Dr.WEB

KATANA Business Edition

Administrator Manual

Trademarks

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 KATANA Business Edition
Version 1.0
Administrator Manual
11/26/2021

Doctor Web Head Office

2-12A, 3rd str. Yamskogo polya, Moscow, Russia, 125124

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

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

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

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions 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 anti-virus 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

1. Introduction

This documentation is an administrator manual for Dr.Web KATANA Business Edition. It describes installation and effective utilization of Dr.Web KATANA Business Edition. The order of the chapters in this manual corresponds the order of your actions with the program. The first chapters describe the processes of installing of Dr.Web KATANA Business Edition, creating profiles, searching stations and installing Dr.Web KATANA to stations; the last chapters—managing protection settings for stations and settings for Dr.Web KATANA Business Edition itself.

This manual does not describe the anti-virus solution Dr.Web KATANA. To find more information about Dr.Web KATANA, read **Dr.Web KATANA. User Manual** or visit the Doctor Web official website.

1.1. Document Conventions

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

Convention	Comment
⚠	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.

1.2. Main features of Dr.Web KATANA Business Edition

With Dr.Web KATANA Business Edition you can centrally install Dr.Web KATANA on network stations. Dr.Web KATANA protects your system against computer threats by means of non-signature-based technologies—using behavior analysis, cloud-based threat detection, and preset rules.

Using Dr.Web KATANA Business Edition, you can manage the security level and state of the stations.

The main features of Dr.Web KATANA Business Edition:

- centralized installation of Dr.Web KATANA on the protected network stations,
- centralized management of Dr.Web KATANA settings,
- monitoring of virus events and the states of Dr.Web KATANA on the protected stations.

1.3. System Requirements

To ensure correct operation of Dr.Web KATANA Business Edition (Management Console), you computer should meet the following system requirements:

Parameter	Requirement
CPU	With an i686-compatible processor and SSE2 instructions.
Free RAM	Minimum 100 MB of RAM.
Hard disk space	150 MB for Dr.Web components. Files created during installation will require additional space.
Operating system	For 32-bit platforms: • Windows XP with Service Pack 3 or later • Windows Vista with Service Pack 2 or later • Windows 7 • Windows 8 • Windows 8.1 • Windows 10 21H2 or earlier • Windows Server 2003 with Service Pack 1 or later • Windows Server 2008 with Service Pack 2 or later For 64-bit platforms: • Windows Vista with Service Pack 2 or later • Windows 7

Parameter	Requirement
	• Windows 8 • Windows 8.1 • Windows 10 21H2 or earlier • Windows 11 • Windows Server 2008 with Service Pack 2 or later • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022
Screen resolution	1024x768 or higher.

To ensure a correct operation of Dr.Web KATANA Business Edition, the following ports must be opened:

Purpose	Direction	Port numbers
To activate and renew the license	outgoing	443
To update (if the option to update using https is enabled)	outgoing	443
To update	outgoing	80

To install Dr.Web KATANA, the stations (protected client computers) should meet the following requirements:

Parameter	Requirement
CPU	An i686-compatible processor.
Free RAM	Minimum 100 MB of RAM.
Hard disk space	150 MB for Dr.Web components. Files created during installation will require additional space.
Operating system	For 32-bit platforms: • Windows XP with Service Pack 2 or later • Windows Vista with Service Pack 2 or later

	• Windows 7 • Windows 8 • Windows 8.1 • Windows 10 21H2 or earlier • Windows Server 2003 with Service Pack 1 or later • Windows Server 2008 For 64-bit platforms: • Windows Vista with Service Pack 2 or later • Windows 7 • Windows 8 • Windows 8.1 • Windows 10 21H2 or earlier • Windows 11 • Windows Server 2008 with Service Pack 2 or later • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022
Screen resolution	1024x768 or higher.

To ensure a correct operation of Dr.Web KATANA, the following ports must be opened:

Purpose	**Direction**	**Port numbers**
To activate and renew the license	outgoing	443
To update (if the option to update using https is enabled)	outgoing	443
To update	outgoing	80
To connect to Dr.Web Cloud	outgoing	2075 (including UDP)

2. Licensing

To use Dr.Web KATANA Business Edition, you need a license. You can purchase it together with the product on the Doctor Web official website or through authorized partners.

License activation

To use Dr.Web KATANA Business Edition, you should activate the license. For this, register the license on the Doctor Web official website and obtain a key file. It is recommended that you activate the license before starting the installation process of Dr.Web KATANA Business Edition. In this case, you can specify the key file during the installation process and start using the program immediately after the installation. Otherwise, Dr.Web KATANA Business Edition will not function until you specify the valid key file.

License cost

The cost of the license for Dr.Web KATANA Business Edition depends on the number of the stations on which you want to install Dr.Web KATANA. The administrator's computer is considered if you install not only Dr.Web KATANA Business Edition but also Dr.Web KATANA on it. You can install Dr.Web KATANA to the administrator's computer manually in the **Installation** section of Dr.Web KATANA Business Edition.

Purchasing a new license

If while using Web KATANA Business Edition you need to install Dr.Web KATANA on more stations than currently allowed by your license, you can buy a new one on the Doctor Web official website or through authorized partners. With a new license, you can install Dr.Web KATANA to more stations and continue managing the stations where Dr.Web KATANA was already installed. At this, your previous license will be blocked.

Dr.Web KATANA will be installed only on the number of stations specified in the license.

2.1. Reactivating License

You may need to reactivate a license if the key file is lost.

> ⚠ When reactivating a license, you receive the same key file as during the previous registration providing that the validity period is not expired.

When you reinstall the product, you will be able to use the previously registered key file. Reactivation of the key file is not required.

The number of requests for a key file receipt is limited. One serial number can be registered not more than 25 times. If more requests are sent, the key file will not be delivered. In this case, to receive a lost key file, contact your technical support describing your problem in detail, stating your personal data input during the registration and the serial number. The key file will be sent by our technical support to your email address.

2.2. Key File

The use rights for Dr.Web are specified in the *key file*. The key file has the `.key` extension and contains the following information:

- List of licensed anti-virus components
- Licensed period for the product
- Availability of technical support for the user
- Other restrictions (for example, the number of remote computers allowed for simultaneous anti-virus scan)

> ⚠ By default, the key file is located in the Dr.Web installation folder. Dr.Web verifies the file regularly. Do not edit or modify the key file to avoid its corruption.
>
> If no valid key file is found, Dr.Web KATANA Business Edition will not function.

