



**Dr.WEB®**

**Agent**

## **User Manual**

Defend what you create

**© 2007-2009 Doctor Web. All rights reserved**

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, the Dr.WEB logo, SpIDer Mail, SpIDer Guard, CureIt!, the Dr.WEB INSIDE 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 Agent**

**Version 5.0**

**User Manual**

**23.04.2009**

Doctor Web Head Office  
2-12A, 3rd str. Yamskogo polya  
Moscow, Russia  
125124

Web site: [www.drweb.com](http://www.drweb.com)  
Phone: +7 (495) 789-45-87

Refer to the official web site 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

<b>Chapter 1: Welcome to Dr.Web® Enterprise Suite</b>	<b>6</b>
<b>1.1. Conventions and Abbreviations</b>	<b>6</b>
<b>1.2. Dr.Web Enterprise Suite Anti-Virus</b>	<b>7</b>
<b>Chapter 2. Dr.Web Agent Component</b>	<b>9</b>
<b>2.1. Main Functions and Parameters of the Dr.Web Agent</b>	<b>9</b>
<b>2.2. System Requirements</b>	<b>10</b>
<b>2.3. Installing and Removing the ES-Agent</b>	<b>10</b>
<b>2.4. Dr.Web Agent Interface Start and Shutdown</b>	<b>12</b>
<b>2.5. Dr.Web Agent Administration</b>	<b>13</b>
<b>Chapter 3. Dr.Web Agent Functionality</b>	<b>19</b>
<b>3.1. Dr.Web Agent Settings</b>	<b>19</b>
3.1.1. Server Connection Settings	<b>20</b>
3.1.2. Log Level of Detail	<b>22</b>
<b>3.2. Updating of the Anti-Virus Software</b>	<b>23</b>
<b>3.3. Agent and Server Interaction Mode</b>	<b>23</b>
<b>3.4. Schedule Setting</b>	<b>24</b>
3.4.1. Local Schedule. The List of Local Jobs	<b>24</b>
3.4.2. Centralized Schedule	<b>35</b>
<b>3.5. Setting the Interface Language</b>	<b>35</b>
<b>3.6. Mobile Mode Settings</b>	<b>35</b>
<b>3.7. Viewing the Statistics</b>	<b>37</b>
<b>3.8. Viewing the Anti-Virus Software Status</b>	<b>38</b>



<b>3.9. Starting the Anti-Virus Scanner</b>	<b>40</b>
<b>3.10. File Monitor Settings</b>	<b>40</b>
<b>3.11. E-Mail Monitor Settings</b>	<b>41</b>
<b>3.12. HTTP Monitor Settings</b>	<b>42</b>
<b>3.13. Office Control Settings</b>	<b>43</b>
3.13.1. URL Filter	<b>45</b>
3.13.2. Local Access	<b>49</b>
<b>3.14. Informational Messages</b>	<b>51</b>
<b>Appendix A. Scanner's Command-Line Switches</b>	<b>55</b>
<b>Appendix B. Installers's Command-Line Switched</b>	<b>61</b>
<b>Index</b>	<b>63</b>





# Chapter 1: Welcome to Dr.Web® Enterprise Suite

## 1.1. Conventions and Abbreviations

The [following](#) conventions are used in the Manual.

**Table 1. Conventions**

Symbol	Comment
 Note, that	Marks important notes or instructions.
 Warning	Warns about possible errors.
<b>Dr.Web Enterprise Suite</b>	Names of <b>Dr.Web</b> products and components.
Anti-virus network	A term in the position of a definition or a link to a definition.
<IP-address>	Placeholders.
<b>Cancel</b>	Names of buttons, windows, menu items and other program interface elements.
CTRL	Keyboard keys names.
C: \Windows\	Names of files and folders, code examples, input to the command line and application output.
<a href="#">Appendix A</a>	Cross-references or Internal Hyperlinks to web pages.

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

- ◆ **Dr.Web GUS** — **Dr.Web Global Update System**,
- ◆ FDD — Floppy Disk Drive - portable magnetic data carrier;



- ◆ GUI — Graphical User Interface, a GUI version of a program — a version using a GUI,
- ◆ LAN — Local area network;
- ◆ OS — operating system,
- ◆ PC — personal computer,
- ◆ URL — Uniform Resource Locator - compact string of characters used to identify or name a resource on the Internet.

## 1.2. Dr.Web Enterprise Suite Anti-Virus

**Dr.Web Enterprise Suite** is designed to organize and control integrated, complex and reliable anti-virus protection of computers of a company.

Protected computers are united in an anti-virus network, which is managed by the administrator through the anti-virus **Server**. The anti-virus protection of company's employees computers is automated and administered centrally, which provides for a reliable safety level, while user interference is minimal.

### **Dr.Web Enterprise Suite provides for**

- ◆ centralized (without user intervention) installation of the anti-virus packages on computers,
- ◆
- ◆ centralized setup of anti-virus packages on protected computers,
- ◆ centralized virus databases and program files updates on protected computers,
- ◆ monitoring of virus events and the state of anti-virus packages and OS's on all protected computers.

Anti-virus **Dr.Web Agents** are installed on protected computers. These programs provide for computer protection and connection with the anti-virus **Server**, through which anti-virus programs and their components are updated and set up in general.

The settings users can change are described in Section [Dr.Web Agent Administration](#).



Do not install other anti-virus programs, including other **Dr. Web** programs, on computers with an installed anti-virus **Agent**.

---





## Chapter 2. Dr.Web Agent Component

### 2.1. Main Functions and Parameters of the Dr.Web Agent

Computers are protected from virus threats and spam by means of programs included in the anti-virus package of **Dr.Web Enterprise Suite**.

The **Dr.Web** Agent facilitates administration of computer protection and connection to the anti-virus **Server**.

**The anti-virus Dr.Web Agent serves the following functions:**

- ◆ installs, updates and sets up the anti-virus package, starts scannings, and performs other tasks given by the anti-virus **Server**;
- ◆ allows to call for execution the **Dr.Web** anti-virus package files through a special interface;
- ◆ sends the results of tasks execution to the anti-virus **Server**;
- ◆ sends notifications of predefined events in the operation of the anti-virus package to the anti-virus **Server**.

**Users can implement the following actions through the Dr.Web Agent:**

- ◆ schedule checkups (scanning) of the computer for viruses;
- ◆ start scanning the computer if necessary;
- ◆ change the settings of certain components of the **Dr.Web** software complex including some settings of the **Agent**;
- ◆ view the statistics of virus events on the computer and other information about the **Dr.Web** program.



A user may change the settings of the **Agent** and the components provided he has corresponding permissions to such actions. A more detailed information is given in the descriptions of the settings of concrete components.

## 2.2. System Requirements

### The anti-virus Dr.Web Agent and the package require

- ◆ Intel® Pentium® II 400 MHz or faster;
- ◆ RAM not less than 32 MB;
- ◆ not less than 108 MB of available disk space (8 MB for executable files, the rest - for logs);
- ◆ Windows 98 SE OS, Windows Me OS , Windows NT4 (with SP6) OS or later
  - Notes: **SpIDer Guard** operates in 32bit systems only.
  - **SpIDerGate** and **Self-Protections** operates under Windows 2000 (SP4) OS or later.



No other anti-virus software (including other versions of **Dr. Web** anti-virus programs) should be installed on the workstations of an anti-virus network managed by **Dr.Web ES-**.

## 2.3. Installing and Removing the ES-Agent

You can have the **Dr.Web Agent** and the anti-virus package installed and removed in two ways:



1. Remotely – on the **Server** through the network. Performed by the anti-virus network administrator. No user interference required (see a detailed description of the creation procedure of an anti-virus station and remote installation of the anti-virus software in Administrator Manual **Dr. Web Enterprise Suite Anti-Virus**).



Remote installation of anti-virus **Agents** is possible only on workstations under Windows NT, Windows 2000, Windows XP Professional, Windows 2003, Windows Vista operating systems.

To perform remote installation, you should have administrator's rights on the workstations.

---

2. Locally – directly on the user's machine. May be performed both by the administrator or the user. See the description of local installation and removal of the anti-virus software below.

## Installing the Anti-Virus Software

### To install the anti-virus software (Dr.Web Agent and anti-virus package)

1. From the workstation, on which you want to install the anti-virus software, enter the network catalog of **Agent's** installation located at the **Server**. By default, it is Installer (see a detailed description of the creation procedure of an anti-virus station and remote installation of the anti-virus software in Administrator Manual **Dr. Web Enterprise Suite Anti-Virus**, Section **Installing the Anti-Virus Agent on Computers**).
2. Run the `drwinst.exe` file. The `drwinst` command may be used with switches (see [Appendix B. Installers's Command-Line Switched](#)).



