Dr.WEB

CureNet!

Administrator Manual

Trademarks

Disclaimer

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

Dr.Web CureNet!
Version 11.0.0
Administrator Manual
4/12/2024

Doctor Web Head Office

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

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

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

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

Doctor Web

Doctor Web develops and distributes Dr.Web information security solutions that provide effective protection against malicious software and spam.

Doctor Web customers include home users around the world, government agencies, small businesses, and nationwide corporations.

Since 1992, Dr.Web anti-virus solutions have been known for their continuous excellence in malware detection and compliance with international information security standards.

The state certificates and awards received by Dr.Web solutions, as well as the worldwide use of our products, are the best evidence of exceptional trust in the company products.

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

Table of Contents

1. Document Conventions

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

Convention	Comment
⚠	A warning about possible errors or important notes that require special attention.
Anti-virus network	A new term or an emphasis on a term in descriptions.
<IP-address>	Placeholders.
Save	Names of buttons, windows, menu items and other program interface elements.
CTRL	Names of keyboard keys.
`C:\Windows\`	Names of files and folders, code examples.
Appendix A	Cross-references to document chapters or internal hyperlinks to webpages.

2. Dr.Web CureNet!

Dr.Web is intended to provide anti-virus scans for computers and servers running Windows operating systems and being on the same network as your computer. The product does not require installation. It runs scanning and cures detected malicious objects even if anti-virus software from other developers is installed on scanned computers (hereinafter stations). Scanning speed and statistics gathering is independent of network load or availability of specific servers and services. Dr.Web CureNet! can be even used to scan stations which have no access to the Internet.

Dr.Web provides you with the following advantages:

- Centralized anti-virus scanning of local network stations running Windows.
- Centralized management of reaction on detection of virus threats.
- Infected objects recovery.
- Anti-virus checks for mail files, archives, and file containers.
- Regular updates to Dr.Web virus databases and Dr.Web components.
- High scanning speed.
- Statistics gathering and reporting to your computer.
- Dr.Web report in XML or CSV.

2.1. System Requirements

System Requirements for administrator’s computer

Dr.Web CureNet! can be installed and run on a computer that meets the following requirements:

Specification	Requirement
OS	• Windows XP Professional with Service Pack 2 or later • Windows Server 2003 with Service Pack 1 or later • Windows Vista (Business, Enterprise, or Ultimate edition) with Service Pack 1 or later • Windows Server 2008 • Windows 7 (Professional, Enterprise, or Ultimate edition) • Windows Server 2008 with Service Pack 2 • Windows 8 and 8.1 (Professional or Enterprise edition) • Windows Server 2012 • Windows 10

Specification	Requirement
Hard disk space	200 MB of disk space.
Free RAM	Minimum 360 MB of RAM.
CPU	i686-compatible processor and SSE2 instruction set.
Other	Internet connection to update virus databases and Dr.Web components. TCP/IP connection to all stations to be checked.

System requirements for the stations

System requirements for stations are the same as for the administrator’s computer, where Administrative Console is started, except for the following:

- **Operating systems:** Windows XP Professional SP2 and later operating systems, except the following versions for 64-bit platforms: Windows Server 2003 x64 Edition and Windows XP Professional SP2 x64 Edition.
- **Other:** Internet connection is not required.

2.2. Preparing Stations

To scan stations using Dr.Web, review the following requirements:

- **Network Discovery** must be turned on the computer with Administrative Console, 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 Advanced Settings).

Before starting anti-virus scans, ensure you have user names and passwords of administrative accounts on all stations you want to scan.

> Preparation of a remote operating system to use Dr.Web CureNet! must be performed under an administrative account.

Advanced Settings

To scan stations using Dr.Web review the following 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 older 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 Microsoft Windows Server 2008, Windows 7, Windows 8, Windows 10, or Microsoft Windows Server 2012 select **Turn on network discovery** and **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 older 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 authenticate as themselves mode**.

> ⚠ By default, connection to a station cannot be established if the used account has a blank password. To connect, set a nonblank password.

4. Close the console.

2.3. 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-CureNet**). 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**.

2.4. Licensing

Obtaining license

To take advantage of Dr.Web, you need a license that allows full use of all program features. You can obtain a license on the official website of Doctor Web. The license has two restrictions: validity period and the number of stations allowed for simultaneous anti-virus scanning. The use rights for the product are regulated by a key file. To view the restrictions of your license, click **Help** and select **About**.

The key file has the .key extension and contains the following information:

- Licensed period for the product
- List of licensed anti-virus components
- Subscription period when the product may be updated
- Other restrictions (for example, the number of stations allowed for simultaneous anti-virus check)

The key file should be located in the Dr.Web folder where you extract program files. If Dr.Web finds several license key files, it automatically chooses the one which allows to perform a requested operation. Details on license usage are saved to the log file **CureNet.log**.

Changing license parameters

If required, you can expand the allowed number of stations or extend the license validity period. For that purpose

1. Start Administrative Console.
2. On the first page, click **My Dr.Web**, or on any other page, click **Help** and select **My Dr.Web**.

   This opens your personal page on the Dr.Web official website with the default Internet browser. There you can change parameters of your license, as well as check all required information about it or send a request to the technical support service.
3. Once your license is valid, you can download the latest version of the Dr.Web distributive package which contains your renewed license.

