiry of the specified period, SpIDer Mail stops scan of the email. Default value is 250 seconds.

Additional actions on messages

In this group, you can configure additional actions to be applied when SpIDer Mail processes emails.

- **Insert “X-AntiVirus” header”.** It instructs to add scan results and information on Dr.Web version to email headers after processing by SpIDer Mail. You cannot edit a header format. This option is enabled by default.
- **Delete modified messages on server.** It instructs to remove emails to which either Delete or Move to Quarantine action was applied by SpIDer Mail. The emails are removed from mail servers regardless of the mail client settings.
- **Check archives.** This option instructs SpIDer Mail to scan archived files transferred via email. After enabling the option, the following parameters are available:
 - **Maximum file size to extract.** If an archive size exceeds the specified value, SpIDer Mail does not unpack and scan the archive. The default value is 30,720 KB;
 - **Maximum compression ratio.** If an archive compression ratio exceeds the specified value, SpIDer Mail does not unpack and check the archive. The default value is 0 KB;
 - **Maximum archive nesting level.** If a nesting level is greater than the specified value, SpIDer Mail proceeds unpacking and scanning the archive until this limit is exceeded. The default value is 64 KB.

3.2.9.1.2. Application Filter



Application filter of SpIDer Mail component can be configured on Dr.Web Server only. Corresponding settings are not provided on stations.



Application filter allows to configure manual interception of email traffic. In this mode, SpIDer Mail serves as a proxy server between mail clients and mail servers and intercepts only those connections that are explicitly defined in the settings. To use this mode, you also need to [configure](#) mail clients on stations.

The list of intercepted addresses includes records. Each record establishes a correspondence between settings of SpIDer Mail and a mail server.



By default, the interception list is empty. You can add the necessary records.

Configuring Mail Interception

1. Make a list of all mail servers whose connections you want to intercept and assign port numbers for these servers in arbitrary order. At this, use only unused non-system ports. The assigned numbers are called *SpIDer Mail ports*.



SpIDer Mail supports POP3, SMTP, IMAP4, and NNTP mail servers.

2. Select the **Anti-virus network** item in the main menu of the Control Center.
3. Click the name of the station or group in the hierarchical list of the opened window.
4. Click the **Configuration > Windows > SpIDer Guard and SpIDer Mail > SpIDer Mail** item in the opened control menu. Open the **Application** filter tab.
5. In the **SpIDer Mail connections settings** section, specify the following parameters:
 - **SpIDer Mail port**—SpIDer Mail port that you assigned for the mail server at step 1;
 - **Server**—the domain name or IP address of the mail server;
 - **Port**—the port number that the mail server uses.
6. If necessary, repeat the step 5 for other servers. To add one more mail server to the list, click .
7. To stop intercepting connections to a certain mail server, click  next to the item of the list that corresponds the server.
8. After you configure all the necessary settings, click **Save** to apply the changes on the station.
9. [Configure](#) the mail client at the station to support the manual interception mode by the SpIDer Mail component.

Configuring Mail Clients

If the SpIDer Mail is configured to manually intercept connections to mail servers, change the settings of a mail client on the station as following:

1. Set the address of the incoming and outgoing mail servers as `localhost`.
2. Set the mail server port to the *SpIDer Mail port* number that you assigned to the corresponding mail server.



Usually, you need to specify the following in the mail server settings:

```
localhost : <SpIDer_Mail_port>
```

where *<SpIDer_Mail_port>* is the number that you assigned to the mail server.

For example:



If you assigned the 7000 *SpIDer Mail port* to a mail server that uses the 110 port and the `pop.mail.ru` address, then specify the `localhost` as a server for the incoming mail and 7000 as a port in the mail client settings.

3.2.9.1.3. Anti-Spam

You can configure the following **Anti-Spam** options:

- **Check email for spam.** This option instructs to enable Anti-Spam.
- **Allow Cyrillic text.** This option instructs to prevent SpIDer Mail from marking emails in Cyrillic encoding as spam without prior analysis. If the option is disabled, such emails are most likely to be marked as spam by the filter. This option is enabled by default.
- **Allow Cyrillic text.** This option instructs to prevent SpIDer Mail from marking emails in Cyrillic encoding as spam without prior analysis. If the option is disabled, such emails are most likely to be marked as spam by the filter. This option is enabled by default.
- **Add a prefix to headers of spam messages.** This option instructs SpIDer Mail to add a special line specified in the **Prefix** field to the subjects of spam emails. This option is enabled by default. Using a prefix allows you to create filter rules for spam in those mail clients (for example, Microsoft Outlook Express) where it is not possible to enable filtering by headers.

The default prefix is **[SPAM]**.

- You can also configure white and black lists for email filtration.
 - You can specify only one object in one field. To add one more object to the list, click .
 - To remove the object from the list of exclusions, click .

3.2.9.1.4. Log

Enable the **Detailed logging** option to log such events as time of updates, starts and stops of SpIDer Mail, virus events, connection interception settings, names of scanned files, names of packers, and contents of scanned archives.

It is recommended that you use this mode when testing mail interception settings.



By default, size of a log file is restricted to 10 MB. If the log file size exceeds the limit, the content is reduced to:

- Specified size if the current session information does not exceed the limit.