A *valid* key file for Dr.Web satisfies the following criteria:

- License is not expired.
- Integrity of the key file is not violated.

If any of the conditions is violated, the key file becomes *invalid*.

It is recommended that you keep the key file until the license or a demo version expires.

3. Installing, Restoring, and Removing Dr.Web KATANA Business Edition

Before installing Dr.Web KATANA Business Edition, note the system requirements and do the following:

- Install all critical updates released by Microsoft for the OS version used on your computer (detailed information about Windows and Windows Server). If the operating system is no longer supported, then upgrade to a newer operating system.
- Check the file system and remove the detected errors.
- Close all active applications.

3.1. Installation of Dr.Web KATANA Business Edition

To install Dr.Web KATANA Business Edition

1. Run the installation file that you received with the license.
2. Read the License Agreement. For this, click the corresponding link in the first window.
3. To specify the installation path and configure other settings, click **Installation parameters**. If you want to use default installation settings, go to step 4.
   - On the first tab, you can select the installation path.
   - On the **Advanced options** tab, you can create shortcuts to run Dr.Web.

   To save the changes, click **OK**. To close the window without saving the changes, click **Cancel**.
4. Click **Next**. Please note that by clicking the Next button you accept the terms of the License agreement.
5. In the open **License** window
   - Select **Specify the path to the valid key file** if you have a key file on the hard drive or removable media. Click **Browse** and select the key file.
   - Select **Receive license later** to continue the installation process without a key file. In this case, you cannot use the program until the valid key file is specified.

   Click **Install** to start the installation.
6. When the installation is completed, you enable the **Run Dr.Web KATANA Business Edition** option to run KATANA Business Edition after installation.

Post-installation procedure of Dr.Web KATANA Business Edition

If the administrator's computer has a third-party firewall installed on it

- Add `dwservice.exe` file in the firewall exception list. The UDP port number should be 55567, the TCP port number may be any.

If the network computers have an third-party firewall installed on them

- Add `katana-console.exe` file in the firewall exceptions list on each computer with Dr.Web KATANA. The numbers of UDP and TCP ports may be any.

Installing Dr.Web KATANA on the administrator's computer

In addition to Dr.Web KATANA Business Edition, you can install Dr.Web KATANA on your computer. For this, when Dr.Web KATANA Business Edition is launched, go to the **Installation** section and continue installation of Dr.Web KATANA on your computer along with the installation of Dr.Web KATANA on other stations.

For more details on the installation of Dr.Web KATANA on stations, refer to Installing Dr.Web KATANA on stations.

3.2. Restoring and Removing Dr.Web KATANA Business Edition

1. To remove or to restore Dr.Web KATANA Business Edition, do the following (depending on the operating system):
   - For Windows XP (depending on the appearance of the Start menu):
     - Start menu: Start → Control Panel → Add or Remove programs.
     - Classic Start menu: Start → Settings → Control Panel → Add or Remove programs.
   - For Windows Vista (depending on the appearance of the Start menu):
     - Start menu: Start → Control Panel, then, depending on the Control Panel view:
     - Classic view: Programs and Features.
     - Control Panel Home: Programs → Programs and Features.
     - Classic Start menu: Start → Settings → Control Panel → Programs and Features.
   - For Windows 7, click Start → Control Panel, then, according to the Control Panel view:
     - Small/large icons: Programs and Features.
     - Category: Programs → Uninstall a program
   - For Windows 8, Windows 8.1, and Windows 10, open Control Panel in any convenient way: for example, right-click the bottom left corner and select the Control Panel item in the shortcut menu. According to the selected View option for the Control Panel, click
     - Small/large icons: Programs and Features.
     - Category: Programs → Uninstall a program
2. In the open window, select the program. Then select the necessary option.
3. In the **Parameters** window, you can save the profile settings that can be necessary during the reinstallation of the program. This option is enabled by default.

4. Getting Started

If during the installation procedure of you specified the valid key file you can start working with Dr.Web KATANA Business Edition once you run it. If you did not specify the valid key file, you need to do it to continue working with Dr.Web KATANA Business Edition.

To start managing stations

1. Create a profile.
2. Prepare stations for Dr.Web KATANA installation.
3. Add stations.
4. Install Dr.Web KATANA on stations.

During the installation procedure, new stations are added to the list in the **Management** section. This section allows you to manage all stations from the list even if the installation is not completed yet on all stations. Other stations appear in **Management** automatically.

5. Profiles

You can work with Dr.Web KATANA Business Edition only if you have a profile with keys, login credentials to access the network, and the Dr.Web KATANA Business Edition settings. You can log in to the existing profile or create a new one in the future.

To create a new profile at launch

1. Click **Start** on the Welcome screen.
2. In the open window, specify a profile name and a password.
3. Generate encryption keys for your profile. You can generate keys automatically or import the existing private key. In the latter case, the public key will be generated automatically.
4. Once a new profile is created, the **Installation** section opens. In this section, you can find stations and install Dr.Web KATANA on them.

> ⚠ Encryption keys must be generated for every profile. Only one pair of keys can be generated for one profile. Then you will be able to generate new encryption keys and distribute them to stations if necessary.

To log in to the existing profile

1. Select the name of the necessary profile in the **Username** list.
2. Enter the password. To view it, click 👁.
3. Click **Log in**.

To create a new profile in the main window

If you need to create a profile while you are working in the program

1. Click ⊞ next to the **Profiles** menu item.
2. In the open window, specify a profile name and a password.
3. Use Dr.Web KATANA Business Edition to generate encryption keys or import the existing private key. In the latter case, a public key will be generated automatically.

   The **Import current settings to the new profile** option allows you to import settings and encryption keys from the profile you are currently working in. All settings are imported to the new profile, including the settings that you have not saved yet. This option is enabled by default.

You can switch between the profiles in the menu at any time.

You can also delete profiles. To do this, place the cursor on the profile name in the menu and click ☒ next to the profile name. While deleting the profile which you are working in, you can log in to one of the existing profiles or create a new one.

6. Preparing Stations

To install Dr.Web KATANA on stations, review the following requirements:

- The **Network Discovery** option must be enabled on the computer together with Dr.Web KATANA Business Edition if you want to find stations in the network using this method.
- Station must be accessible through the network.
- The user account which is used to connect to stations must exist and have all necessary administrative privileges.
- If a remote computer is protected by a firewall, the following settings should be performed.