It is recommended to run the `drwinst` command in the command line specifying the name or the IP address of the anti-virus **Server** in the format:

```
drwinst.exe <Server_IP/name>
```



This will reduce the time of **Agent**'s installation as there will be no need to search for an anti-virus **Server**, and will eliminate possible errors if there is more than 1 anti-virus **Server** in the network.

---

3. After the station has been approved at the **Server** (if it is required by anti-virus **Server** settings), the anti-virus package will be automatically installed.
4. Restart the computer on **Agent**'s request.


## Removing the Anti-Virus Software

You can remove the station's anti-virus software (**Dr.Web Agent** and anti-virus package) by means of standard Windows OS services.

On the Windows **Start** menu, select **Settings** → **Control Panel** → **Add or Remove Programs**. In the opened list, select **Dr.Web Agent** and click the **Remove** button (or **Remove/Change** depending on the version of Windows OS). The station's anti-virus software will be removed.

## 2.4. Dr.Web Agent Interface Start and Shutdown

The **Agent** is started automatically after the installation and at every Windows OS load.

The anti-virus **Dr.Web Agent** launched under Windows OS displays an icon  in the Taskbar notification area (An element of the Microsoft Windows Desktop that displays the icons of active applications and is located in the right part of the taskbar, which by default is positioned in the bottom of the desktop).




The **Exit** command of the [context menu](#) of the **Agent** just removes the icon from the notification area of the **Taskbar**. The Agent continues its operation.

---



The **Agent's** icon is automatically shown in the notification area of the **Taskbar** when the **Agent** is launched after Windows OS start. To display the icon (if it was removed by the **Exit** command) without restarting the computer, you can start the **Agent's** interface by means of the **Start AgentUI** command on the Windows **Start** menu → **Programs** → **Dr.Web Enterprise Suite**.

## 2.5. Dr.Web Agent Administration

The anti-virus **Dr.Web Agent** launched under Windows OS displays an icon  in the notification area of the **Taskbar**.

The functions of the **Dr.Web Agent** available for editing and viewing are called from the context menu of the **Dr.Web Agent's** icon. Right-click the icon and select the necessary command.

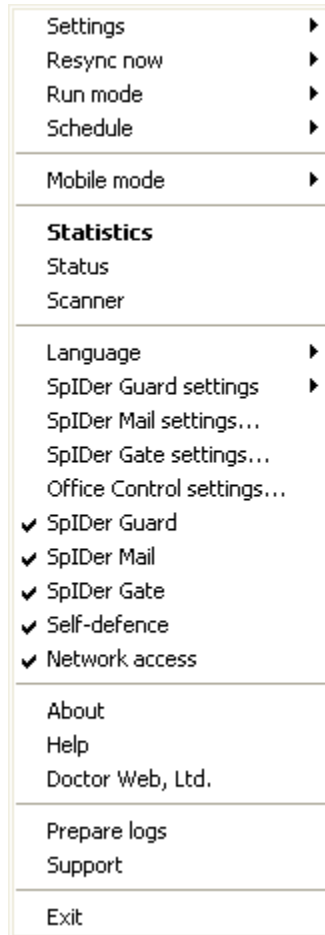


Figure 2-1. Dr.Web Agent context menu

**The context menu includes**

- ◆ **Exit** - remove the **Dr.Web Agent's** icon from the notification area of the **Taskbar** (see p. [Dr.Web Agent Interface Start and Shutdown](#)).
- ◆ **Support** - go to the web page of **Dr.Web Technical Support**



service to receive subscriber's technical support.

- ◆ **Prepare logs** - archive (zip) log files and files with system data to send to the technical support.
- ◆ **Doctor Web, Ltd** - go to the site of **Dr.Web** Company.
- ◆ **Help** - open **Dr.Web Agent's** help.
- ◆ **About** - view information about the program and its version. From the information window you can go to the web site of **Dr. Web** Company or to the web page of **Dr.Web Technical Support** service.
- ◆ **Network access** - when the item is selected, it is allowed to access the LAN and the Internet, otherwise the access is blocked.
- ◆ **Self-defence** - enable/disable the **System Monitor**.

This component protects **Dr.Web** files and catalogs from unpermitted or unintentional interference, for example deletion or modification by viruses. When the **System Monitor** is enabled, only **Dr.Web** programs may access the indicated resources.

- ◆ **SpIDer Gate** - enable/disable the **File Monitor SpIDer Gate**.

By configuring **SpIDer Gate** you can turn on or turn off monitoring of incoming and outgoing traffic and list applications which traffic you want or do not want to monitor.

- ◆ **SpIDer Mail** - enable/disable the **File Monitor SpIDer Mail**.

**SpIDer Mail** is an e-mail monitor. With default settings, **SpIDer Mail** automatically intercepts all calls of any mail programs on your computer to mail servers.

- ◆ **SpIDer Guard** - enable/disable the **File Monitor SpIDer Guard**.

**SpIDer Guard** constantly resides in the main memory checking all opened files on-access and monitors running processes for virus-like activity.

To learn more about this component's functions and dialog boxes, open the application and press F1.

Detailed information about other menu items is given in Chapter 3 of



this Manual. To open the necessary section, click the respective item of the context menu on [figure 2-1](#).



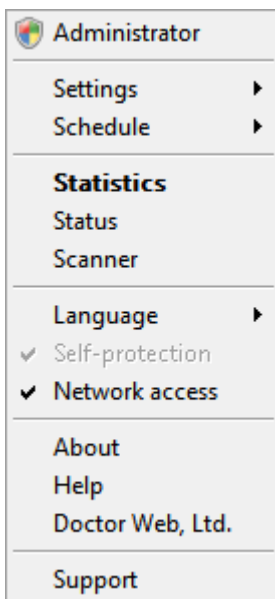
The number of settings available on the context menu of the **Dr.Web Agent**'s icon can vary subject to the configuration of the workstation set by the means of the anti-virus network. The anti-virus network administrator can limit user's rights to administer and set up the anti-virus tools installed on his computer.

If some items of the context menu are not available, it may be for the following two reasons:

- 1) the permissions to change these settings are disabled at the **Server** by the anti-virus network administrator;
  - 2) the user has no administrator rights on this computer.
- 

The context menu of an **Agent** started without administrator rights under Windows Vista OS includes an additional item **Administrator** (see [figure 2-2](#)). This menu item enables the user to start the **Agent** under administrator rights and fully access to the functionality of the **Agent**, namely all menu items approved at the anti-virus **Server** will become available.





**Figure 2-2. Context menu of the Dr.Web Agent under a Windows Vista OS user**



---

In all dialog boxes of the **Dr.Web Agent**, to receive help, press F1. To learn about the function of any element of the windows, right-click it.







---

The **Dr.Web Agent's** icon can have different aspects depending on whether the workstation is connected to the **Server** and other parameters.



Possible variants and the components statuses corresponding to them are given in [Table 2](#).

**Table 2. Possible aspects of the icon and components statuses corresponding to them**

Icon	Description	Action
	The black picture on the green background.	The <b>Agent</b> is operating normally and is connected to the <b>Server</b> .
	A crossed Server icon on the basic background.	The <b>Server</b> is unavailable.
	An exclamation mark in a yellow triangle over the icon.	The <b>Agent</b> requests to restart the computer.
	The background of the icon changes color from green to red.	An error occurred during updating of the package components.
	The background of the icon is constantly red.	The <b>Agent</b> is stopped or not running.
	The background of the icon is yellow.	The <b>Agent</b> is working in the <a href="#">mobile mode</a> .



# Chapter 3. Dr.Web Agent Functionality

## 3.1. Dr.Web Agent Settings

To access **Dr.Web Agent's** settings, on the [context menu](#) of the **Agent** click **Settings**.

In the drop-down list of the **Settings** menu you can mark the type of notifications about virus events on your PC that you want to receive:

- ◆ **Major messages** - receive only important messages. Such notifications include messages about
  - starting errors of some of the anti-virus software components;
  - updating errors of the anti-virus software or some of the components;
  - the necessity to restart the computer.
- ◆ **Minor messages** - receive only minor messages. Such notifications include messages about
  - the beginning of updating of the anti-virus software or some of the components;
  - the end of updating of the anti-virus software or some of the components.
- ◆ **Virus messages** - receive only messages about viruses. This type of notification includes messages about virus(es) detection by one of the anti-virus software components.

To do this, select the checkbox near the respective menu item (click the item).

If you want to receive all groups of messages, select all three checkboxes. Otherwise only messages of selected groups will be shown (see also p. [Informational Messages](#)).



To enable system time synchronization with the **Server**, select the **Synchronize time** checkbox. In this mode, the **Agent** adjusts the system time on your computer in correspondence with the time on the **Server**.

To view or change **Server** connection settings, select **Connection...** (see p. [Server Connection Settings](#)).

To view or change the parameters of logging of virus events on your computer, select **Log level** (see p. [Log Level of Detail](#)).



