Dr.WEB

Enterprise Security Suite

Managing stations under Windows

Dr.Web Enterprise Security Suite. Managing stations under Windows
Version 10.01.0
Administrator Manual
7/21/2020

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

1.1. About Manual

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

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

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

To get additional information, please refer the following manuals:

- **User Manual** of Dr.Web for Windows anti-virus solution contains the information about configuration of 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 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 web site of Doctor Web at https://download.drweb.com/doc/?lng=en

1.2. Conventions and Abbreviations

Conventions

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

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

Abbreviations

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

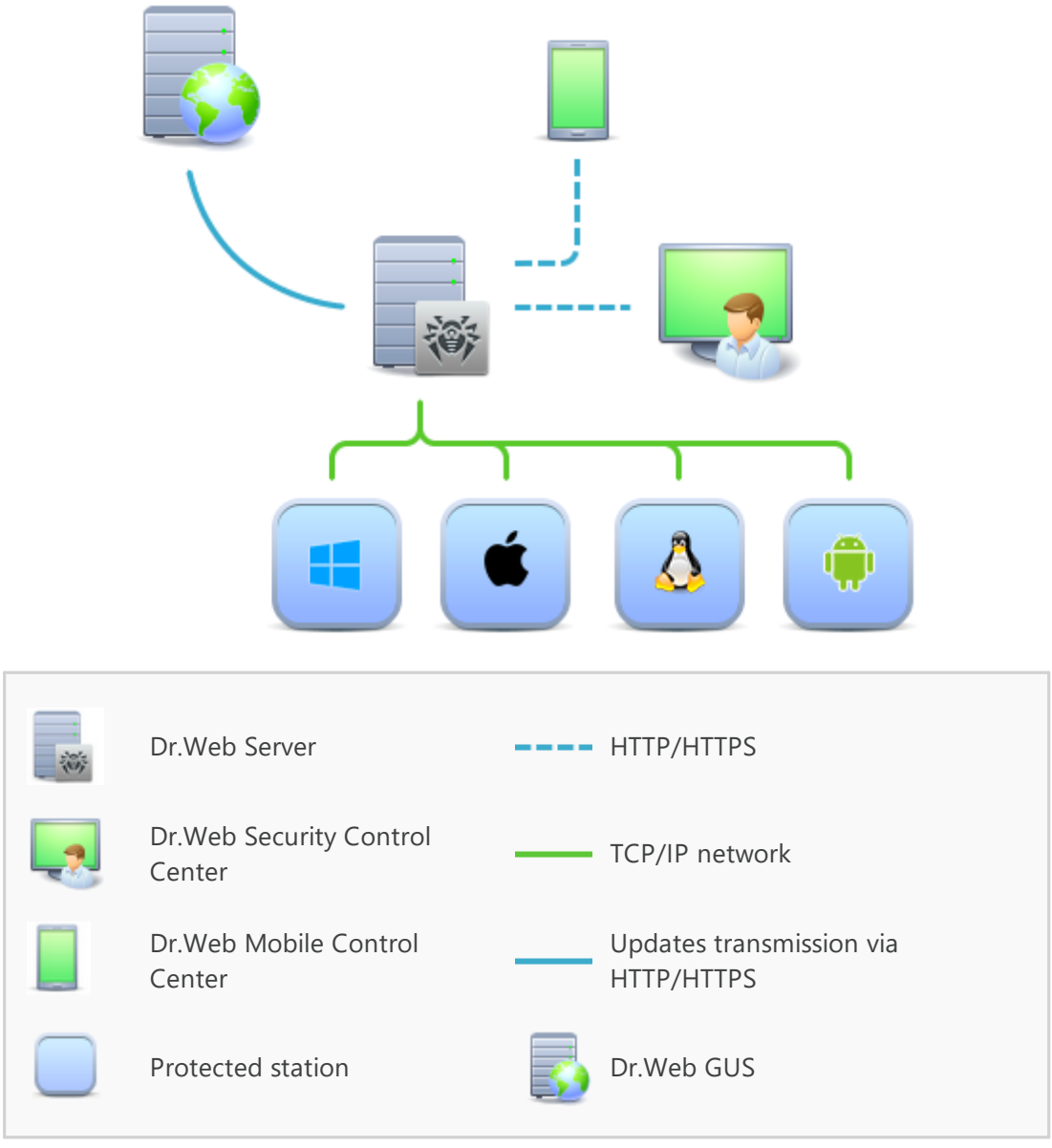
- DNS—Domain Name System,
- Dr.Web GUS—Dr.Web Global Update System,
- GUI—Graphical User Interface, a GUI version of a program—a version using a GUI,
- LAN—Local Area Network,
- NAP—Network Access Protection,
- OS—operating system.