  If you use Windows Firewall, in its settings click **Additional Settings**, select **Inbound Rules** and turn on the following exceptions for the firewall **Private** profile: **Netlogon Service (NP-In)** and **File and Printer Sharing (SMB-In)**. However, if the station is in the domain, the exceptions should be turned on for the **Domain** profile.

  If you use other firewalls it is necessary to open port 445.
- Additional configuration is required (see below).

Before starting anti-virus scans, make sure you have usernames and passwords of administrative accounts on all stations.

⚠ Preparation of a remote operating system must be performed with administrator privileges.

Advanced Settings

To install Dr.Web KATANA on stations, review the following additional requirements:

- The User Account Control (UAC) restrictions must be disabled if the station is running Windows Vista or later operating system. You do not need to perform this setting, if you work under the built-in Administrator account. If so, skip this step.

  Open a registry editor.

  1. Locate and select the following registry subkey: HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM.
  2. If the **LocalAccountTokenFilterPolicy** registry entry does not exist, create the entry:
     a. On the **Edit** menu, select **New**, then click **DWORD Value**.
     b. In the entry name field, type **LocalAccountTokenFilterPolicy**.
  3. Right-click **LocalAccountTokenFilterPolicy** and select **Modify**.
  4. In the **Value data** box, type **1**.
  5. Click **OK** and exit the registry editor.

6. Restart the station.
7. Repeat the steps for all stations you want to scan.

> ⚠ This operation is recommended for experienced users only. Serious problems might occur if the registry is modified incorrectly. Microsoft recommends to backup the registry before you modify it.

- All necessary network services must be installed and configured properly.

To check network settings

1. Open Control Panel on the station.
   - When configuring operating systems earlier than Windows Vista, select **Network and Internet** (if this item is absent, click **Switch to Classic View**).
   - When configuring Windows Vista, select the view mode by category. In the **Network and Internet** section, click **View network status and tasks** → **Manage Network Connections**.
   - When configuring Windows 7 or Windows Server 2008, select the view mode by category. In the **Network and Internet** section, click **View network status and tasks** → **Change adapter settings**.
   - When configuring Windows 8, Windows 10 or Microsoft Windows Server 2012, in the **Network and Internet** section, click **Network and Sharing Center** → **Change adapter settings**.
2. Right-click the connection to the network then select **Properties**.
3. Ensure that the following services are installed and configured:
   - Client for Microsoft Networks
   - File and Printer Sharing for Microsoft Networks
   - Internet Protocol version 4 (TCP/IPv4) or version 6 (TCP/IPv6)
4. Save the changes and close the window.

- Sharing settings must enable advanced configuration.

To enable advanced sharing

1. Open Control Panel on the station.
   - When configuring Windows XP and Windows Server 2003, select **Windows Firewall** (if this item is absent, click **Switch to Classic View**).
   - When configuring Windows Vista, select the view mode by category. In the **Network and Internet** section, click **Set up file sharing**.
   - When configuring Windows 7 or Microsoft Windows Server 2008, select the view mode by category. In the **Network and Internet** section, select **Network and Sharing Center** and then click **Change advanced sharing settings**.

    - When configuring Windows 8, Windows 10 or Microsoft Windows Server 2012, in the **Network and sharing center** section, select **Network and Sharing Center** and then click **Change advanced sharing settings**.

  2. In the open window, select one of the following:

     - When configuring Windows XP or Microsoft Windows Server 2003, open the **Exceptions** tab and enable **File and Printer Sharing**.
     - When configuring Windows Vista, select **Network discovery** and **File and printer sharing**.
     - When configuring Windows 7, select **Turn on network discovery** and **Turn on file and printer sharing**.
     - When configuring Microsoft Windows Server 2008, Windows 8, Windows 10, or Microsoft Windows Server 2012 select **Turn on file and printer sharing**.

  3. Save the changes and close the window.

- Classic sharing and security model for local accounts must be configured.

To enable classic user authentication method

1. Open Control Panel on the station.

   - When configuring operating systems earlier than Windows Vista, select **Administrative tools** (if this item is absent, click **Switch to Classic View**) and run the **Local Security Policy** tool.
   - When configuring Windows Vista or later operating systems, select the view mode by category. In the **System and Security** section, select **Administrative tools** and run the **Local Security Policy** tool.

   > ⚠ To open the Local Security Policy tool, you can type `secpol.msc` in Windows Search and click ENTER.

2. Under the **Local Policies** node in the policy tree, select **Security Options**.
3. Right-click the **Sharing and security model for local accounts** policy, select **Properties** and then set the **Classic—local users authenticated as themselves** mode.

   > ⚠ By default, connection to a station can be established only if the used account has a nonblank password. To connect to the station, specify a nonblank password.

4. Close the console.

7. Configuring Active Directory Domain Controller

If your organization uses an Active Directory domain controller, configure:

- File and printer sharing options
- Security options

For that, you can create a new group policy object (GPO) or change the parameters of an already existing object.

To create a new group policy object

1. In the command prompt window, type `gpmc.msc` and run Group Policy Management Console (**GPMC**).
2. Create a new group policy object (for example, **GPO-KATANABUSINESSEDITION**). For that, in the **GPMC** console tree right-click **Group Policy Objects** in the forest and domain in which you want to create a new object (GPO). Click **New**. In the New GPO dialog box, specify a name for the new object, and then click **OK**.
3. Link the created object to the required domain.
4. Right-click the created object, select **Edit** and adjust the settings according to the description below.

If you decided not to create a new object and to adjust the parameters of an existing one, open the window with appropriate settings.

1. On a computer that has the Group Policy Management feature installed, click **Start** → **Administrative Tools** → **Group Policy Management**.
2. If the User Account Control dialog box appears, check the displayed data and click **Continue**.
3. In the navigation pane, expand **Forest: YourForestName**, then expand **Group Policy Objects** and right-click the GPO for which you want to create the rule.
4. On the open menu, click **Edit**.

Setting up file and printer sharing

Allow inbound requests from client computers. Enabling of this firewall exception rule opens UDP ports 137 and 138 as well as TCP port 445 to the IP addresses specified in the rule.

To allow file and printer sharing

1. In the navigation pane of the open window, expand the following: **Computer Configuration** → **Policies** → **Administrative Templates** → **Network** → **Network Connections** → **Windows Firewall** → **Domain Profile**.