Getting demo

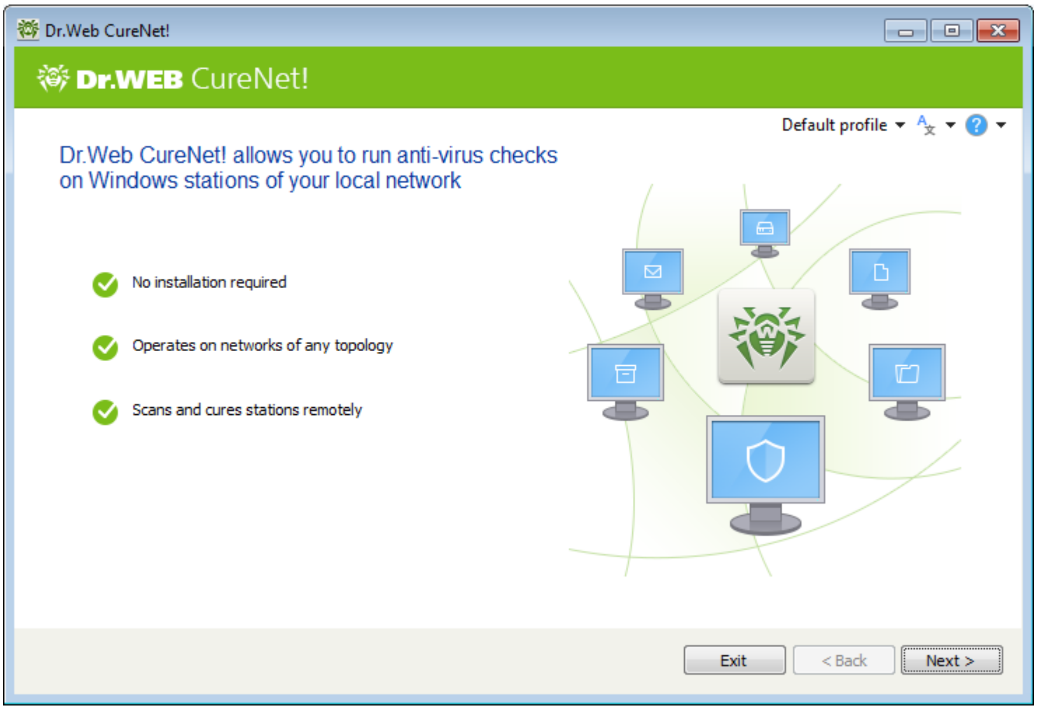
If you want to evaluate the product before purchasing it, you can activate a demo period. To do that, fill in a special form on the company official website. Dr.Web CureNet! demo version does not provide recovery, but you can see how the scan procedures are deployed on stations, scan the stations for information security threats and get report of detected (but not yet cured) viruses and malicious software. To recover stations, you need to purchase a commercial license.

3. Starting Dr.Web

Dr.Web does not require installation on scanned stations. To start using the application and run anti-virus scans, do the following:

- Copy the Dr.Web distributive package to your computer and run it. This extracts the application files to the Dr.Web folder, automatically creates Dr.Web repository, and starts Administrative Console.
- Ensure accessibility of stations you want to scan.
- Ensure that stations are prepared for scanning.

Administrative Console starts automatically when you run the Dr.Web distributive package.



Dr.Web CureNet! allows you to run anti-virus checks on Windows stations of your local network

✓ No installation required

✓ Operates on networks of any topology

✓ Scans and cures stations remotely

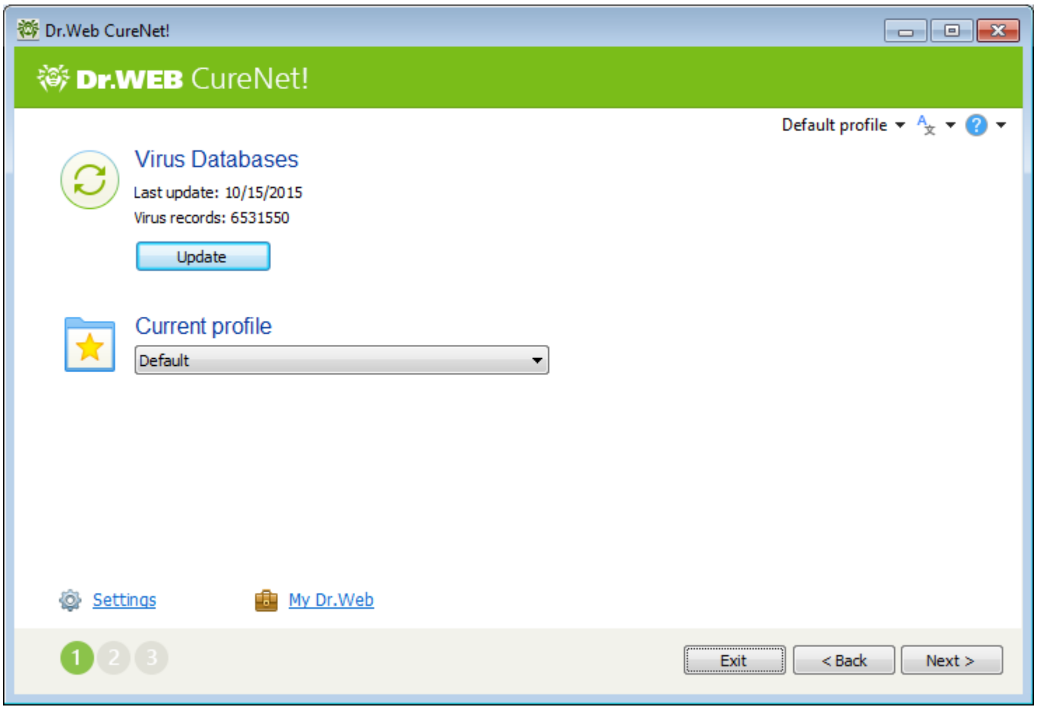
Picture 1. Dr.Web Administrative Console.