The **Connection** and **Log level** options are available on the **Settings** menu only provided the user has

- 1) the permissions to change these settings. The permissions are set at the **Server** by the anti-virus network administrator.
  - 2) administrator rights on the computer.
- 

### 3.1.1. Server Connection Settings

To view and edit the settings of connection with the anti-virus **Server**, on the [context menu](#) click **Settings** → **Connection...**



The **Connection** option is available on the **Settings** menu only if the user is granted with the permissions to change the settings. The permissions are set at the **Server** by the anti-virus network administrator.

---

In the dialog box for setting a connection with a **Dr.Web** anti-virus **Server** you can change the parameters of connection to the current Server or set up a connection with a new anti-virus Server.



Settings - Dr.Web Antivirus

Server:

ID:

Password:

Password, again:

**Figure 3-1. Server Connection Settings**



Anti-virus **Server** connection settings should be altered only upon coordination with the anti-virus network administrator, or your computer will be disconnected from the network.

If necessary, change the parameters:

- ◆ **Server** - anti-virus **Server** name or IP address,
- ◆ **ID** - identifier assigned to your computer for registration at the **Server**,
- ◆ **Password** - **Agent** password to connect to the **Server**.

To close the window and save the changes, click **OK**.

To close the window and skip the changes, click **Cancel**.

To reset all **Server** connection settings, click **Newbie**. The **Agent** will be disconnected from the **Server** and the anti-virus package on your computer will not be able to provide ultimate safety. To set up a connection to the **Server** again, you will have to enter new **Server** registration data in this dialog box. After the registration has been confirmed by the anti-virus network administrator, your computer will be reconnected to the anti-virus **Server**.



In all dialog boxes of the **Dr.Web Agent**, to receive help about the active window, press F1. To learn about the function of any element of the window, right-click it.

### 3.1.2. Log Level of Detail

To change the level of detail of events logging on your computer, on the [context menu](#) click **Settings** → **Log level**.



The **Log level** option is available on the **Settings** menu only provided the user has

- 1) the permissions to change these settings. The permissions are set at the **Server** by the anti-virus network administrator.
- 2) administrator rights on the computer.

Select the necessary value (**Debug3** - logging in maximum detail, **Critical error** - logging in minimum detail, only critical errors are registered):

- ◆ **Debug, Debug 1, Debug 2, Debug 3** — instruct to log debugging events. The options are displayed in the ascending order according to the level of detail. **Debug** instructs to log in the minimum level of detail; **Debug 3** instructs to log in the maximum level of detail.
- ◆ **Trace, Trace 1, Trace 2, Trace 3** — enable tracing events. The options are displayed in the ascending order according to the level of detail. **Trace** instructs to log in the minimum level of detail; **Trace 3** instructs to log in the maximum level of detail.
- ◆ **Info** — display information messages,
- ◆ **Notice** — display important information messages,
- ◆ **Warning** — warn about errors,
- ◆ **Error** — notify of operation errors,
- ◆ **Critical error** — instructs to inform only of the most severe errors,



## 3.2. Updating of the Anti-Virus Software

**Dr.Web** software updates are loaded and installed automatically as they become available. Still in critical situations you can manually update the software components (upon prior consultation with the administrator).

To update the anti-virus software installed on your computer, click **Resync now** on the [context menu](#).

- ◆ When the icon background turns from green to red, you must force synchronization of the components that failed to update. For this, select **Resync now** → **Only failed components** in the [Agent context menu](#).
- ◆ When it is necessary to update all installed components of the anti-virus (e.g., when the **Agent** has not been connected to the **Server** for a long time, etc.), on the [context menu](#) select **Resync now** → **All components**.

## 3.3. Agent and Server Interaction Mode

To view and edit the parameters of **Agent**'s interaction with the **Server**, select **Run mode** on the **Agent**'s [context menu](#).



---

The **Run mode** option is available on context menu only provided the user has

- 1) the permissions to change these settings. The permissions are set at the **Server** by the anti-virus network administrator.
  - 2) administrator rights on the computer.
- 

The following items are available on the **Mode** drop-down list:

- ◆ **Connect to Dr.Web Enterprise Server** - use this option to send statistics to the Administrator and receive **Server** instructions and **Dr.Web** updates.



- ◆ **Accept Jobs** - use this option to accept virus check jobs from the Administrator of your Antivirus network.
- ◆ **Accept Updates** - use this option to receive regular updates of anti-virus components and virus databases.
- ◆ **Accumulate Events** - use this option to collect information about virus events on your computer.

## 3.4. Schedule Setting

Against the permissions at the **Server**, you may edit and view the schedule of the anti-virus Scanner:

- ◆ set and edit [the local checks schedule](#);
- ◆ view [the centralized checks schedule](#).

To do this, select the respective item on the drop-down menu of the **Schedule** command of the **Agent's context menu**.

### 3.4.1. Local Schedule. The List of Local Jobs

Against the permissions at the **Server**, you may create your own schedule, to which you may add certain types of jobs to check the computer.



---

The **Local** item is available on the **Schedule** menu only provided the user has

- 1) the permissions to change these settings. The permissions are set at the **Server** by the anti-virus network administrator.
  - 2) administrator rights on the computer.
- 

By clicking **Schedule** → **Local** on the [context menu](#) you can view your own schedule.

If you want to schedule a task to scan your computer, click **Add** and select the type of job in the opened window:





- ◆ [Hourly](#)
- ◆ [Daily](#)
- ◆ [Weekly](#)
- ◆ [Monthly](#)
- ◆ [Every N minutes](#)
- ◆ [Startup](#)
- ◆ [Shutdown](#)

If you need to edit an assigned job, select it in the list and click **Edit**.

To remove a job, select it in the list and click **Remove**.

You can start scanning immediately by selecting the **Scanner** command on [the context menu of the Dr.Web Agent's icon](#) or on the Windows **Start** menu → **Programs**.

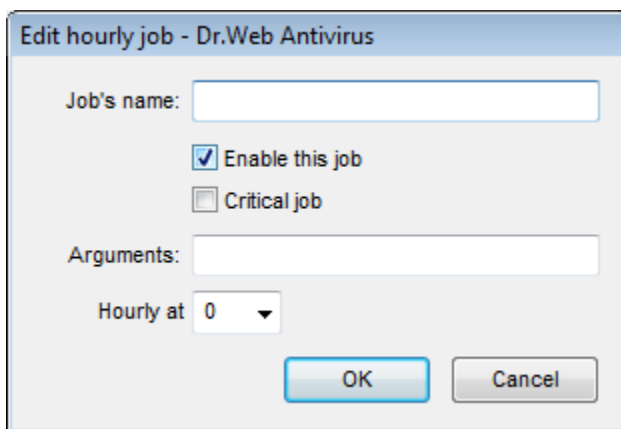


In all dialog boxes of the **Dr.Web Agent**, to receive help about the active window, press F1. To learn about the function of any element of the window, right-click it.

---

### 3.4.1.1. Hourly Job

This job type is performed every hour on the specified minute of the hour.



**Figure 3-2. Hourly job dialog box**

In the dialog box of an hourly job (see [Figure 3-2](#)) you can set the following parameters:

- ◆ **Job's name** - type a name of the task.
- ◆ To enable the job, select the checkbox **Enable this job**.  
To disable the job, clear the checkbox. The job will remain on the list but will not be executed.
- ◆ A selected checkbox **Critical job** instructs to perform the job at next **Dr.Web Agent** launch, if execution of this job is omitted (the **Dr.Web Agent** is switched off at the due time). If a task is omitted several times within a certain period of time, then it will be performed only once after the **Dr.Web Agent** has been launched.
- ◆ **Arguments** - specify, when necessary, additional job launch parameters. Use the command-line parameters specified in p. [Scanner's Command-Line Switches](#).
- ◆ **Hourly at** - specify the minute when the job should be performed.

To close the window and save the parameters of the task, click **OK**.

To close the window without saving the changes/new task, click



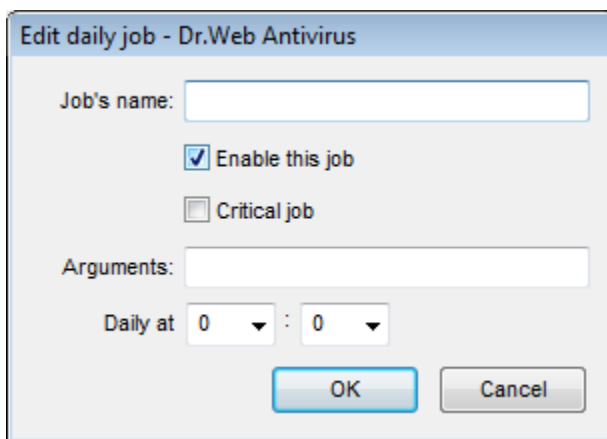
Cancel.



In all dialog boxes of the **Dr.Web Agent**, to receive help about the active window, press F1. To learn about the function of any element of the window, right-click it.

### 3.4.1.2. Daily Job

This job type is performed every day at the specified time.