2. In the details pane, double-click **Windows Firewall: Allow inbound file and printer sharing exception** and enable the rule.
3. In the **Allow unsolicited incoming messages from these IP addresses** text box, specify the required range of IP addresses.
4. Click **OK** to save the changes.

Configuring security options

Configure **Network access: Sharing and security model for local accounts policy** so as to allow local users to authenticate as themselves over network.

To allow users to authenticate as themselves over network

1. In the navigation pane of the open window, expand the following: **Computer Configuration** → **Policies** → **Windows Settings** → **Security Settings** → **Local Policies** → **Security Options**.
2. For **Network access: Sharing and security model for local accounts policy**, set the value to **Classic—local users authenticate as themselves**.

Applying configuration changes

To apply these changes in domain policies (regardless of whether a new Group Policy Object was created or an existing Group Policy Object was configured), open the command prompt window and enter the following command: `gpupdate/force`.

8. Searching for Stations and Installing Dr.Web KATANA

To start managing stations and set the security level for the stations, you should search for the stations and install Dr.Web KATANA.

> ⚠ Stations should be installed on the same network segment as Dr.Web KATANA Business Edition.

If you do not have enough privileges to access the network, you will see the corresponding warning. To install Dr.Web KATANA successfully on the stations, specify a username and a password to access the network in Settings or restart Dr.Web KATANA Business Edition with the administrator privileges. Otherwise, the installation of Dr.Web KATANA on stations may fail.

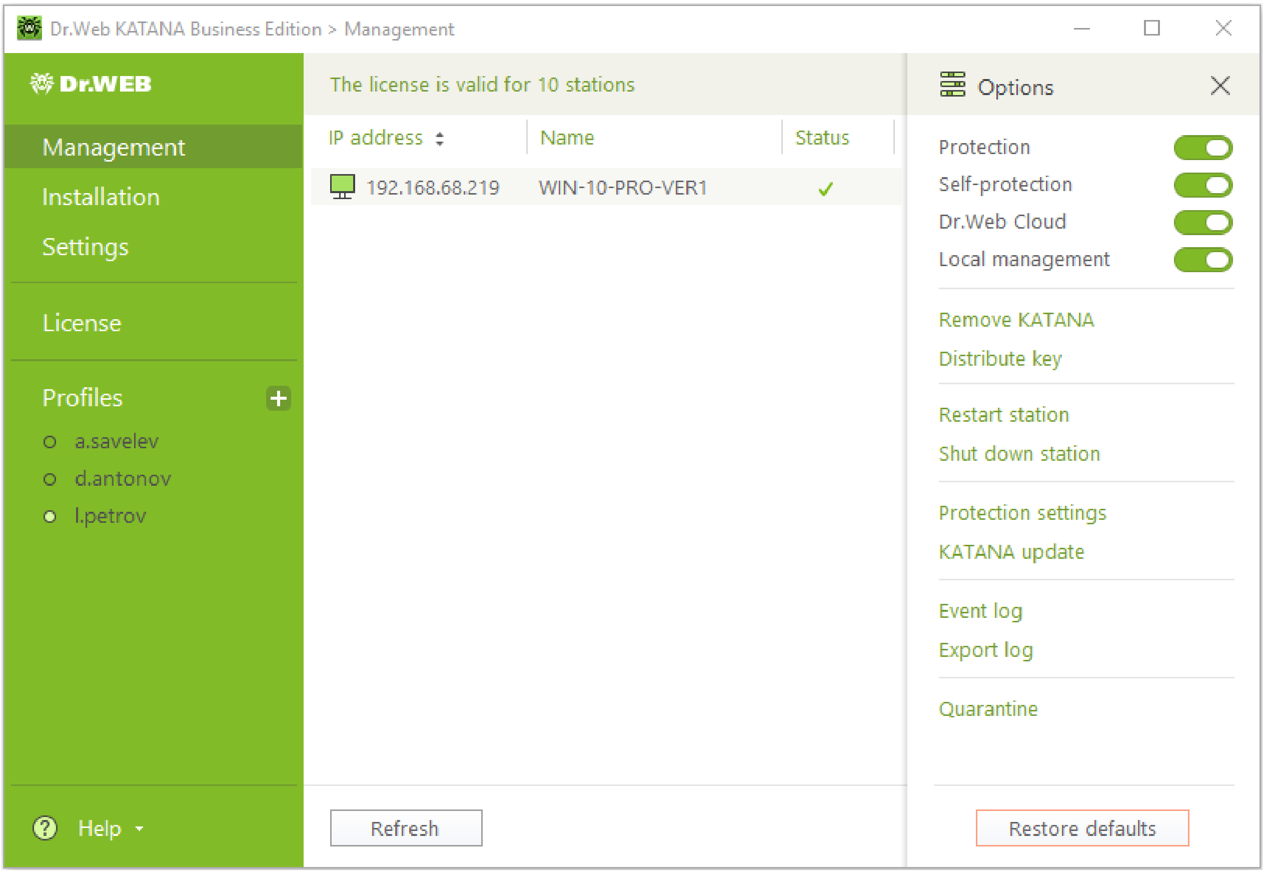
To search for stations and install Dr.Web KATANA

1. In the **Installation** section, click **Add stations**.
2. In the window of adding stations, select the station search mode:
   - Network discovery
   - Search Active Directory
   - Add stations manually (you can specify IP address of the station, its network name, an address range with a hyphen (“-”) or a mask).
3. Click **Search stations** to start searching for stations. Once all available stations are found, the search will stop automatically. You can stop the search by clicking **Stop searching**. At this, all stations that have already been found will remain in the list.
4. Once the search is finished, select the necessary stations on the list and click **Install KATANA**.
5. The Dr.Web KATANA Installation window opens. The window contains a list of the selected stations, which is stored in the **Installation** section until you restart Dr.Web KATANA Business Edition.

> ⚠ Dr.Web KATANA will be installed only on the number of stations allowed by the license.

Dr.Web KATANA is installed automatically. During the installation procedure, new stations are added to the list in the **Management** section. This section allows you to manage all stations from the list even if the installation was not completed yet on all stations. Other stations appear in **Management** automatically.

If any of the selected stations have a standalone version of Dr.Web KATANA installed, the program will not be reinstalled. These stations will automatically be added to the list of the **Management** section. To start managing these station, distribute the existing public key.