4. Updating

It is strongly recommended to install all updates released by Doctor Web. With the updates of the virus databases, Dr.Web CureNet! for iOS can detect new viruses, block their spreading and sometimes cure infected files which were incurable before. From time to time, updates also include enhancements to anti-virus algorithms in executable files and software libraries. Dr.Web anti-virus operation experience helps to fix bugs in software, update the support service and documentation.

Dr.Web is a tool for centralized scanning, therefore all files necessary for scanning are deployed on selected stations when you start anti-virus scans. To use the latest virus databases on all remote computers, you need to keep just the central Dr.Web repository up-to-date. When Dr.Web virus databases become considerably outdated, Administrative Console displays an appropriate warning.

Dr.Web repository cannot be created or updated manually.



Virus Databases

Last update: 10/15/2015

Virus records: 6531550

Current profile: Default

Picture 2. Updating Dr.Web.

Internet connection is required for an update.

To update Dr.Web CureNet! repository

1. Dr.Web checks whether a key file is blocked at the Doctor Web website. If your key file is blocked due to misuse, the program displays an appropriate warning, terminates the

update, and blocks the components. In this case, purchase a license or contact Doctor Web technical support.

2. If a valid key file is found, updating is started and Dr.Web downloads all updated files that correspond to your program version. Wait until the process finishes.

Administrative Console and other program components can be updated with updating Dr.Web repository or distributive package. When updating the repository, Dr.Web checks for a new version of the console. If there is a newer version, the user will be prompt to restart the program to update the Administrative Console. Otherwise, the console will be update with the next launch of the program.

Note that the key file is not downloaded if you update the console in such a way. To update the license in the program, update the distributive package via My Dr.Web.

To update Dr.Web distributive package via My Dr.Web

> ⚠ During the licensed period, you may update the Dr.Web distributive package without limit.

1. Start Administrative Console.
2. On the profiles page, click **My Dr.Web**, or on any other page, click **Help** ❓ ▾ and select **My Dr.Web**.

   This opens your personal portal on the official Doctor Web website with the default Internet browser. From this page, you can download the latest version of the Dr.Web distributive package provided that you license has not expired, or renew you license.
3. Save the updated Dr.Web distributive package.
4. To extract files and start the updated Administrative Console, run the Dr.Web distributive package.

5. Dr.Web Functions

You can configure operation of Dr.Web using Administrative Console.

> ⚠ To ensure complete scanning using Dr.Web, we recommend to manually disable Automatic Windows Updates during anti-virus scans.

Getting Started

1. Start Administrative Console and click **Next**.
2. In the open windows, select the required profile.
3. When Dr.Web virus databases become considerably outdated, Administrative Console displays an appropriate warning. In this case, it is strongly recommended to start an update by clicking the **Update** button. Click **Next** to proceed.
4. Select stations for scanning. Configure accounts for Dr.Web to use when connecting to the selected stations. Click **Next**. The page for selection an operating mode appears.

You can add new stations later: during scanning or when working with quarantine.

Scanning procedure

1. Specify one of the scanning modes.
2. By clicking **Settings**, you can view and, if required, adjust the following parameters of Dr.Web Scanner operation:
   - General settings of Dr.Web scans on stations such as notification of remote users and restart options
   - Types of objects (archives and containers) to scan for viruses
   - Actions to perform to neutralize virus threats
   - Network settings during anti-virus scans and check of station availability before deploying Dr.Web files
   - Network connection parameters to use when updating Dr.Web repository
3. To start scanning, click **Start**.

During scanning, you can add other stations to scan, as well as suspend, resume, or stop the process for any station. For that, right-click the station name in the table and select the required action on the open shortcut menu.

Note the following issues:

- Some actions (modification of registry keys or files used by other Windows applications, etc.) cannot be executed immediately on detection of a virus threat. Dr.Web Scanner marks the corresponding objects as requiring actions after system restart and displays appropriate information in the report. To neutralize such threats, enable Dr.Web Scanner to automatically reboot if necessary or shutdown stations once the anti-virus scan completes. Users of the station will be provided with appropriate warnings and a short period of time to complete current tasks and save information. For details on how to configure actions upon malicious objects, refer to Advanced Settings.

- When a virus threat is detected in the master boot record (MBR), Dr.Web Scanner terminates the anti-virus scan and reboots the station immediately to avert the threat. In such cases, stations are restarted regardless of whether the option to **Restart station** after curing is enabled or not.

Anti-virus scans of stations run independently of Administrative Console. To exit Administrative Console, click **Exit**. Scanning on the station will continue, but statistics will not be available.

Viewing scan results

Dr.Web report reflects progress of the anti-virus scans and their results. If necessary, you can export the report in CSV or XML.

You can also view details on scanning of a particular station.

Working with quarantine

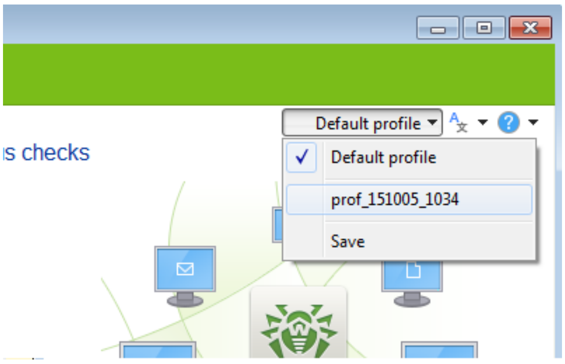
1. On the page where you can specify operation mode, select **Quarantine Manager**.
2. Click **Start**.
3. The Quarantine Manager window opens, where you can view information about quarantine on every selected station, restore quarantine objects to a selected folder, remove them, or download to your computer.

5.1. Profiles

Dr.Web allows you to save all scan settings in profile files: program language, list of stations to scan, credentials required to access selected stations, reaction of Dr.Web Scanner on threat detection and other parameters.