- Size of the current session if the session information exceeds the limit.

If the **Detailed logging** option is enabled, operation of corresponding component is logged in the debug mode with maximal detailing. Limitations on the file size are disabled in this mode. This leads to significant increasing of the log file size. Also note, that the rotation of the log file is not performed (in all logging modes).

Debug logging mode decrease performance of Anti-virus and operating system of a station. It is recommended that you use this mode only when problems occur in component operation or on request of technical support service. It is not recommended to enable logging debug mode for extended period of time.



On the Control Center, the logging settings are specified separately for each component on the **Log** sections. On stations, logging settings are specified in the **Advanced** common section.

3.2.9.2. SpIDer Gate

3.2.9.2.1. Actions

On the **Actions** page, you can configure the main settings of station scanning by SpIDer Gate.



- **Scan mode.** Select the traffic scanning mode. The **Check incoming traffic** option is enabled by default.
- **Block malicious programs.** This setting group allows you to select malicious programs to be blocked. By default, SpIDer Gate blocks suspicious programs, adware, and dialers.
- **Block objects.** SpIDer Gate can block malformed or unchecked objects. This option is disabled by default.
- **Additional.** This setting group allows you to configure scan of archive and installation packages. By default, scanning of archives and installation packages is disabled.
- **Scan priority.** This setting allows you to adjust distribution of resources depending on traffic scanning priority. Internet connection speed decreases when SpIDer Gate operates with lower priority, since the monitor have to wait longer for downloading and scans larger portions of data. When you increase the priority, SpIDer Gate starts scanning data more often, thus increasing speed of your Internet connection. However, frequent scans also increase processor load.
- **Blocking parameters.** In this group, you can enable automatic blocking of URLs listed due to a notice from copyright owners and blocking of unreliable websites. Access to sites from the white list will be allowed regardless of other restrictions.



By default, SpIDer Gate blocks access to websites known as infection sources. At that, applications from the exclusion list are not blocked.

- **White list.** Configure a list of websites that can be accessed regardless of other restrictions.



1. To add a certain site to the white list, enter its name into the corresponding field.
2. You can specify only one site in one field. To add one more site to the list, click .
3. To remove the website from the white list, click  next to the list item that corresponds the website.

3.2.9.2.2. Application Filter

Enable the **Check traffic and URLs in IM clients** option to enable checking of links and data transmitted by instant messaging clients (Mail.RU Agent, ICQ, and Jabber clients). Only incoming traffic is checked. The option is enabled by default.

3.2.9.2.3. Log

Enable the **Detailed logging** option to log such events as the time of updates, starts and stops of SpIDer Gate, virus events, connection interception settings, names of scanned files, names of packers, and contents of scanned archives.

It is recommended that you use this mode for receiving more detailed information on the checked objects and operation of the web anti-virus.



By default, size of a log file is restricted to 10 MB. If the log file size exceeds the limit, the content is reduced to:

- Specified size if the current session information does not exceed the limit.
- Size of the current session if the session information exceeds the limit.

If the **Detailed logging** option is enabled, operation of corresponding component is logged in the debug mode with maximal detailing. Limitations on the file size are disabled in this mode. This leads to significant increasing of the log file size. Also note, that the rotation of the log file is not performed (in all logging modes).

Debug logging mode decrease performance of Anti-virus and operating system of a station. It is recommended that you use this mode only when problems occur in component operation or on request of technical support service. It is not recommended to enable logging debug mode for extended period of time.



On the Control Center, the logging settings are specified separately for each component on the **Log** sections. On stations, logging settings are specified in the **Advanced** common section.


3.2.9.3. Exclusions

In the **Excluded applications** list, you can specify the list of applications and processes that will not be scanned by SpIDer Mail and SpIDer Gate.





By default, the list is empty.

To configure list of exclusions

1. To add an application to the list, click .
2. Specify the path to the executable file of this application in the **Application path** field.
3. Specify additional options.

Option	Description
Regardless of whether the application has a digital signature	Select this option to exclude the application from scanning regardless of whether it has a valid digital signature or not.
If the application has a valid digital signature	Select this option to exclude the application from scanning only if it has a valid digital signature. Otherwise, the application will be scanned by the SpIDer Mail and SpIDer Gate components.
Any traffic	Select this option to exclude encrypted and non-encrypted application traffic from scanning.
Encrypted traffic	Select this option to exclude only encrypted application traffic from scanning.
On all IP addresses and ports	Select this option to exclude traffic on all IP addresses and ports from scanning.
On specific IP addresses and ports	Select this option to exclude specific IP addresses and ports from scanning. Traffic from other IP addresses and ports will be scanned (unless it is excluded by other settings).
To specify addresses and ports	To configure exclusion settings follow the guidance below: <ul style="list-style-type: none">• To exclude a specific domain corresponding to a particular port from scanning, enter site.com:80, for example.• To exclude scanning of traffic on a custom port (for example, 1111), enter *:1111.• To exclude scanning of traffic on any port, enter site:*

4. Click **Save**.
5. To remove an application from the exclusions list, click  next to the corresponding item.
6. To edit parameters of the existing application exclusion, select the corresponding item in the list and click .



Appendix A. Technical support

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

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

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

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

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