**Figure 3-3. Daily job dialog box**

In the dialog box of a daily job (see [Figure 3-3](#)) you can set the following parameters:

- ◆ **Job's name** - type a name of the task.
- ◆ To enable the job, select the checkbox **Enable this job**.  
To disable the job, clear the checkbox. The job will remain on the list but will not be executed.
- ◆ A selected checkbox **Critical job** instructs to perform the job at next **Dr.Web Agent** launch, if execution of this job is omitted (the **Dr.Web Agent** is switched off at the due time). If a task is



omitted several times within a certain period of time, then it will be performed only once after the **Dr.Web Agent** has been launched.

- ◆ **Arguments** - specify, when necessary, additional job launch parameters. Use the command-line parameters specified in p. [Scanner's Command-Line Switches](#).
- ◆ **Daily at** - specify the hour and the minute when the job should be performed.

To close the window and save the parameters of the task, click **OK**.

To close the window without saving the changes/new task, click **Cancel**.

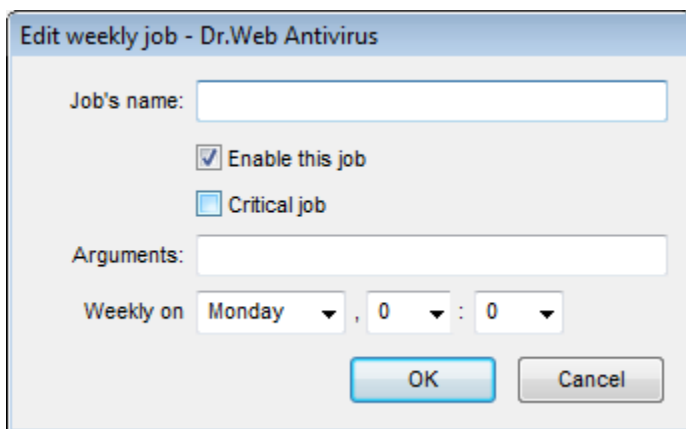


In all dialog boxes of the **Dr.Web Agent**, to receive help about the active window, press F1. To learn about the function of any element of the window, right-click it.

---

### 3.4.1.3. Weekly Job

This job type is performed every week on the specified weekday at the fixed time.



**Figure 3-4. Weekly job dialog box**

In the dialog box of a weekly job (see [Figure 3-4](#)) you can set the following parameters:

- ◆ **Job's name** - type a name of the task.
- ◆ To enable the job, select the checkbox **Enable this job**.  
To disable the job, clear the checkbox. The job will remain on the list but will not be executed.
- ◆ A selected checkbox **Critical job** instructs to perform the job at next **Dr.Web Agent** launch, if execution of this job is omitted (the **Dr.Web Agent** is switched off at the due time). If a task is omitted several times within a certain period of time, then it will be performed only once after the **Dr.Web Agent** has been launched.
- ◆ **Arguments** - specify, when necessary, additional job launch parameters. Use the command-line parameters specified in p. [Scanner's Command-Line Switches](#).
- ◆ **Weekly on** - specify the day of week, the hour and the minute when the job should be performed.

To close the window and save the parameters of the task, click **OK**.

To close the window without saving the changes/new task, click



Cancel.



In all dialog boxes of the **Dr.Web Agent**, to receive help about the active window, press F1. To learn about the function of any element of the window, right-click it.

### 3.4.1.4. Monthly Job

This job type is performed every month on the specified day of month at the fixed time.

The screenshot shows a dialog box titled "Edit monthly job - Dr.Web Antivirus". It contains the following elements:

- Job's name:** A text input field.
- Enable this job:** A checked checkbox.
- Critical job:** An unchecked checkbox.
- Arguments:** A text input field.
- Monthly on:** Three dropdown menus showing the values "1", "0", and "0".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

**Figure 3-5. Monthly job dialog box**

In the dialog box of a monthly job (see [Figure 3-5](#)) you can set the following parameters:

- ◆ **Job's name** - type a name of the task.
- ◆ To enable the job, select the checkbox **Enable this job**.  
To disable the job, clear the checkbox. The job will remain on the list but will not be executed.
- ◆ A selected checkbox **Critical job** instructs to perform the job at next **Dr.Web Agent** launch, if execution of this job is omitted



(the **Dr.Web Agent** is switched off at the due time). If a task is omitted several times within a certain period of time, then it will be performed only once after the **Dr.Web Agent** has been launched.

- ◆ **Arguments** - specify, when necessary, additional job launch parameters. Use the command-line parameters specified in p. [Scanner's Command-Line Switches](#).
- ◆ **Monthly at** - specify the day of month, the hour and the minute when the job should be performed.

To close the window and save the parameters of the task, click **OK**.

To close the window without saving the changes/new task, click **Cancel**.

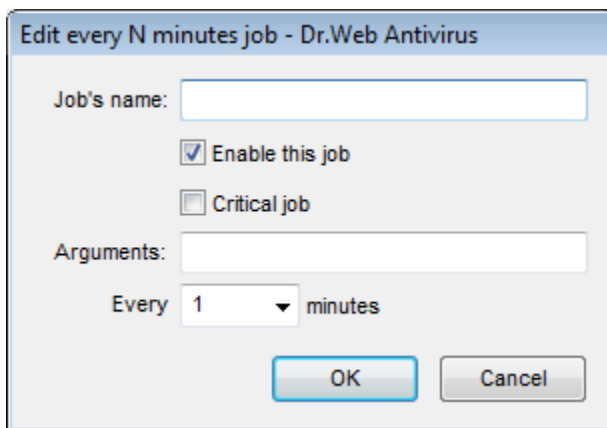


In all dialog boxes of the **Dr.Web Agent**, to receive help about the active window, press F1. To learn about the function of any element of the window, right-click it.

---

### 3.4.1.5. Every N Minutes Job

This job type is performed in a certain time span set in minutes.



**Figure 3-6. Job dialog box**

In the dialog box of a job (see [Figure 3-6](#)) you can set the following parameters:

- ◆ **Job's name** - type a name of the task.
- ◆ To enable the job, select the checkbox **Enable this job**.  
To disable the job, clear the checkbox. The job will remain on the list but will not be executed.
- ◆ A selected checkbox **Critical job** instructs to perform the job at next **Dr.Web Agent** launch, if execution of this job is omitted (the **Dr.Web Agent** is switched off at the due time). If a task is omitted several times within a certain period of time, then it will be performed only once after the **Dr.Web Agent** has been launched.
- ◆ **Arguments** - specify, when necessary, additional job launch parameters. Use the command-line parameters specified in p. [Scanner's Command-Line Switches](#).
- ◆ **Every <...> minutes** - specify a time span in minutes.

To close the window and save the parameters of the task, click **OK**.

To close the window without saving the changes/new task, click **Cancel**.

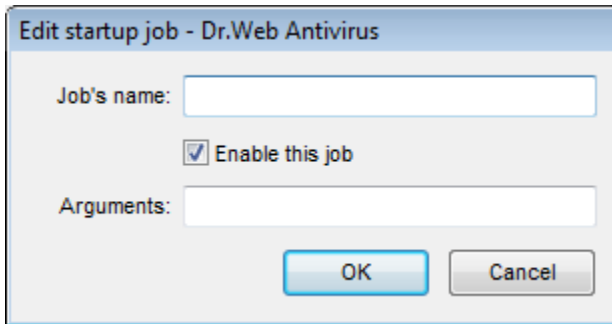




In all dialog boxes of the **Dr.Web Agent**, to receive help about the active window, press F1. To learn about the function of any element of the window, right-click it.

### 3.4.1.6. Startup Job

This job type is performed at computer startup.



**Figure 3-7. Job dialog box**

In the dialog box of a job (see [Figure 3-7](#)) you can set the following parameters:

- ◆ **Job's name** - type a name of the task.
- ◆ To enable the job, select the checkbox **Enable this job**.  
To disable the job, clear the checkbox. The job will remain on the list but will not be executed.
- ◆ **Arguments** - specify, when necessary, additional job launch parameters. Use the command-line parameters specified in p. [Scanner's Command-Line Switches](#).

To close the window and save the parameters of the task, click **OK**.

To close the window without saving the changes/new task, click **Cancel**.

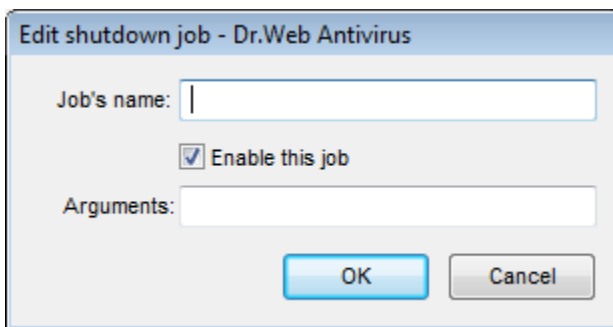


In all dialog boxes of the **Dr.Web Agent**, to receive help about the active window, press F1. To learn about the function of any element of the window, right-click it.