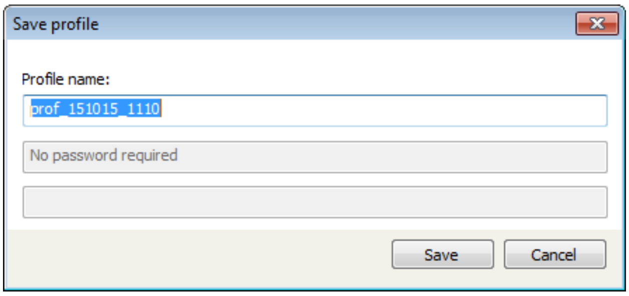
To create a new profile

1. Click the profile name in the top part of any page (by default, **Default profile**) and select **Save**.
2. In the open window, enter the name for the profile and, if necessary, the password to use when accessing it. Access password is required only when you save connection passwords in the profile.



Picture 3. Profiles

3. Click **Save**.
4. Proceed to the following pages or click **Exit**.


Save profile

Profile name:

prof_151015_1110

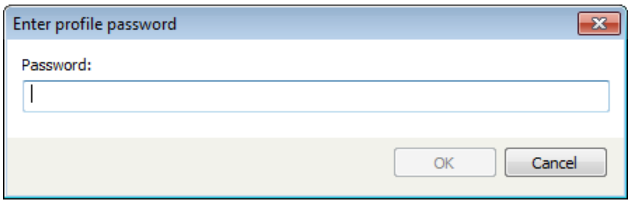
No password required

Profile 4. Save profile.

Administrative Console does not save changes in scan settings automatically. To preserve modifications to the profile, save the profile under the same name again.

To log in to the existing profile

1. In any step prior to selecting actions, click the profile name in the top part of a page (by default, **Default profile**) and select the profile to use. On the update page, you can also select the profile to use in the main window of Administrative Console.
2. If required, enter the access password for the profile.


Enter profile password

Password:

Picture 5. Accessing profile.

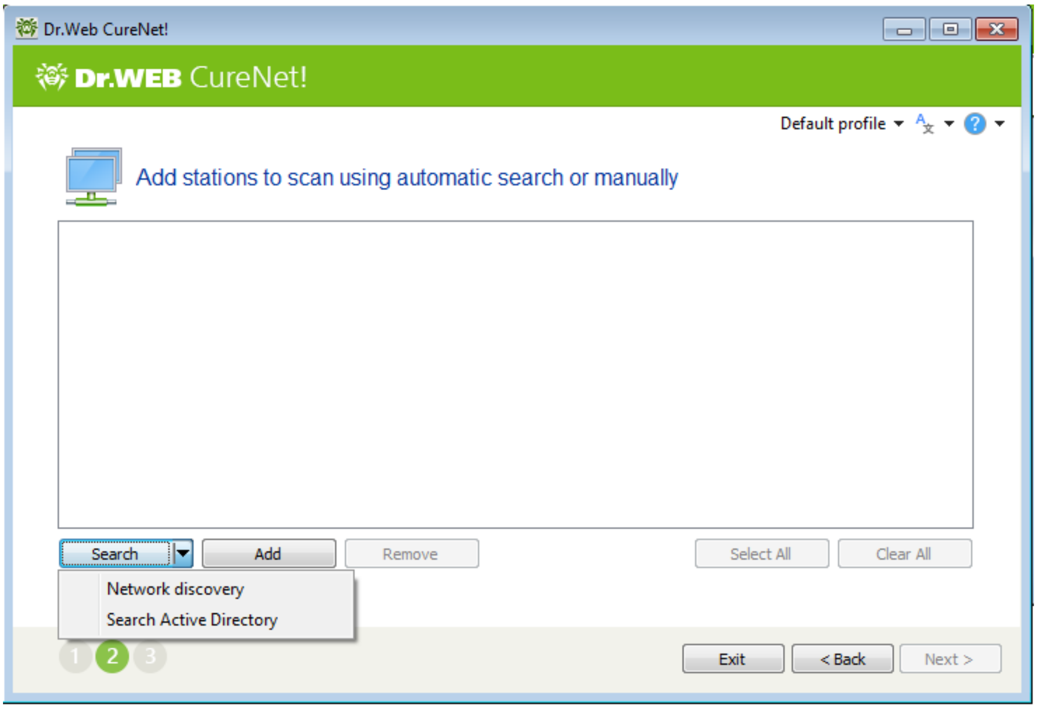
3. Administrative Console configures all scan settings according to the information in the selected profile. If necessary, proceed to the following pages and modify scan settings.

To delete a profile

You cannot delete profiles using Dr.Web. To do it, delete an XML file with the profile name in the Profiles subfolder of the Dr.Web folder.

5.2. Selecting Stations

This page helps you to compose the list of stations to scan or to view their quarantined objects and configure access parameters.



Picture 6. Selecting stations.

Dr.Web allows to add stations manually or using automatic search on all networks available for the computer where Administrative Console is running.

Dr.Web detects only those networks and stations that are visible under the account used by Administrative Console.

Automatic search

1. Click **Search** and select the required search mode.

   If your organization uses an Active Directory domain controller, it is recommended to select **Search Active Directory**. In this case, stations will be found for a shorter time period and the list will display all stations, even those that are shut down.

If you select the **Network discovery** option, the full search may take considerable time. At any time, you can click **Stop Searching**. All found stations will be added to the station list. If a required station was not found, add it manually.

2. Select stations to scan:
   - To add a station, select the check box next to the appropriate item in the list.
   - To add all listed stations, click **Select All**.
   - To deselect all stations, click **Clear All**.