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 either local company network including mobile devices, or home computers of employers.

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



The logical structure of the anti-virus network

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

2.2. Workstations Protection

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

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

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

Installation

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

1. Locally. Local installation is performed directly on a user's computer or mobile device. Installation may be implemented either by administrator or by user.
2. Remotely. Remote installation is 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.

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

Management

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

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

  At this, administrator can either deny or grant user's permissions to change Anti-virus settings on stations on one's own.
- Configure the schedule for anti-virus scans and other tasks to execute on a station.

- Get scan statistics and other information on anti-virus components operation and on stations state.
- Start and stop anti-virus scans and etc.

Update

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

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

The principle of stations operation in the Mobile mode is described in the **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 anti-virus scan of stations from the Control Center including rootkits check is supported.

Description of Dr.Web Agent Scanner settings and remote scan launch via the Control Center you can find in the **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 removable media.

SpIDer Mail

Checks all incoming and outgoing mail messages when using the mail clients.

The spam filter is is also available (if the license permits this function).

SpIDer Gate

Checks all calls to web sites via the HTTP protocol. Neutralizes malicious software in HTTP traffic (for example, in uploaded and downloaded files) and blocks the access to suspicious or incorrect resources.

Office Control

Controls access to network and local resources, in particular, limits access to web sites. 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 (settings are available on a station only)

Protects computers from external unauthorized access and prevents leak of vital data via Internet. Monitors connection attempts and data transfer via the Internet and blocks suspicious connections both on network and application levels.

Quarantine

Isolates malware and suspicious objects in the specific folder.

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

Self-protection

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

Preventive protection

Prevents of potential security threats. Controls the access to the operating system critical objects, controls drivers loading, programs autorun and system services operation and also monitors running processes and blocks them 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 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 primary group and set them as a personal—copy settings of this section from a primary group and set them for selected stations. Inheritance is not set and stations settings considered as a 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 **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 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 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 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 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 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 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 in this place the name must contain this particular character.
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.

You can also disable check 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 to 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 infected with unknown viruses. The option is enabled by default. If this option is disabled, only the signature analysis is used for scanning.
3. The **Scan for rootkits** option allows to perform background scanning of the operating system for complex threats and curing of cure active infections when necessary. During 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.

Advanced settings

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 apply 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 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 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 SpIDer Guard checks.

The **Exclude system files from the scan** option instructs to exclude from scanning system files, which are included in the internal list of 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 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 path.
   - To exclude all objects with a particular name, specify the name to 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 entry the field. 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 in this place the name must contain this particular character.
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 to use this mode to determine the most frequent objects scanned by SpIDer Guard. If necessary, you can add these objects to the list of exclusions in order to increase 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 to 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. SpIDer Mail

3.2.3.1. General

On the **General** tab, you can select actions to apply to threats detected by SpIDer 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 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 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 mail scanning parameters:

- **Use heuristic analysis**. In this mode, special methods are used to detect suspicious objects in emails that are most likely infected with unknown viruses. Disable this option to not use the heuristic analysys.
- **Scan 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 scanning 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 check of the email. Default 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. The 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.
- **Scan 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 check the archive. 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. 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. Default value is 64 KB.

3.2.3.2. 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 mail traffic. In this mode, SpIDer Mail serves as a proxy between mail clients and mail servers and intercepts only those connections that are explicitly defined in the settings. To use this mode, you need also to configure mail clients on stations.

The list of intercepted addresses includes records each one of which establishes a correspondence between settings of SpIDer Mail and a mail server.

By default, the interception list is empty. You can add 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 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 to this server.
8. In the **Excluded applications** list, you can specify the list of applications whose mail traffic will not be intercepted and checked by SpIDer Mail:
   a) To exclude the application from the check, specify the path to the executable file of this application.
   b) Only one excluded application is specified in each field. To add one more element to the list, click  .
   c) To remove an application from the exclusions list, click  next to the item of the list that corresponds to this application.
9. After you configure all necessary settings, click **Save** to apply the changes on the station.

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

10. 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 configured to manual intercept connections with mail servers, change the settings of a mail client on the station as the following:

1. Set the addresses 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 set mail client to connect to `localhost` via the `7000` port.