### 3.4.1.7. Shutdown Job

This job type is performed at computer shutdown.

The Shutdown job is not executed for **Dr.Web Enterprise Scanner** and **Dr.Web Scanner for Windows**.



**Figure 3-8. Job dialog box**

In the dialog box of a job (see [Figure 3-8](#)) you can set the following parameters:

- ◆ **Job's name** - type a name of the task.
- ◆ To enable the job, select the checkbox **Enable this job**.  
To disable the job, clear the checkbox. The job will remain on the list but will not be executed.
- ◆ **Arguments** - specify, when necessary, additional job launch parameters. Use the command-line parameters specified in p. [Scanner's Command-Line Switches](#).

To close the window and save the parameters of the task, click **OK**.



To close the window without saving the changes/new task, click **Cancel**.



In all dialog boxes of the **Dr.Web Agent**, to receive help about the active window, press F1. To learn about the function of any element of the window, right-click it.

---

### 3.4.2. Centralized Schedule

In the window of the centralized checkups schedule you can view scanning tasks assigned by the anti-virus **Server** to be performed in the anti-virus network.



In all dialog boxes of the **Dr.Web Agent**, to receive help about the active window, press F1. To learn about the function of any element of the window, right-click it.

---

## 3.5. Setting the Interface Language

To change the language of the **Dr.Web Agent** and **Dr.Web** anti-virus components, select **Language** on the [context menu](#) of its icon. In the drop-down-list, specify the necessary language of the interface.



Changing the language of all anti-virus components could be done only through the **Dr.Web Agent**.

---

## 3.6. Mobile Mode Settings

If your computer (laptop) has no connection to **Enterprise Server(s)** for a long time, to receive updates opportunely from the **Dr.Web GUS**, you are well advised to set the **Agent** to the mobile mode of



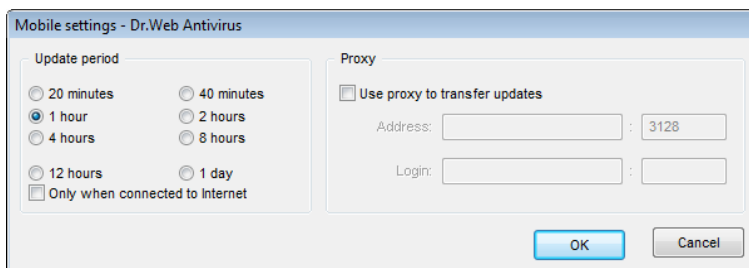
operation. To do this, on the context menu of the **Agent**'s icon in the notification area of the **Taskbar**, select **Mobile mode** → **Enabled**. The icon will turn yellow.

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 an interval of about a minute.



The **Mobile mode** option will be available on the context menu provided that the mobile mode of using the **Dr.Web GUS** has been allowed in the station's permissions.

To adjust the settings of the mobile mode, select **Mobile mode** → **Settings**.



**Figure 3-9. Mobile mode settings dialog box**

In the **Update period** group box, set the frequency of checking the availability of updates on the **GUS**:

- ◆ **20 minutes** - check for updates every 20 minutes.
- ◆ **40 minutes** - check for updates every 40 minutes.
- ◆ **1 hour** - check for updates every hour.
- ◆ **2 hours** - check for updates every 2 hours.
- ◆ **4 hours** - check for updates every 4 hours.
- ◆ **8 hours** - check for updates every 8 hours.
- ◆ **12 hours** - check for updates every 12 hours.
- ◆ **1 day** - check for updates once a day.



If necessary, select the **Only when connected to Internet** checkbox.

When using a proxy server, select the **Use proxy to transfer updates** checkbox and below specify the address and the port of the proxy server, and the parameters of authorization. In this case the following fields will become active:

- ◆ **Address** - type the address and the port of the proxy server.
- ◆ **Login** - type the login and the password for authorization at the proxy server.

In the mobile mode, to initiate updating immediately, select **Mobile mode** → **Start update**.



---

When the **Agent** is functioning in the mobile mode, the **Agent** is not connected to the anti-virus **Enterprise Server**. All changes made for this workstation at the **Server**, will take effect once the **Agent**'s mobile mode is switched off and the connection with the **Server** is re-established. In the mobile mode only virus databases are updated.

---

To switch off the mobile mode, on the context menu of the **Agent**'s icon select **Mobile mode** and clear the **Enabled** option. The color of the icon will change from yellow to green and the **Agent** will be reconnected to the **Server**.



---

In all dialog boxes of the **Dr.Web Agent**, to receive help about the active window, press F1. To learn about the function of any element of the window, right-click it.

---

## 3.7. Viewing the Statistics

To view the statistics of your workstation, select **Statistics** on the **Agent**'s **context menu** or double-click the **Agent**'s icon. A window with a table containing all the statistics on the anti-virus software operation will open.



In the first column the **Dr.Web** components installed on your computer are listed, in the other columns the number of objects checked by them is specified.

These scanned objects are classified as follows:

- ◆ infected objects,
- ◆ modifications,
- ◆ suspicious,
- ◆ activities.

Then the number of the following categories of treated objects is specified:

- ◆ cured,
- ◆ deleted,
- ◆ renamed,
- ◆ moved,
- ◆ blocked.

Then the number of errors and the scanning speed are given.

For more about these statistics categories, please refer to the **Statistics Tab** section of the **Dr.Web for Windows** help built in **Dr.Web** anti-virus programs.



In all dialog boxes of the **Dr.Web Agent**, to receive help about the active window, press F1. To learn about the function of any element of the window, right-click it.

---

## 3.8. Viewing the Anti-Virus Software Status

To view the status of the anti-virus software installed on your workstation, select **Status** on the **Agent's** [context menu](#).

In the top of the opened window you can view general information:



- ◆ total number of records in the virus databases,
- ◆ last update time,
- ◆ version of the **Agent** installed on the computer,
- ◆ scanning activity (whether the Scanner is working or not).

The status window includes the following tabs:

- ◆ **Databases.** Contains detailed information about all virus databases installed:
  - virus database file name,
  - virus database version,
  - number of records in a virus database,
  - virus database creation date.
- ◆ **Components.** Contains detailed information about all **Dr.Web** anti-virus components installed on the workstation:
  - component name,
  - component status: **running** or **not running**.
- ◆ **Modules.** Contains detailed information about all **Dr.Web** anti-virus modules:
  - product module file name.
  - full module version.
  - module description - its functional name.

In the bottom of the status window, you can find

- ◆ status bar displaying the status of the anti-virus software. It shows important notifications (see p. [Agent Settings](#)). When the **Agent** is running without errors, a message "**No action required**" is displayed;
- ◆ **Agent's ID** (unique identification number).



In all dialog boxes of the **Dr.Web Agent**, to receive help about the active window, press F1. To learn about the function of any element of the window, right-click it.

---



## 3.9. Starting the Anti-Virus Scanner

The **Scanner** command of the **Agent's context menu** starts the anti-virus Scanner of **Dr.Web** to check your computer for viruses and malware. When you start the Scanner, its main window will open (for more, see the **Dr.Web for Windows** help, section **Scanner's main window**). At start the Scanner performs a preliminary check of your files, then you may instruct a more comprehensive scanning in one of the modes.

Against the permissions at the **Server**, you may optimize the anti-virus check parameters: select the objects to check, types of actions over detected objects, etc. in Scanner's settings (for more, see the **Dr.Web for Windows** help, section **Dr.Web Scanner for Windows**).



---

To open the **Dr.Web for Windows** help, press F1 in any window of the Scanner. To receive help about any element of the windows, right-click it.

---

## 3.10. File Monitor Settings

**SpIDer Guard for Windows** is an anti-virus guard (also called a monitor). The program constantly resides in the main memory checking all opened files on-access and monitors running processes for virus-like activity.

Against the permissions at the **Server**, you may set up the File Monitor **SpIDer Guard**. To do this, select **File monitor settings** on the **Agent's context menu**.



---

The **File monitor settings** option is available on the **Agent's** context menu only provided the user has

- 1) the permissions to change these settings. The permissions are set at the **Server** by the anti-virus network administrator.





2) administrator rights on the computer.

---

To view or modify the scan parameters, on the **Agent's** context menu select **File monitor settings** → **Scan settings**. A window with **SpIDer Guard** settings will open. The settings are described in detail in the **SpIDer Guard for Windows** help, the **SpIDer Guard Settings** section.

To view or modify the Guard's launch parameters, operation and an alert settings, on the **Agent's** context menu select **File monitor settings** → **Scan settings**. A window with **SpIDer Guard** settings will open. The administration options are described in detail in the **SpIDer Guard for Windows** help, the **Control** section.

To open the **SpIDer Guard for Windows** help, press F1 in any window of the **Guard**.