To add stations manually

1. To add one or several stations, click **Add**.
2. In the **Add stations** window, enter one of the following values:
   - IP address or network name of the station
   - A range of IP addresses with a hyphen ('-') or using masks (for details, see Appendix C. Network Masks).

> ⚠ When adding a station to the list, make sure that the specified IP address is not a broadcast address (reserved for sending information to all hosts on the given network).

3. Click **OK**.
4. Stations added manually are automatically selected for further operation. To exclude stations from the list, clear the corresponding check boxes.
5. After you make your selection, configure accounts for Dr.Web for connection to the selected stations. By default, the account running Administrative Console is used. If Dr.Web cannot connect to a station using the default account, listed accounts are used in consecutive order.

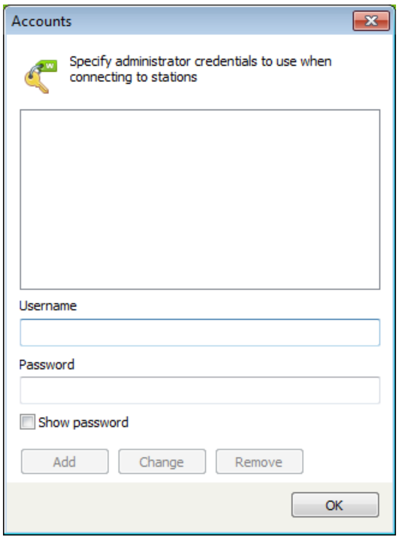
To remove a station from the list

1. Select the stations you want to remove from the list. To make quick selection of all stations, click the corresponding group name.
2. Click **Remove**.

After you make your selection, configure accounts for Dr.Web for connection to the selected stations. By default, the account running Administrative Console is used. If Dr.Web cannot connect to a station using the default account, listed accounts are used in consecutive order.

Configure Accounts

1. To configure or display the account list, click **Credentials**. The **Accounts** window displays.


Accounts
Specify administrator credentials to use when connecting to stations
Username
Password
☐ Show password
Add
Change
Remove
OK

Picture 7. Account management.

2. Edit the list. When adding an account, note important aspects:
   - Username must be entered in one of the following formats:

     *<domain>**<username>*, where *<domain>* is the name of the network domain with the account.

     *<station>**<username>*, where *<station>* is the network name of the computer with the account.
   - If all stations that you want to add reside outside domains and have identical administrative accounts, you may speed up scanning by adding to the list one common account only and omitting station names. Dr.Web will try to connect to all stations using this account.

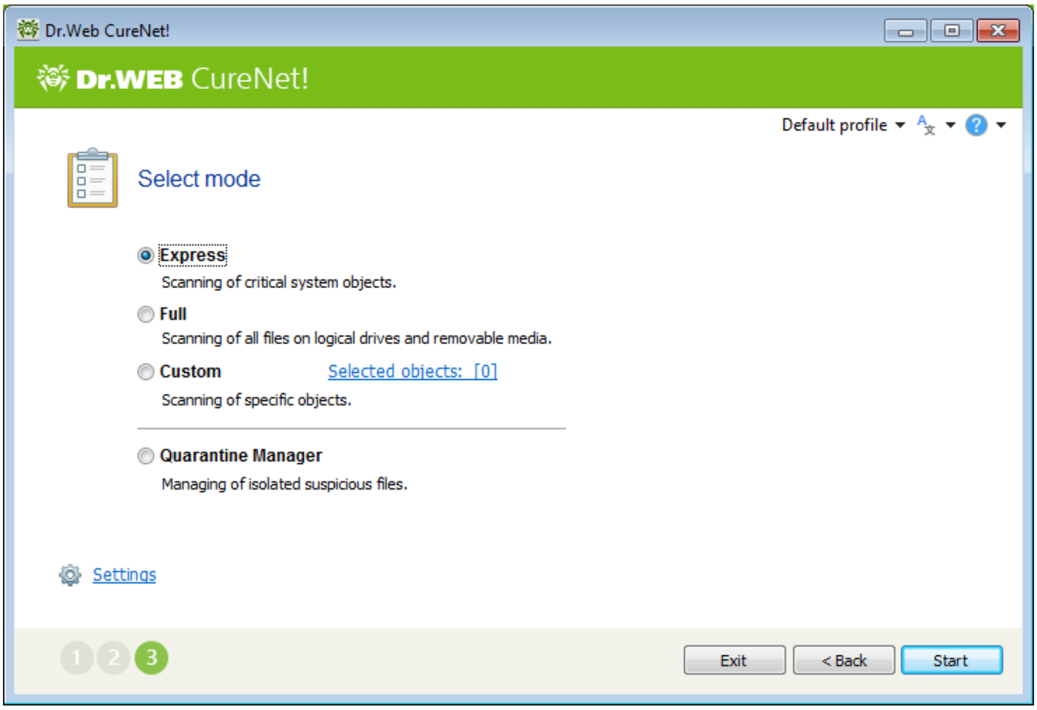
   You cannot use this method if network is configured incorrectly.
3. Click **OK**.

Adding stations during scanning

1. Right-click anywhere in the table and select **Add station** on the shortcut menu.
2. Enter IP address or network name of the station.
3. Click **OK**. The corresponding station will appear on the list of stations to scan.

5.3. Selecting Mode

This page helps you configure scanning options such as extent of anti-virus scan on stations and actions to perform to avert virus threats.



Dr.Web CureNet!

Select mode

● Express
Scanning of critical system objects.

○ Full
Scanning of all files on logical drives and removable media.

○ Custom Selected objects: [0]
Scanning of specific objects.

○ Quarantine Manager
Managing of isolated suspicious files.

Picture 8. Selecting Mode.

Scan Mode

By default, immediately after Dr.Web uploads files, Dr.Web Scanner starts on the station and performs an **Express scan**.