3.2.3.3. Antispam

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 Asian text**. This option instructs to prevent SpIDer Mail from marking emails on most common Asian languages 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** 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  .

3.2.3.4. 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 to 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 to 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.

3.2.4. SpIDer Gate

3.2.4.1. 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 not checked 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 access to which must be allowed 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.

3.2.4.2. 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. By default, this option is enabled.
- In the **Excluded applications** list, you can add applications traffic of which will not be intercepted and scanned by SpIDer Gate:
  1. To exclude an application from scanning, specify its path to the application executable file.
  2. You can specify only one excluded application in one field. To add one more unit to the list, click  .
  3. To remove an application from the list of exclusions, click  next to the list item that corresponds the application.

3.2.4.3. Log

Enable the **Detailed logging** option to log such events as 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 to use this mode for reception of more detailed information on the checked objects and work 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 to 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. Office Control

3.2.5.1. 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.
- Enable the **Block sending tasks to a printer** option to block sending print tasks to printers.
- Enable the **Block access to data on removable media** option to block access to data on USB flash, floppy, CD/DVD, ZIP drives, etc.
- Enable the **Protected folders and files** option to block access to all resources listed below.

  To configure list of protected files and folders

  1. To add an object, enter the path in the corresponding field.
  2. Select limitation mode:
     - **Read-only**—an added object will become read only.
     - **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 **Protected folders and files** option.

- Enable the **Control access to the following objects** option to block access to predefined resources added to the **Protected objects list**. To block the access to an object, set the **Block** option next to the correspondent object type in the given list..

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

- **Block data transfer over network**
- **Control access to the following objects > Protected objects list > Network adapters**

These options block all network interaction for stations. You cannot also use Control Center to change settings remotely.

3.2.5.2. Web filtering

On the **General** page, you can configure access to Internet resources:

- 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 websites to the manually populated black and while lists 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 those in the white list.

In any mode except the **No restrictions** mode, 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.
   - To add a certain website, enter its full address (for example, `www.example.com`). Access to all webpages located on this website will be defined by this record.
   - To configure access to websites with similar names, enter the common part of their domain names. For example, if you enter `example`, then the access to `example.com`, `example.test.com`, `test.com/example`, `test.example222.ru`, and other similar websites will be defined by this record.

- To allow access to websites within a particular domain, enter the domain name with a period (`.`) character. This record defines access to all resources 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 configure within this domain. For example, if you enter `example.com/test`, the access to such webpages as `example.com/test11`, `template.example.com/test22`, and so on will be handled.

Your input may be unified.

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 websites, repeat steps 1 to 2.

3.2.5.3. Time limits

On the **Time limits** page, you can set restrictions on time spent on the Internet or working on the computer.

By default, no time limits on computer and Internet use are set. You can set time limits for users via a table with timeslots.

To set time limits using the table

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

- Green—**No restrictions**
- Blue—**Block Internet access**
- Red—**Block all**: to block access to the computer 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 cells changes cyclically according to the color scheme below the table.

- To change the mode of the whole table row (of one day), click on the marker of the corresponding color from the right of the necessary row.
- To change the mode of the whole table column (of one 30-minute time interval for all weekdays), click on the marker of the corresponding color below the necessary column.

3.2.6. Dr.Web Agent

3.2.6.1. 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 start of the OS and execution of the startup scan task, if it was scheduled for the Agent. The 1 minute delay is by default. Set the 0 value to perform the scan task without any delay, i.e. immediately after the start of 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 **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 from station by Agent 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 time synchronization with Dr.Web Server (is set by the **Synchronize time** flag).
- Set the **Block user activity emulation** flag to prevent any changes in Dr.Web operation, except those made manually by user. This option allows to prevent any automatic changes in 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 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 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

3.2.6.2. Network

On the **Network** tab, you can specify parameters determining interaction with the Server:

- In the **Public key** field specify the public encryption key of Dr.Web Server (`drwcsd.pub`) which is stored on the station. To select the key file, click  .

  Several public keys can be stored on the station at the same time, e.g., during the process of encryption keys replacement or during moving from one Server to another. Note that keys must be unique, i.e. you cannot specify two similar public keys.

  To add one more public key, click  and select the key file.

  To remove existing key from the station, click  .

  If the **Allow operating without public key** flag is cleared, you cannot remove the last public key.