## 3.11. E-Mail Monitor Settings

**SpIDer Mail for Windows Workstations** is an e-mail monitor. With default settings, **SpIDer Mail** automatically intercepts all calls of any mail programs on your computer to mail servers.

By default, the program is included in the set of installed components, constantly resides in the main memory and is automatically restarted at Windows OS load.

Against the permissions at the **Server**, you may set up the E-Mail Monitor **SpIDer Mail**. To do this, select **E-Mail monitor settings** on the **Agent's** [context menu](#).



The **E-Mail monitor settings** option is available on the **Agent's** context menu only provided the user has

- 1) the permissions to change these settings. The permissions are set at the **Server** by the anti-virus network administrator.



2) administrator rights on the computer.

---

A window with **SpIDer Mail** settings will open. The administration options of **SpIDer Mail** are described in detail in the **Dr.Web for Windows** help, the **Setting SpIDer Mail for Windows workstations** section.

To open the **Dr.Web for Windows** help, press F1 in any window of the **Guard**.

## 3.12. HTTP Monitor Settings

The HTTP Monitor module is installed by default. It constantly resides in main memory and starts automatically with the operating system.

By configuring **SpIDer Gate** you can turn on or turn off monitoring of incoming and outgoing traffic and list applications which traffic you want or do not want to monitor.

Use **SpIDer Gate** settings to configure HTTP monitoring.

Modification of check parameters of the HTTP monitor **SpIDer Gate** may be allowed or blocked by the **Enterprise Suite** administrator. To view or configure **SpIDer Gate** settings, select **HTTP monitor settings** in the **Agent context menu**.



The **HTTP monitor settings** option is available on the **Agent's** context menu only provided the user has

- 1) the permissions to change these settings. The permissions are set at the **Server** by the anti-virus network administrator.
  - 2) administrator rights on the computer.
- 

By default the monitor checks all HTTP traffic (data transferred through the HTTP protocol).



For more information on **SpIDer Gate** settings, refer to section **SpIDer Gate Settings** in **Dr.Web for Windows** Online Help, which you can access by pressing F1 in any **SpIDer Gate** window.

## 3.13. Office Control Settings

**Dr.Web Office Control** helps limit user access to certain local resources and web sites.

This allows you to maintain integrity of important files and protect them from virus infection, as well as prevent unauthorized access to confidential data on your computer.

With **Office Control** you can protect files and folders stored on local disks or removable devices (as long as they are connected to the computer), as well as deny access to removable storages completely.

By controlling Internet access you can protect users from visiting websites which promote violence, gambling or other undesirable topics, or limit available websites to those which you list in **Office Control** settings.

Against the permissions at the **Server**, you may set up the **Office Control** module. To configure **Office Control**, select **Office Control settings** in the **Agent context menu**.



---

The **Office Control settings** option is available only provided the user has

- 1) the permissions to configure **Office Control**. The permissions are set at the **Server** by the anti-virus network administrator.
  - 2) administrator rights on the computer.
- 

Administrators of your Antivirus network have the right to change settings of **Office Control**. Administrator settings automatically override user settings.



---



The list of resources is password-protected from editing. The password is set at the first usage of the module. You can change the password in the **Office Control** settings window or ask the **Enterprise Suite** administrator to do it.

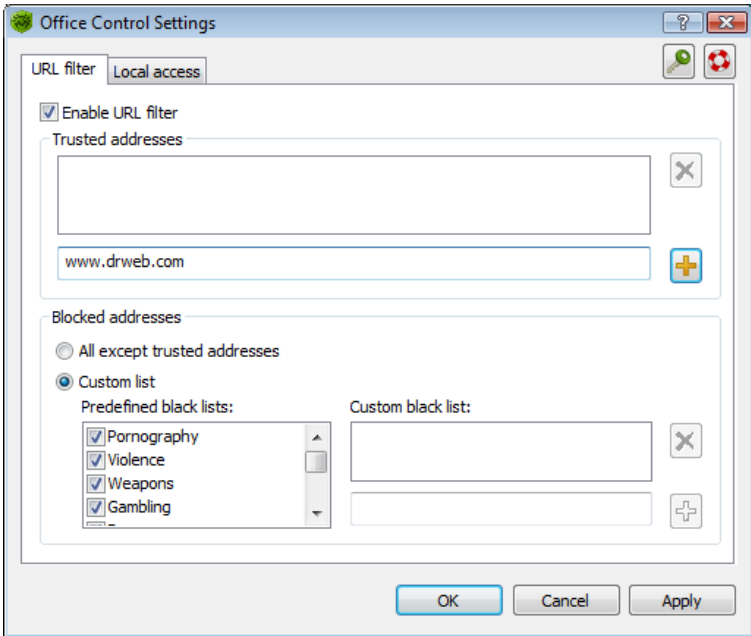
By default the monitor blocks access to all folders of the **Dr.Web** Anti-Virus.

### To configure Office Control:

1. Enter password which you set up on first access to **Office Control** settings. You can change the password by clicking  (**Change password**) in the Settings window.
2. Change **Office Control** settings as needed. See [URL Filter](#) and [Local Access](#) for details.
3. Click  (**Help**) to get help on a window.
4. To save changes without closing the window, click **Apply**. To save changes and close the window, click **OK**. To close the windows without saving changes, click **Cancel**.



### 3.13.1. URL Filter



**Figure 3-10. Office Control Settings. URL Filter Tab**

Use the **URL Filter** tab to configure access to Internet websites.

#### To configure Internet access

1. To turn on Internet access rules, select **Enable URL Filter**. This enables access control options.



To deny access to the Internet completely, select **Network access** on the [Local access](#) tab.



You can enable URL Filter when [antivirus check on incoming traffic](#) is enabled only.

---

2. Configure the list of **Trusted URLs**, which you want users to access without restrictions. **Office Control** never denies access to trusted URLs. For more information on how to list trusted URLs, see [Domain Names List](#).
3. Configure the list of **Blocked URLs**, which you do not want users to access. For this, select one of the following options:
  - a) To block all websites which are not listed as **Trusted URLs**, select **All except trusted URLs**.
  - b) To configure a custom list of websites which you want to block, select **Custom URLs**. You can block websites by subject or URL.

If you selected **Custom URLs** for the blocking rule, use **Categories** options to select topics which you want to block. **Office Control** URL filter automatically recognizes and blocks websites which contain undesirable information.



Filter lists for all categories are updated with virus database updates.

---

You can also populate the **Address bar content** list with URLs of known undesirable websites, or address templates. For more information on how to list forbidden websites, see [Domain Names List](#).

4. To save changes without closing the window, click **Apply**. To save changes and close the window, click **OK**. To close the windows without saving changes, click **Cancel**.


## Domain Names List

**Office Control** uses domain names lists to configure Internet access. On the **URL Filter** tab, you can select domains which you want to block or domains which you want users to access.



### To configure domain names list

Do one of the following:

- 1) To add a new item to the list, enter an URL and click  **Add**. You can enter either a full address, or a part of address which determines websites with similar names. See Table 4 for examples of how URL Filter interprets list items.

**Table 4. Filter examples**


String	Filtering rule
domainname	<p>This string determines any website which URL contains the "domainname" substring. For example, the following web pages are filtered:</p> <ul style="list-style-type: none"><li>◆ www.<b>domainname</b>.com</li><li>◆ www.top<b>domainname</b>.com</li><li>◆ www.<b>domainname</b>.com/path/index.html</li><li>◆ www.subdomain.<b>domainname</b>.org</li><li>◆ www.toplevel.org/<b>domainname</b>system.html</li></ul>
domainname.com	<p>The dot (.) defines this string as a domain name. All pages in this domain and its subdomains are filtered.</p>
domainname.com/ path	<p>The slash (/) defines this string as a path in the domain. The first part of the string is interpreted as a domain name, while the second part is interpreted as a specific path.</p> <p>This rule filters all resources in the domain <b>domainname.com</b> and its subdomains, which address starts with path. For example, the following web pages are filtered:</p> <ul style="list-style-type: none"><li>◆ www.<b>domainname.com/path</b></li><li>◆ www.<b>domainname.com/path</b>/index.html</li><li>◆ www.subdomain.<b>domainname.com/path</b>/</li><li>◆ www.<b>domainname.com/pathetic</b></li></ul>



String	Filtering rule
	<p>Note, that a website is filtered only when its address contains the string in the given sequence. For example, the following pages are <b>not</b> filtered:</p> <ul style="list-style-type: none"><li>◆ www.domainname.com</li><li>◆ www.domainname.com/wrongpath</li></ul>
domainname.com? param=256	<p>This string determines any page on the domain which contains the "<b>param=256</b>" substring. The question mark (?) stands for any number of other characters. For example, the following web pages are filtered:</p> <ul style="list-style-type: none"><li>◆ www.<b>domainname.com?param=256</b></li><li>◆ www.<b>domainname.com?first=512&amp;param=256</b></li></ul>