In this mode the following objects are scanned:

- Random access memory
- Boot sectors of all disks
- Boot disk root folder
- Windows system folder
- User documents folder (My documents)
- System temporary folder
- User temporary folder

User documents folder and user temporary folder are scanned for all accounts registered on the station.

In this mode, files in archives are not scanned.

You can change the default scan mode to one of the following:

- **Full scan**, which instructs Dr.Web Scanner to check RAM and all hard drives including their boot sectors, as well as run a check on rootkits.

- **Custom scan**, which instructs Dr.Web Scanner to check only those objects that are selected by the user. To select the objects to scan, click **Selected objects** and specify necessary objects to scan. When you save the profile, the list of objects is added to it.

Quarantine Manager Mode

This mode allows you to view and edit quarantine, created on stations, as well as to copy isolated files to your computer for further analysis. Quarantine serves for isolation of files that are suspected to be malicious. Quarantine also stores backup copies of files processed by Dr.Web.

5.4. Advanced Settings

The default settings are optimal for most cases.

If necessary, you can enable scanning of archives and email, change default Dr.Web Scanner reaction on detection of virus threats, and configure network settings of remote computers.

To modify default settings

1. To open the settings window, click**Settings**.
2. Configure options on the following tabs:
   - General
   - Exclusions
   - Actions
   - Network
   - Update

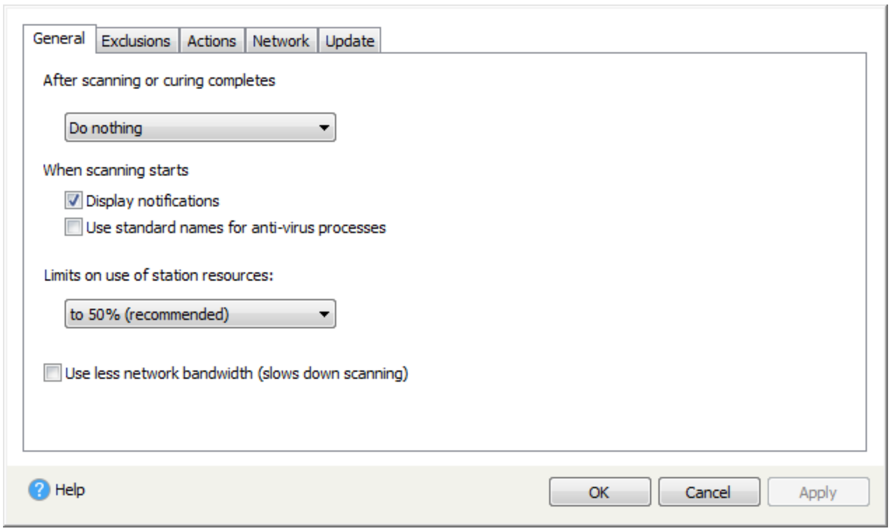
   If necessary, click **Apply**.
3. After you make you selection, click **OK** to save changes, or click **Cancel** to cancel changes.

Changes affect only the current scan. Next time you start Dr.Web, the application uses the default settings. Use scan profiles to save the settings.

5.4.1. General Tab

On this tab, you can configure general settings of Dr.Web scans on stations.

Aversion of some threats requires a system reboot. For example, when infected files are in use during scan or when it is necessary to modify registry keys. On this tab, you can configure settings for curing such infections.



After scanning or curing completes

Do nothing

When scanning starts

☑ Display notifications

□ Use standard names for anti-virus processes

Limits on use of station resources:

to 50% (recommended)

□ Use less network bandwidth (slows down scanning)

Picture 9. CureNet! Dr.Web Settings. General tab.

The **Restart station** or **Shut down station** modes instruct Dr.Web Scanner to perform the selected action on a remote computer if necessary once the scan finishes. The user of the remote computer is provided with an appropriate warning and a short period of time to complete current tasks and save information. A restart is performed only once, after scanning completes.

The **Do nothing** mode allows users to continue operating without restart, but in this case some infections may not be cured completely.

When a virus threat is detected in the master boot record (MBR), Dr.Web Scanner terminates the anti-virus scan and reboots the station immediately to avert the threat. In such cases, remote computers are rebooted regardless of the selected mode.

By default, Dr.Web notifies users of stations with a message above the notification taskbar before starting anti-virus scans. Clear the checkbox **Display notifications** to scan stations without any message.

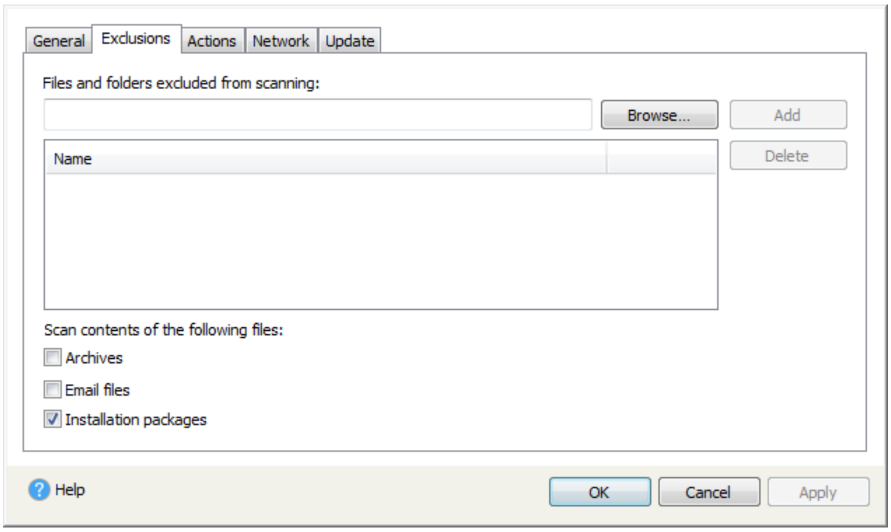
By default, Dr.Web files are copied to a station under random names. If anti-virus software with a firewall is installed on the station, the administrator may have to set firewall exceptions before every scan. If so, it is recommended to enable the **Use standard names for anti-virus processes** option, which allows Dr.Web files to be copied under their standard names. Thus, the administrator will need to set an exception only once.