- Set the **Allow operating without public key** flag to allow connecting Agents if they do not have public encryption key (`drwcsd.pub`) or the file has incorrect structure.
- Set the **Allow operating with invalid public key** flag to allow connecting Agents if they have incorrect public encryption key (`drwcsd.pub`).
- In the **Server** field, you can specify the address of Dr.Web Server. You may leave this field blank. Then the Agent will use the address of Dr.Web Server that is set on the user's local computer (the address of the Server from which the installation has been performed).

  Either one Server address or several different Servers addresses can be set. To add one more Server address, click  and specify an address in the added field. Format of Server network addresses is described in the **Appendices** document, in the **Appendix E. The Specification of Network Addresses** section.

  Server address example:

  tcp/10.4.0.18:2193

  tcp/10.4.0.19

  10.4.0.20

  If the **Server** parameter value is set incorrectly/invalid, the Agents will disconnect from the Server and will not be able to reconnect. In this case you will have to set the Server address on the stations directly.

- In the **Search retries number** field, set the parameter determining the number of attempts to find Dr.Web Server via the connection using the *Mulicasting* mode.

- In the **Search timeout (sec.)** field, set the interval between attempts to find Dr.Web Server in seconds via the connection using the *Mulicasting* mode.
- The **Compression mode** and **Encryption mode** fields determine the compression and encryption settings of network traffic correspondingly.
- In the **Network listening parameters** field, specify the UDP port for Dr.Web Security Control Center to search for working Dr.Web Agents in a network. To disable ports listening, enter **NONE**.

  This parameter should be specified in the network addresses format described in the **Appendixes** document, in the **Appendix E. The Specification of Network Addresses** section.

  By default, the **udp/:2193** is used, which means "all interfaces, port `2193`".

3.2.6.3. Mobility

On the **Mobility** tab, you can specify parameters of Mobile Mode of the Agent:

- In the **Update period** field, specify the time interval between anti-virus software updates.

  In the **Manual** mode, automatic updates become disabled. In this case, to receive the latest virus databases, 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 user's computer has no connection to Dr.Web Server for a long time, to receive updates opportunely from the Dr.Web GUS, it is recommended to 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 unsuccessful, 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 mobile mode configuration at the Agent side is given in the **User Manual**.

3.2.6.4. Log

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

- The **Agent log verbosity level** parameter determines the level of detail of Agent logging.
- The **Engine log verbosity level** parameter determines the level of detail of Scanning Engine logging.
- The **Update log verbosity level** parameter determines the level of detail of Dr.Web updating module logging.
- Set the **Create memory dumps at scan errors**, to create memory dumps in cases of scan errors occur. It is recommended to enable this setting for Dr.Web operation errors analysis.

3.2.6.5. 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 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 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 requiring reboot is displayed in the **State** table. Administrator is able to reboot a station from the Control Center if it is needed.

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 rights.
- **Threats 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 a 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 administrator from the Control Center;
- USB device (keyboard) connected/blocked within protection from BadUSB vulnerable.

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 separate desktop, i.e. on top of running full-screen application. It is recommended to enable this option to avoid blocking of network connections which are used by this full screen mode application without possibility to enable them in the time of Dr.Web Firewall request receipt.

3.2.7. Dr.Web for Microsoft Outlook

3.2.7.1. General

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

3.2.7.2. Actions

On the **Actions** tab, you can select actions to apply 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.

3.2.7.3. 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, and 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 to 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.

3.2.7.4. Antispam

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 emails filtration.
  a) Specify an address in the corresponding field. Rules to specify 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.

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 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 ensure delivery of messages sent from email address with a certain user name from any domain, use an asterisk (*) instead of the domain name in the address. For example, if you want to receive messages from all senders with the `john` mailbox name, enter `john@*`.

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 `mail.com` domain will not be processed with the anti-spam filter.

3.2.8. Preventive Protection

On the **Preventive Protection** tab, you can configure Dr.Web reaction to such actions of other programs that can compromise workstation security and 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 apply to all other processes.

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 being 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 blocked automatically.
Interactive 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

On 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 (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 the one of the following position:

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

  If you change table settings when one of 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 SpIDer 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 SpIDer Guard component are not monitored. To protect your data from unauthorized modifications, it is recommended to 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

Parameter	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, AppInit_DLLs, LoadAppInit_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)
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

Parameter	Registry branch
Session Manager parameters	System\ControlSetXXX\Control\Session Manager\SubSystems, Windows
System services	System\CurrentControlXXX\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  next 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.

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.