Dr.Web KATANA Business Edition > Management

The license is valid for 10 stations

IP address	Name	Status
192.168.68.219	WIN-10-PRO-VER1	✓

Options

- Protection: on
- Self-protection: on
- Dr.Web Cloud: on
- Local management: on

Figure 1. Managing stations

Stations list

The list in the **Installation** section contains three columns: **IP address**, **Name**, and **Status**. If necessary, you may sort the list by any column. The station icon in the **IP address** column displays the following installation states:

- 🟩—the installation is completed successfully.
- 🟦—Dr.Web KATANA is being installed normally.
- 🟥—the installation fails. To view more information about the error, double-click ⚠.

To filter stations on the list, select the relevant filtering parameter from the drop-down list at the bottom of the window.

Reinstall. Click this button to restart the installation procedure if installation of Dr.Web KATANA failed on one or several stations.

Add stations. Click this button to add new stations to the current ones.

If you face any difficulties during the installation of Dr.Web KATANA to the stations, you can always refer to the Help of the program. For that, click **Help** in the menu.

9. Managing Stations

In the **Management** section, you can manage settings of the stations on which Dr.Web KATANA is installed, adjust their protection level, and view status of the Dr.Web KATANA components on selected stations. You can start managing stations even if Dr.Web KATANA is still being installed on other stations. They will be added to the **Management** stations list automatically. To configure how stations will be displayed in the list, click ▽. To configure stations settings, click ☰.

Stations list

There are three columns in the list: **IP address**, **Name**, and **Status**. If necessary, you can sort the list by any column. The **IP address** column indicates the station status. The **Status** column contains information on Dr.Web KATANA operation on the station. You can see the following information in these columns:

IP address	Status
🖥—the station is available for managing.	Possible statuses 1. ✓ —the station is well-protected; 2. ⚠—the station is not fully protected for one of the following reasons: • Self-protection is disabled. • Preventive Protection is disabled. • Automatic update is disabled. • License is expired. • Restart of the station is required. Click ⚠ to view the Dr.Web KATANA operation status on the selected station. To securely protect the station, it is recommended that you enable all necessary components or restart the station if necessary.
🖥—the station is not available for managing.	⚠—the station is not protected because you did not distribute the new public key to the station (for details see Keys Management). **To distribute a new key** 1. Make sure that all the requirements from the Preparing Stations section are met. 2. Select one or several stations. 3. Open the **Options** sidebar and click **Distribute key**.

The list contains only the stations that are online. The list does not contain the stations that are offline or those that are restarting. Dr.Web KATANA Business Edition automatically updates the station list. If necessary, you can force the update by clicking **Refresh**.

9.1. Filter

To configure filter settings for the station list, click ▽. The station list is changed automatically depending on the selected parameters. After closing the sidebar, the specified parameters are saved until you exit the program.

9.2. Options

Click ☰ to open the sidebar where you can change settings of the selected stations. After closing the sidebar, the specified parameters are saved. Some settings can be applied to several stations at a time.

Protection Settings for Stations

- **Protection**. Enable or disable Dr.Web KATANA protection on the station. This setting can be applied only to one station.
- **Self-protection**. Enable or disable protection of Dr.Web KATANA files and processes on the selected station from unauthorized access or from accidental damage. This setting can be applied only to one station.
- **Dr.Web Cloud**. Allow or disallow the connection to Doctor Web cloud service and to Dr.Web quality improvement program. Dr.Web Cloud provides most recent information on threats which is updated on Doctor Web servers in real-time mode and used for anti-virus protection. This setting can be applied only to one station.
- **Local management**. Allow or disallow the local management of Dr.Web KATANA. If this option is disabled, a user cannot manage Dr.Web KATANA settings, as they are inactive. This setting can be applied only to one station.

Additional Protection Settings for Stations

- **Remove KATANA**. Remove Dr.Web KATANA from one or several selected stations.
- **Distribute key**. Distribute the new public key to one or several selected stations.
- **Protection Settings**. Configure Dr.Web KATANA reaction to such actions of other programs that can compromise security of the selected station, and adjust protection level against exploits. This setting can be applied only to one station.
- **KATANA update**. Specify Dr.Web KATANA update options on the selected station. This setting can be applied only to one station.
- **Quarantine**. View information on the Quarantine component of the station which serves for isolation of files that are suspected to be malicious. This setting can be applied only to one station.

Operation Settings for Stations

- **Restart station**. Restart one or several selected stations.

- **Shut down station**. Shut down one or several selected stations.

Even Log Settings

- **Event Log**. Open detailed information about Dr.Web KATANA operation on the selected station. This setting can be applied only to one station.
- **Export log**. Save the event log for one or several stations.

9.2.1. Distributing Keys

Once new encryption keys are created or imported to Settings, you should send them to stations. Otherwise, you will not be able to manage the stations.

> ⚠ You cannot manage stations with new encryption keys via profiles that use the old encryption key.

To send new encryption keys

1. Make sure that all the requirements from the Preparing Stations section are met.
2. Select one or more stations with an active license.
3. Click **Distribute key**.

9.2.2. Shutting down and Restarting Stations

To restart or shut down stations

1. Select one or more stations with an active license.
2. Click **Restart station** or **Shut down station**.
3. In the opened window select the time when stations are restarted or shut down.
4. If necessary, add the message which is displayed to a station user before a selected action is applied, in the **Message** field.

9.2.3. Updating Dr.Web KATANA

Update frequency. Specify the frequency to check for Dr.Web KATANA updates. The default value (30 minutes) is optimal to keep information on threats up to date.

Use proxy server. Enable this option if you want to use the proxy server for updating Dr.Web KATANA and specify the connection settings.

Option	Description
Address	Specify the address of the proxy server.
Port	Specify the port of the proxy server.
Username	Specify the username to use when connecting to the proxy server.
Password	Specify the password for the profile that is used for connection to the proxy server.
Authorization type	Select an authorization type required to connect to the proxy server.

9.2.4. Event Log

This window provides a detailed information about the Dr.Web KATANA operation on a selected station. The event log contains the data about status of the Dr.Web KATANA components. Errors and warnings during the program operation are also recorded here.

Filter

To configure filter settings for events, click ▽. The events list is changed automatically depending on the selected parameters. After closing the sidebar, the specified parameters are saved until you exit the program.

Options

Click ☰ to open a sidebar where you can configure the following advanced settings of the event log:

- **Show details**. If the option is enabled, detailed information on a selected event will be displayed in an additional window. The option is enabled by default.
- **Export log**. Click this button to save the event log for the selected station. In the opened window, select the file format, parameters for event filtering, and the path to save the file.
- **Clear log**. Select this option to remove all event records on a selected station.