You can also limit the use of resources of a scanned station. By default, the value is set to 50%. You can change this value or disable this restriction by selecting the required item in the **Limits on use of station resources** drop-down list.

In case of network congestion you can enable the setting **Use less network bandwidth (slows down scanning)**. In this mode Dr.Web copies program files to stations one after another and increases the time period before a station sends data to the administrator. Note that this setting slows down scanning.

5.4.2. Exclusions Tab

On this tab, you can specify the list of files and folders on the station to exclude from scanning. You can exclude the anti-virus quarantine folders, working folders of some programs, temporary files (paging file), and so on. By default, this list is empty.



Files and folders excluded from scanning:

Scan contents of the following files:

□ Archives

□ Email files

☑ Installation packages

Picture 10. Dr.Web Settings. Exclusions tab.

To configure list of exclusions

1. To add a file or folder to the exclusion list, do one of the following:
   - To add an existing file or folder, click **Browse** and select the item in the standard dialog window. You can enter the full path to the file or folder or edit the path in the field before adding it to the list.
   - To exclude all files or folders with a particular name, enter the name without path.
   - To exclude a group of files or folders, enter the mask of their names. ▾Details

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

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

   Examples:

   - `Report*.doc` defines all Microsoft Word documents whose names start with the word "Report" (`ReportFebruary.doc`, `Report121209.doc`, etc.)
   - `*.exe` defines all executable files; i.e., that have the EXE extension (`setup.exe`, `iTunes.exe`, etc.)
   - `photo????09.jpg` defines all JPG images which names start with the word "photo", end with "09" and contain exact number of 4 other characters in the middle (`photo121209.jpg`, `photoJoe09.jpg`, or `photo----09.jpg`, etc.)
2. Click **OK**. The file or folder will appear on the list.

Examples:

- `C:\folder` or `C:\folder\**`—excludes from scanning all files stored in C:\folder. The files stored within subfolders will be scanned.
- `C:\folder\*`—excludes all files located in C:\folder and its subfolders.
- `C:\folder\*.txt`—excludes all *.txt files stored in C:\folder. The *.txt files stored within subfolders will be scanned.
- `C:\folder\*\*.txt`—excludes all *.txt files stored in the first-level subfolders of C:\folder.
- `C:\folder\**\*.txt`—excludes all *.txt files stored in subfolders of any level within C:\folder. The files stored in C:\folder itself, including *.txt files, will be still scanned.

If necessary, you can select the following objects to scan:

- **Archives**—select this check box to scan files in archives.
- **Email files**—select this check box to scan mail files.
- **Installation packages**—select this check box to scan installation files.

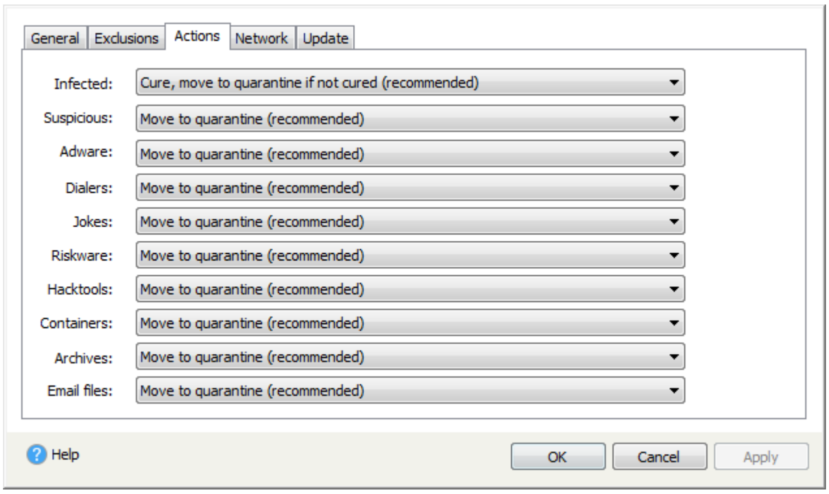
If an infected object is detected in an archive, Dr.Web Scanner performs an action specified for archives. The reaction is applied to the archive as a whole.

Note that this action may significantly slow down scanning and increase system load on stations.

5.4.3. Actions Tab

> Actions to avert threats are only executed when operating in a regular mode (with valid license key file). When operating in a demo mode, Dr.Web only informs you on detected threats.

On this tab, you can set Dr.Web Scanner reaction on detection of virus threats depending on the type of threat and infected object.



Infected: Cure, move to quarantine if not cured (recommended)
Suspicious: Move to quarantine (recommended)
Adware: Move to quarantine (recommended)
Dialers: Move to quarantine (recommended)
Jokes: Move to quarantine (recommended)
Riskware: Move to quarantine (recommended)
Hacktools: Move to quarantine (recommended)
Containers: Move to quarantine (recommended)
Archives: Move to quarantine (recommended)
Email files: Move to quarantine (recommended)

Picture 11. Dr.Web Settings. Actions tab.

The reaction is specified separately for each type of objects:

- **Infected**—modified by a known and supposedly curable virus.
- **Suspicious**—supposedly present a threat to information security.

You can also separately specify the reaction for different types of malicious software and packages (archives, emails, and file containers).