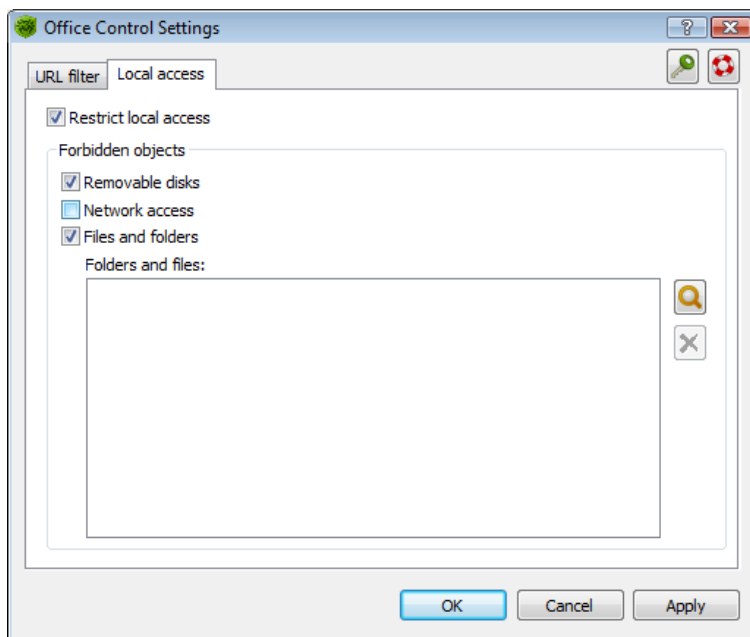
The address may be converted to a more simple structure (e. g. `http://www.domainname.com` will be converted to `www.domainname.com`).

- 2) To remove an item from the list, select the item and click  **(Delete)**.





### 3.13.2. Local Access



**Figure 3-11. Office Control Settings. Local Access Tab**

Use the **Local Access** tab to configure access to local resources.

#### To configure local access

1. To turn on local access rules, select **Restrict local access**. This enables access control options.
2. Configure the list of **Forbidden objects**, which you do not want users of your computer to access. See Table 5 for options description.



Table 5. Local Access Rules Options

Flag	Description
Removable disks	<p>Select this checkbox to deny access to and usage of removable media.</p> <p>Clear the checkbox to allow usage of removable media.</p> <p>Removable disks include, for example:</p> <ul style="list-style-type: none"><li>◆ CD and DVD disks;</li><li>◆ floppy disks (FDD);</li><li>◆ flash drives and other data carriers connectible through USB;</li><li>◆ etc.</li></ul>
Network access	<p>Select this option to block all network connections to your computer. This denies access to local networks and the Internet.</p> <p>Clear the option to allow access to the local network and the Internet.</p>
Files and folders	<p>Select this checkbox to create a list of local resources (files and folders) access to which you want to block.</p> <p>Blocked files and folders are specified in the <b>Folders and files</b> list.</p> <p>For more information on how to list forbidden local resources, see <a href="#">Configure blocked files and folders list</a>.</p>



You cannot use **Office Control** to restrict access to the following folders or their root directories:

- ◆ System disk,
- ◆ User Profile folder,
- ◆ Program Files folder.

If you need to restrict access to files stored in these folders, configure **Office Control** to block subfolders which contain restricted data.



**Office Control** cannot restrict access to network files and folders.



3. To save changes without closing the window, click **Apply**. To save changes and close the window, click **OK**. To close the windows without saving changes, click **Cancel**.

### To configure blocked files and folders list

1. To turn on local access rules on your computer, select Protect files and folders checkbox.
2. Do one of the following:

- ◆ To add a new item to the list, click  (**Browse**), select a file or folder to add in File Manager and click **Open**.
- ◆ To remove a item from the list, select the item and click  (**Delete**).

## 3.14. Informational Messages

The user is notified about system events by means of popup windows emerging near the **Agent's** icon.

The messages in popups can contain miscellaneous information:

- ◆ Notifications – detailed information about actions performed or to be performed over the anti-virus software or your PC.
- ◆ **Agent's** summary – combined data about the operation and status of the anti-virus software.
- ◆ Messages from the administrator.

### Notifications

Informational messages may notify about virus events and actions of the anti-virus software on your PC (for more, see p. [Agent Settings](#)).

Besides the function of informing, popup messages may also perform control functions. For example, the dialog box prompting to restart the PC after anti-virus components have been updated has the buttons to restart the PC or delay the restart (see [Figure 3-12](#)).



**Figure 3-12. Notification from the Dr.Web Agent**

## Agent's Summary

When you point the mouse cursor to the **Agent's** icon, an informational popup window appears with data about:

- ◆ the statistics of virus events (see also p. [Viewing the Statistics](#)),
- ◆ the status of the anti-virus software components,
- ◆ the date of last update.



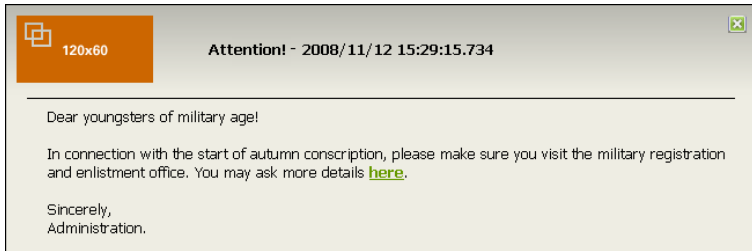
**Figure 3-13. Message window of the Dr.Web Agent**

### Messages from the Administrator (Provider)

The user may receive informational messages from the anti-virus network administrator (provider) including:

- ◆ message text;
- ◆ hyperlinks to Internet resources;
- ◆ company's logo (or any other graphic presentation);
- ◆ exact date of message receipt in the title of the window.

These messages appear as popup windows (see [Figure 3-14](#)).



**Figure 3-14. Message window from the administrator (provider)**



Windows with messages from the administrator are displayed until the user closes them, unlike popup windows with notifications and **Agent's** summary, which are hidden after having been inactive for a certain period of time.



## Appendix A. Scanner's Command-Line Switches

When scanning task is launched, it is performed by **Dr.Web Scanner**. If necessary, you can specify additional parameters of the checkup. You can enter the following switches (separated by spaces) in the **Arguments** entry field:

- ◆ /@ <file\_name> or /@+<file\_name> instructs to scan objects listed in the specified file. Each object is specified in a separate line of the list-file. It can be either a full path with the file name or the ?boot string which means that scanning of boot sectors should be performed. For the GUI version of the scanner the file names with mask and directory names should be specified there. The list-file can be prepared manually in any text editor; this can also be done automatically via applications using the scanner to check certain files. After the scanning is completed, the scanner deletes the list-file, if used without the + character.
- ◆ /AL – to scan all files in the given device, or in the given folder, regardless the extensions or the internal format.
- ◆ /AR – to scan files inside the archives. At present, the scanning of archives (without curing) created by the ARJ, PKZIP, ALZIP, AL RAR, LHA, GZIP, TAR, BZIP2, 7-ZIP, ACE, etc. archivers, as well as of MS CAB-archives – Windows Cabinet Files (QUANTUM packing is not supported yet) and ISO-images of optical disks (CD and DVD) is available. As it is specified (/AR) the switch instructs to inform a user when an archive with infected or suspicious files is detected. If the switch is supplemented with the D, M or R modifier, other actions are taken:
  - /ARD – delete;
  - /ARM – move (by default, to the infected.!!! folder);
  - /ARR – rename (by default, the first symbol of the extension is replaced by the # character).



- The switch may end with the **N** modifier, and in this case the name of the archiver after the name of the archived file will not be printed.
- ◆ **/CU** – actions with infected files and boot sectors of drives. The curable objects are cured and the incurable files are deleted without additional **D**, **M** or **R** modifiers (if different action is not specified by the **/IC** switch). Other actions taken towards infected files:
  - **/CUD** – delete;
  - **/CUM** – move (by default, to the `infected.!!!` folder);
  - **/CUR** – rename (by default, the first symbol of extension is replaced by the **#** character).
- ◆ **/SPR**, **/SPD** or **/SPM** – actions with suspicious files:
  - **/SPR** – rename;
  - **/SPD** – delete;
  - **/SPM** – move.
- ◆ **/ICR**, **/ICD** or **/ICM** – actions with infected files which cannot be cured:
  - **/ICR** – rename;
  - **/ICD** – delete;
  - **/ICM** – move.
- ◆ **/MW** – actions with all types of unsolicited programs. As it is specified (**/MW**) the switch instructs to inform a user. If the switch is supplemented with the **D**, **M**, **R** or **I** modifier, other actions are taken:
  - **/MWD** – delete;
  - **/MWM** – move (by default, to the `infected.!!!` folder);
  - **/MWR** – rename (by default, the first symbol of extension is replaced by the **#** character);
  - **/MWI** – ignore. Actions with certain types of unsolicited programs are specified by the **/ADW**, **/DLS**, **/JOK**, **/RSK**, **/HCK** switches.