9.2.5. Exporting Log

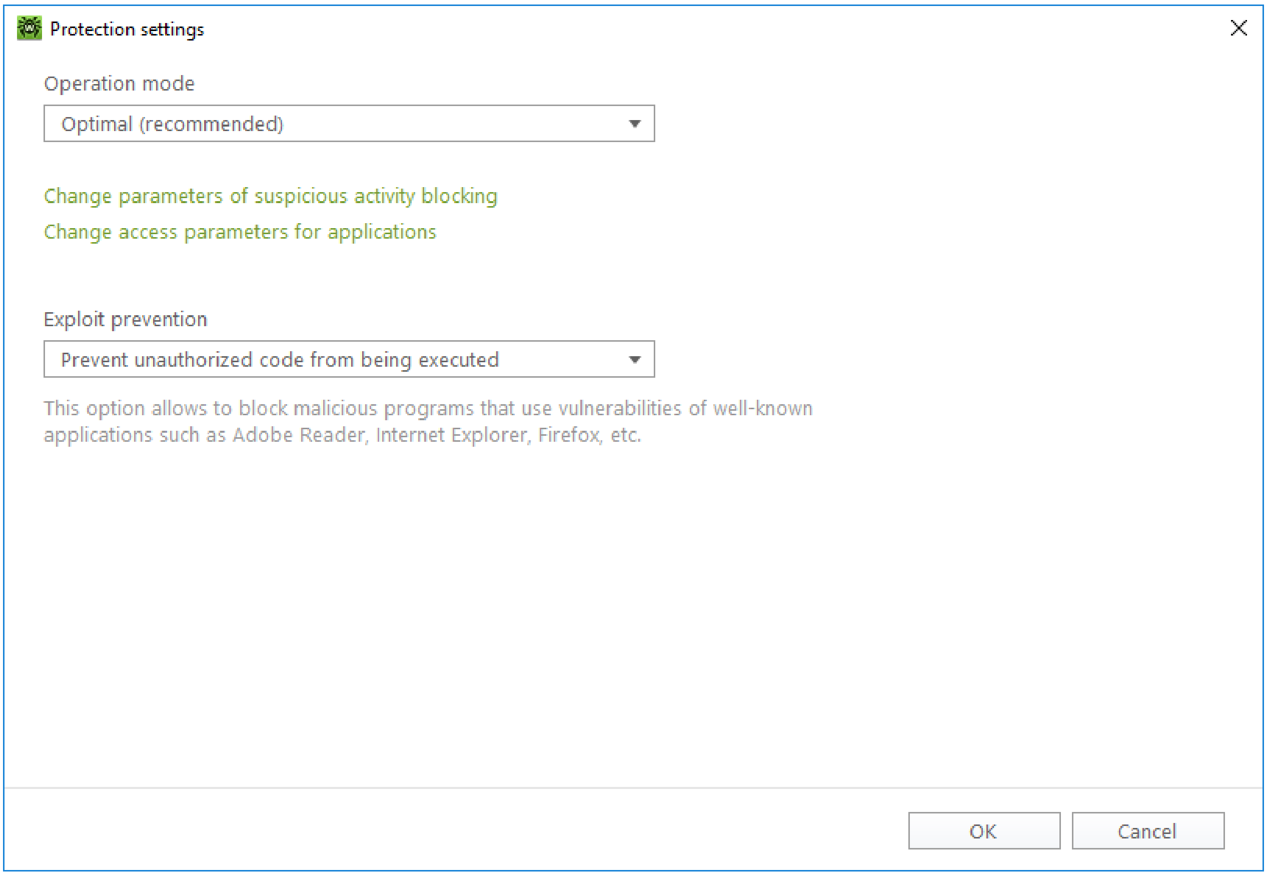
To export event log

1. Select stations for which you want to export the event log and click **Export log**.
2. In the open window, select the file format, the type of the events, and the period when these events occur. Specify also the path to save the log file.

If you want to save the log file only for one station and you previously specified the filter parameters for this station in the setting window of the file log, these parameters will be saved.

9.2.6. Protection Settings

In this window, you can configure Dr.Web KATANA reaction to such actions of other programs, which can compromise security of a station, and select a level of protection against exploits.



Protection settings

Operation mode

Optimal (recommended)

Change parameters of suspicious activity blocking

Change access parameters for applications

Exploit prevention

Prevent unauthorized code from being executed

This option allows to block malicious programs that use vulnerabilities of well-known applications such as Adobe Reader, Internet Explorer, Firefox, etc.

Figure 2. Protection settings

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.

To configure the general mode of preventive protection, select it from the **Operation mode** list or click **Change parameters of suspicious activity blocking**. As a result of the second action, a window opens providing you with mode settings and editing options. All changes are saved in the **User-defined** mode. In this window, you can also create a new profile for saving necessary settings.

Preventive Protection Level

In the **Optimal** mode, Dr.Web disables automatic changes of system objects whose modification explicitly signifies a malicious attempt to harm the operating system. It also blocks low-level access to the disk and protects the HOSTS file from modification.

If there is a high risk of your computer getting infected, you can increase protection by selecting the **Medium** mode. In this mode, access to the critical objects, which can be potentially used by malicious software, is blocked.

> ⚠ Using this mode may lead to compatibility problems with a third-party software that uses the protected registry branches.

When total control of access to critical Windows objects is required, you can select the **Paranoid** mode. In this mode, Dr.Web also provides you with interactive control over loading of drivers and automatic running of programs.

The **User-defined** mode allows you to set a custom protection level for various objects.

Protected object	**Description**
Integrity of running applications	This option allows detection of processes that inject their code into running applications. It indicates that the process may compromise computer security.
Integrity of users files	This option allows detection of processes that modify user files with the known algorithm, which indicates that the process may compromise computer security.
HOSTS file	The operating system uses the HOSTS file when connecting to the Internet. Changes to this file may indicate virus infection.
Low level disk access	Block applications from writing on disks by sectors while avoiding the file system.
Drivers loading	Block applications from loading new or unknown drivers.
Critical Windows objects	Other options allow protection of the following registry branches from modification (in the system profile as well as in all user profiles). 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 registry keys: • Software\Microsoft\Windows NT\CurrentVersion\Winlogon, Userinit, Shell, UIHost, System, Taskman, GinaDLL Winlogon notifiers: • Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify

Protected object	Description
	Windows registry startup keys: • Software\Microsoft\Windows NT\CurrentVersion\Windows, AppInit_DLLs, LoadAppInit_DLLs, Load, Run, IconServiceLib Executable file associations: • Software\Classes\.exe, .pif, .com, .bat, .cmd, .scr, .lnk (keys) • Software\Classes\exefile, piffile, comfile, batfile, cmdfile, scrfile, lnkfile (keys) Software Restriction Policies (SRP): • Software\Policies\Microsoft\Windows\Safer Browser Helper Objects for Internet Explorer (BHO): • Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects Autorun of programs: • 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 Autorun of policies: • Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run Safe mode configuration: • SYSTEM\ControlSetXXX\Control\SafeBoot\Minimal • SYSTEM\ControlSetXXX\Control\SafeBoot\Network Session Manager parameters: • System\ControlSetXXX\Control\Session Manager\SubSystems, Windows System services: • System\CurrentControlXXX\Services

> If any problems occur during installation of important Microsoft updates or during installation and operation of programs (including defragmentation programs), temporarily disable Preventive Protection.

Exploit prevention

This option allows to block 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	An attempt of a malicious object to exploit software vulnerabilities to get access to critical areas of the operating system will be allowed automatically.

9.2.7. Quarantine

This window contains information on the Quarantine component that serves to isolate files. The quarantine contains backup copies of objects created before they are deleted by Dr.Web. The quarantine stores malicious programs that are identified by Dr.Web Process Heuristic as programs that modify user files (for example, encryption ransomware), and programs that inject their code into the processes of other applications.

The central table displays the following information on quarantined objects:

- **Object**—name of the quarantined object;
- **Threat**—malware class of the object determined by Dr.Web when the object is quarantined.
- **Date Added**—the date when the object was moved to Quarantine.
- **Path**—full path to the previous location of the object.

Working with quarantined objects

The following buttons are available:

- **Download**—download the selected object from stations to the network administrator’s computer.
- **Restore**—move the selected object to the original folder on the station;

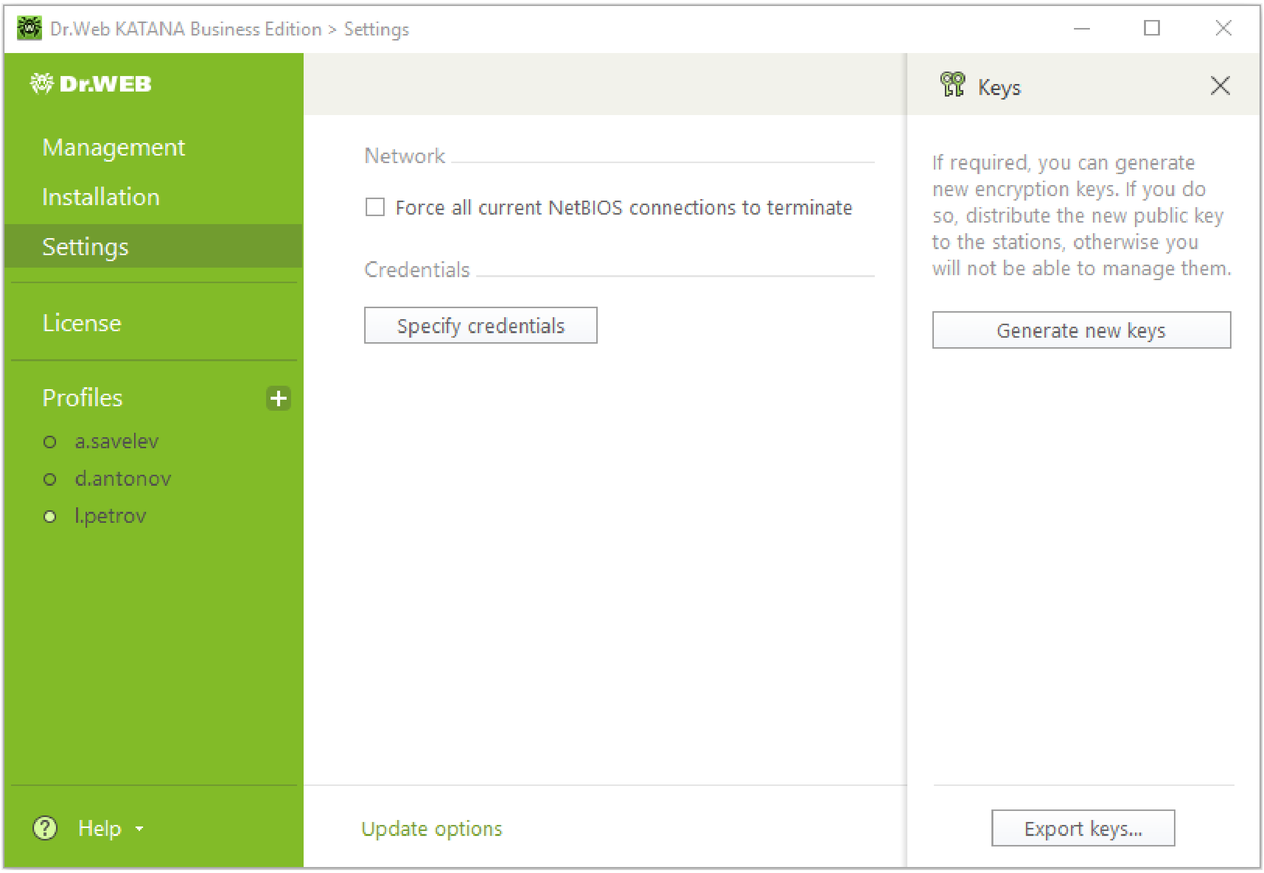
> Use this option only when you are sure that the selected object is safe.

- **Delete**—delete one or several objects from quarantine and from the system.
- **Clear quarantine**—delete all quarantined objects.

10. Settings

In the **Settings** section, you can manage the Dr.Web KATANA Business Edition settings and settings related to interaction between the administrator computer and the stations on which Dr.Web KATANA has been installed. You can configure the following settings:

- Program language;
- Key management;
- Network interaction;
- Parameters of the network access;
- Update of Dr.Web KATANA Business Edition.



□ Force all current NetBIOS connections to terminate

If required, you can generate new encryption keys. If you do so, distribute the new public key to the stations, otherwise you will not be able to manage them.

Figure 3. Settings

All modified settings will be applied to the current session. You can save them to the current profile when closing the program or changing the profile.