- ◆ /DA – to scan the computer once a day. The next check date is logged into the configuration file and that is why it should be accessible for writing and subsequent rewriting.
- ◆ /EX – to scan files with extensions listed in the configuration file by default, or, if unavailable, these are EXE, COM, DLL, SYS, VXD, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, 386, FON, DO?, XL?, WIZ, RTF, CL\*, HT\*, VB\*, JS\*, INF, PP?, OBJ, LIB, PIF, AR?, ZIP, R??. GZ, Z, TGZ, TAR, TAZ, CAB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SH, SHB, SHS, SHT\*, MSG, CHM, XML, PRC, ASP, LSP, MSO, OBD, THE\*, EML, NWS, SWF, MPP, TBB.



If an element of the list of scanned objects contains the explicit file extension, and it is used with special characters \* and ?, all files specified in this element of the list will be scanned and not only those matching this list of extensions.

- ◆ /FN – to load Russian letters to the video display decoder (for **Dr.Web for DOS** only).
- ◆ /GO – batch mode of the program. All questions implying answers from a user are skipped; solutions implying a choice are taken automatically. This mode is useful for automatic scanning of files, for example, during a daily or weekly check of the hard disk.
- ◆ /SCP: <n> – sets the priority of the scanning process, where <n> is a number ranging from 1 to 50.
- ◆ /SHELL – for the GUI version of the scanner. The switch disables the splash screen display, scanning of the memory and autorun files. The earlier saved lists of paths to files and folders scanned by default are not loaded for scanning. This mode allows to use the GUI version of the scanner instead of the console version to scan only those objects which are listed in the command line switches.
- ◆ /ST – sets stealth mode of the GUI version of the scanner. The program operates without any windows opened and self-terminates. But, if during scanning virus objects were detected, the scanner window will be opened after the scanning is



completed. Such scanner mode presupposes, that the list of the scanned objects is specified in the command line.

- ◆ /HA – to perform heuristic scanning of files and search for unknown viruses in them.
- ◆ /INI: <path> – use alternative configuration file with specified name or path.
- ◆ /NI – do not use parameters specified in `drweb32.ini` configuration file.
- ◆ /LNG: <file\_name> or /LNG – use alternative language resources file (DWL-file) with specified name or path, and if the path is not specified – the inbuilt (English) language.
- ◆ /ML – scan files of e-mail format (UUENCODE, XXENCODE, BINHEX and MIME). As it is specified (/ML) the switch instructs to inform a user if an infected or suspicious object is detected in a mail archive. If the switch is supplemented with the D, M or R modifier, other actions are taken:
  - /MLD – delete;
  - /MLM – move (by default, to the `infected.!!!` folder);
  - /MLR – rename (by default, the first symbol of extension is replaced by the # character);
  - In addition the switch may be supplemented by an extra modifier N (at the same basic modifiers may also be set). In this case information output about mail archive messages is disabled.
- ◆ /NS – disable interrupting of computer scanning. With this switch specified, a user will not be able to interrupt scanning by pressing ESC.
- ◆ /OK – display full list of scanned objects and mark the uninfected ones with **Ok**.
- ◆ /PF – prompt on, if multiple floppies are scanned.
- ◆ /PR – prompt for confirmation before action.
- ◆ /QU – the scanner checks the objects specified in the command line (files, disks, folders) and then automatically terminates (for the GUI version of the scanner only).
- ◆ /RP<file\_name> or /RP+<file\_name> – log to the file



specified in the switch. If no name is specified, log to a default file. If the + character is present, the file is appended. If there is no character, a new one is created.

- ◆ /NR – do not create a log file.
- ◆ /SD – scan subfolders.
- ◆ /SO – enable sounds.
- ◆ /SS – save the mode, specified during the current program launch in the configuration file when the program terminates.
- ◆ /TB – scan boot sectors and master boot records (MBR) of the hard drive.
- ◆ /TM – search for viruses in main memory (including Windows OS system area). Available for scanners for Windows OS only.
- ◆ /TS – search for viruses in autorun files (in Autorun directory, system INI-files, Windows OS registry). Used only in scanners for Windows OS.
- ◆ /UPN – disable the output of the names of the programs used for packing, conversion or vaccination of the scanned executable files to the log file by the scanners.
- ◆ /WA – do not terminate the program until any key is pressed, if viruses or suspicious objects are found (for console scanners only).
- ◆ /? – display short help on the program.

Certain switches allow the "-" character to be used at the end. In such "negative" form the switch means cancellation of the mode. Such option can be useful if a certain mode is enabled by default, or with the settings specified earlier in the configuration file. Here is the list of the command line switches allowing the "negative" form:

/ADW /AR /CU /DLS /FN /HCK /JOK /HA /IC /ML /MW /OK /PF /PR /RSK /SD /SO /SP/SS /TB /TM /TS /UP /WA

For /CU, /IC and /SP switches the "negative" form cancels any actions specified in the description of these switches. This means that infected and suspicious objects will be reported but no actions will be applied.

For /INI and /RP switches the "negative" form is written as /NI



and /NR accordingly.

For /AL and /EX switches the "negative" form is not allowed. However, specifying one of them cancels the other.

If several alternative parameters are found in the command line, the last of them takes effect.



## Appendix B. Installers's Command-Line Switched

At installer's start you can set additional parameters of **Agent's** installation.



---

By default the `drwinst` instruction launched without parameters will scan the network for **ES- Servers** and try to install the **Agent** from the first found **Server**.

---

- ◆ To view the installation log in the real time mode, use the `-interactive` parameter.
- ◆ It is strongly recommended to specify a domain name for the **ES- Server** in the DNS service and use this name when installing the **Agent**: `drwinst -interactive <antivirus_Server_DNS_name>`. It is especially useful in case you would like to reinstall the **ES- Server** on a different computer.

Or you can expressly specify the **Server's** address as follows:

```
drwinst -interactive 192.168.1.3
```

- ◆ The `-useolddlg` switch used together with the `-interactive` switch allows the dialog with the **Agent** installation log to be displayed.
- ◆ Using the `-regagent` switch during the installation will allow you to register the **Agent** in the Add or Remove Programs list.
- ◆ When the **drwinst** program is run with the `-config` switch a dialog box will open, which allows to change the default settings of the installer and some of the basic default settings of the **Agent** and to specify the components of the anti-virus package to be installed.



---

The settings available in the interface of the network installer are expanded in Administrator Manual **Dr. Web Enterprise Suite Anti-Virus**, p. **Remote Installation of the Anti-Virus Agent**.

---

The full list of possible switches of the network installer is given in Administrator Manual **Dr. Web Enterprise Suite Anti-Virus**, **Appendix H4**.

---



# Index

## A

- access restriction
  - Internet 42, 45
  - local resources 49
- administrator's messages 51
- Agent
  - administration 13
  - functions 9
  - installing, uninstalling 10
  - interface 12
  - language 35
  - menu 14
  - start, stop 12
- anti-virus software
  - installing, uninstalling 10
  - status 38
  - updating 23
- arguments, command line 55

## B

- blocking
  - HTTP-traffic 42, 45
  - local resources 49

## C

- centralized schedule 35
- context menu, Agent 14

## D

- daily job 27

- Dr.Web®, anti-virus 7

## E

- e-mail monitor 41

## F

- file monitor 40
- functions
  - Dr. Web Enterprise Suite 7

## H

- hourly job 25
- HTTP-monitor 42
- HTTP-traffic, blocking 42, 45

## I

- informational messages 51

## J

- job
  - daily 27
  - every N minutes 31
  - hourly 25
  - monthly 30
  - shutdown 34
  - startup 33
  - weekly 28
- jobs, local 24

## L

- language, setting 35



# Index

- level of detail, log 22
- local resources, blocking 49
- local schedule 24
- logging 22
- M**
- messages 19
- mobile mode 35
- mode
  - mobile 35
- monitor
  - e-mail 41
  - file 40
  - HTTP 42
  - system 15
- monthly job 30
- O**
- Office Control 43
- P**
- popup windows 51
- R**
- removable disks 49
- run mode
  - Server interaction 23
- S**
- scanner 40
- schedule
  - centralized 35
  - local 24
- Server
  - connection 20
- Server, interaction with
  - connection settings 20
  - run mode 23
- shutdown job 34
- shutdown, Agent 12
- SpIDer Gate 42
- SpIDer Guard 40
- SpIDer Mail 41
- start
  - Agent 12
- start the scanner 40
- startup job 33
- statistics 37
- status, anti-virus components 38
- switches
  - command line 55
  - installer 61
- synchronization 23
- system monitoring 15
- system requirements 10
- T**
- taskbar 12
- U**
- updating 23





# Index

## V

virus

    databases, status 38

    messages 19

## W

weekly job 28