If you face any difficulties while changing the settings of Dr.Web KATANA Business Edition, you can always refer to the Help. For that, click **Help** in the menu.

10.1. Program Language

To set another program language, select it from the corresponding drop-down list by clicking 🌐 New languages are automatically added to the list. Thus, it contains all localization languages that are currently available for the Dr.Web graphical interface.

10.2. Key Management

If required, you can export existing encryption keys or generate new ones.

To create new keys

1. In the **Settings** section, click 🔑.
2. In the open sidebar, click the **Generate both encryption keys automatically** button.
3. When new keys are generated, distribute them to the station in the **Management** section by using the **Options** sidebar.

> ⚠ You cannot continue managing the stations until you distribute the new public key. For these stations, the status ⚠ will be specified in the **Management** section.

To export existing keys

1. In the **Settings** section, click 🔑.
2. In the open sidebar, click the **Export keys** button.
3. Choose a folder to save the encryption keys.

10.3. Network Communication Settings

If required, you can manage network communication between the administrator's computer and stations. Select the **Force all current NetBIOS connections to terminate** mode to terminate all existing NetBIOS connections with stations, including ones with opened files and running processes, before the installation procedure. This is required to copy files and to run Dr.Web KATANA.

10.4. Configuring Access Settings

If you do not have privileges to access the network, you will see the corresponding warning in **Installation**. Specify the username and the password by clicking **Specify credentials** in the **Settings** section, so that Dr.Web KATANA is successfully installed. You can create a new account or delete the current one.

- To create a new user account, enter a username and a password. Click **Add**. The user account will be added to the list.
- To delete the existing user account, mouse over it on the list and click ☒.

Note that the administrator cannot view passwords of the user accounts.

10.5. Dr.Web KATANA Business Edition Update

To change the update options for Dr.Web KATANA Business Edition, go to the **Settings** section and click **Update options**.

Automatic update of the program

If the **Check for updates automatically** option is enabled, Dr.Web KATANA Business Edition checks for available updates and downloads them. At this, in the menu next to the name of the **Help** section, the ⬇ image appears. Restart Dr.Web KATANA Business Edition to complete the update the program. For this, do the following:

1. In the drop-down menu of the **Help** section, select **About**.
2. In the open window, click **Restart to update**.

Manual update of the program

If the **Check for updates automatically** option is disabled, you need to update Dr.Web KATANA Business Edition manually. To update the program, do the following:

1. In the drop-down menu of the **Help** section, select **About**, then click **Check for updates**. If there are available updates, the program starts downloading them.
2. Restart Dr.Web KATANA Business Edition to complete the update procedure. For this, do the following:
   a) In the drop-down menu of the **Help** section, select **About**.
   b) In the open window, click **Restart to update**.

Update options

If necessary, you can select one of the following modes to update Dr.Web KATANA Business Edition:

- **Use HTTPS connections**—enable this option to download updates via a secure protocol.

- **Use proxy server**—enable this option if you want to use the proxy server. Specify the connection settings:

Option	Description
Address	Specify the address of the proxy server.
Port	Specify the port of the proxy server.
Username	Specify the username to use when connecting to the proxy server.
Password	Specify the password for the profile that is used for connection to the proxy server.
Authorization type	Select an authorization type required to connect to the proxy server.

11. License Management

In the **License** section, you can view information about your current license for Dr.Web KATANA Business Edition.

In some situations, for example, when the license expires or you want to install Dr.Web KATANA to more stations, you may need to purchase a new Dr.Web license. In this section you can change you current license with a new one.

To change the license

1. Click **Change license**.
2. In the open window, specify the path to a new valid key file.

> ⚠ Once you add a new license, the program will distribute it automatically to stations where Dr.Web KATANA is installed. At this, you do not need to reinstall or interrupt Dr.Web KATANA Business Edition and Dr.Web KATANA on the stations.

The My Dr.Web link opens your personal page of the Doctor Web official website in the default Internet browser. This page provides you with information on your license, including usage period and serial number, and allows to renew the license, contact technical support, and so on.

The License Agreement link opens the license agreement on the Doctor Web official website.

12. Appendix A. Detection Methods

Dr.Web KATANA uses technologies for blocking malicious processes by analyzing their behavior.

The behavior analysis technology Dr.Web Process Heuristic protects systems against new and highly prolific malicious programs that are capable of avoiding detection by traditional signature-based analysis and heuristic mechanisms.

Dr.Web Process Heuristic analyzes the behavior of each running program in real time by comparing it with Dr.Web Cloud which is constantly updated. It determines whether the program is dangerous and then takes whatever measures are necessary to neutralize the threat.

This data protection technology helps minimize losses resulting from the actions of unknown malware—and consumes very few of the protected system resources.

Dr.Web Process Heuristic monitors any attempts to modify the system:

- Detects malicious processes that modify files (such as encryption ransomware)
- Prevents malware from injecting its code into the processes of other applications
- Protects critical system areas from being modified by malware
- Detects and stops the execution of malicious, suspicious or unreliable scripts and processes
- Prevents malware from modifying boot sectors so that malicious code cannot be executed on the computer
- Blocks changes in the Windows Registry to make sure that the safe mode will not be disabled
- Prevents malware from changing launch permissions
- Prevents new or unknown drivers from being downloaded without the user’s consent
- Prevents malware and certain other applications, such as anti-antiviruses, from adding their entries to the Windows Registry, so that they could be launched automatically
- Locks registry branches containing information about virtual device drivers, ensuring that no malicious programs will be installed as new virtual devices
- Prevents malware from disrupting system routines

Dr.Web Process Heuristic includes the Dr.Web ShellGuard technology which protects system from programs that exploit vulnerabilities. Exploits are malicious objects that take advantage of software flaws to gain control over a targeted application or the operating system.

Dr.Web ShellGuard protects common applications installed on computers running Windows:

- Web browsers (Internet Explorer, Mozilla Firefox, Google Chrome, and Vivaldi Browser)
- MS Office applications including MS Office 2016
- System applications
- Applications that use java, flash and pdf

- Media players (software)

Updating from the cloud for non-signature Dr.Web ShellGuard blocking routines

To detect malicious actions, Dr.Web ShellGuard uses information stored by the anti-virus locally as well as reputation data from Dr.Web Cloud which includes:

- Information about the routines used by programs with malicious intentions
- Information about files that are 100% clean
- Information about the compromised digital signatures of well-known software developers
- Information about digital signatures used by adware and riskware
- Protection routines used by specific applications