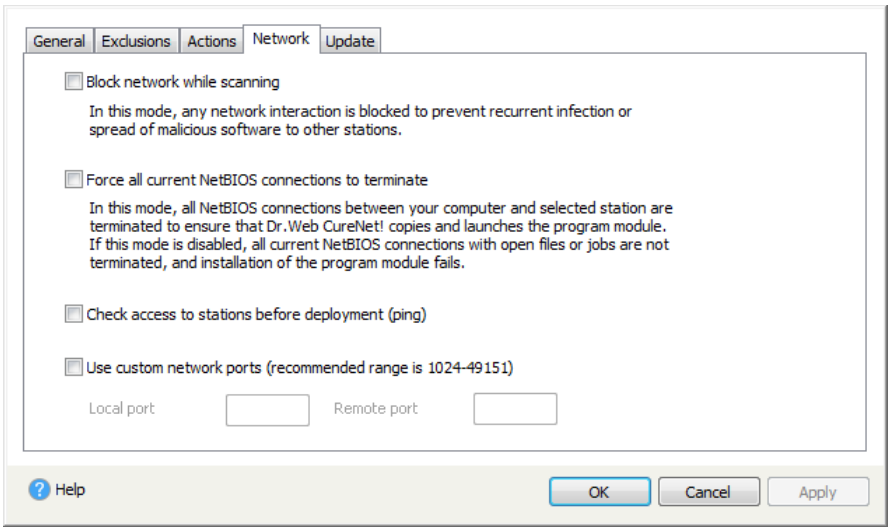
> ⚠ If an infected object is detected in an archive, Dr.Web performs an action specified for archives. The reaction is applied to the whole archive. Dr.Web cannot apply reactions only to the infected objects.

If necessary, you can modify the default action to one of the following:

- **Cure, move to quarantine if not cured (recommended)**—(available for infected objects only) instructs Dr.Web Scanner to try to cure objects infected with a known virus. If the virus is incurable or the attempt of curing failed, the file is moved to the Quarantine.
- **Move to quarantine (recommended)**—(not available for boot sectors) instructs Dr.Web Scanner to move infected or suspicious objects to the Quarantine.
- **Ignore**—(available for malicious software only) not to register the event in the Dr.Web report.
- **Inform**—provide information on malicious or suspicious objects for displaying in the Dr.Web report.

5.4.4. Network Tab

On this tab, you can configure options of network communication for the stations during anti-virus scans.



□ Block network while scanning

In this mode, any network interaction is blocked to prevent recurrent infection or spread of malicious software to other stations.

□ Force all current NetBIOS connections to terminate

In this mode, all NetBIOS connections between your computer and selected station are terminated to ensure that Dr.Web CureNet! copies and launches the program module. If this mode is disabled, all current NetBIOS connections with open files or jobs are not terminated, and installation of the program module fails.

□ Check access to stations before deployment (ping)

□ Use custom network ports (recommended range is 1024-49151)

Local port
Remote port

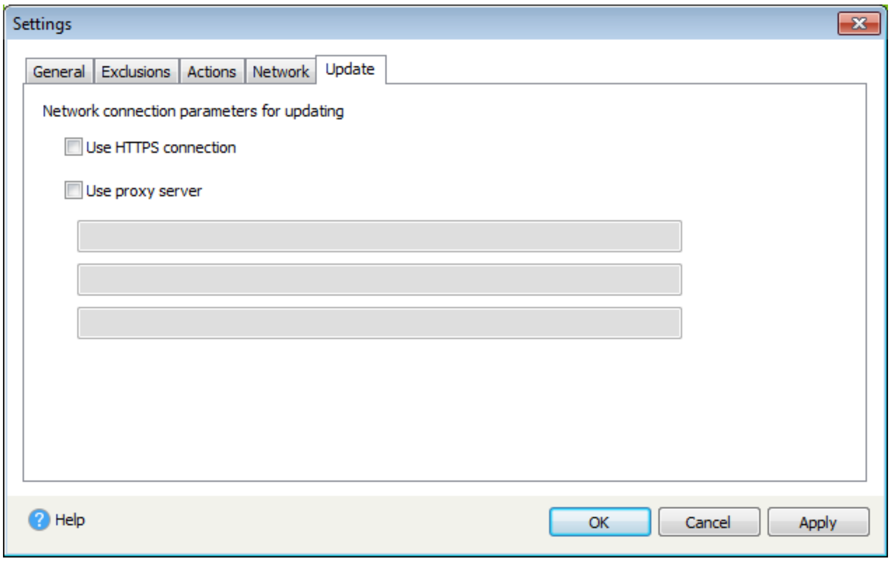
Picture 12. Dr.Web Settings. Network tab.

If necessary, you can select one of the following modes:

- **Block network while scanning**—enable this mode to disable network communication of the stations during scanning and prevent recurrent infection and spread of the infection over the network.
- **Force all current NetBIOS connections to terminate**—enable this mode to terminate all existing NetBIOS connections prior to starting anti-virus scans, including connections with open files or jobs (required to ensure uploading and starting of the Dr.Web Scanner on remote computers).
- **Check access to stations before deployment (ping)**—enable this mode to determine presence of the station on the network prior to attempting to upload Dr.Web files.
- **Use custom network ports (recommended range is 1024-49151)**—enable this mode to specify the ports used for network communication between Dr.Web Scanner and station during scanning.

5.4.5. Update Tab

On this tab, you can configure network connection parameters to use when updating Dr.Web repository.



Network connection parameters for updating

□ Use HTTPS connection

□ Use proxy server

Picture 13. Dr.Web Settings. Update tab.

If necessary, you can select one of the following modes:

- **Use HTTPS connection**—select this mode if you want to download updates via a secure protocol.
- **Use proxy server**—select this check box, if you want to use a proxy server. Enter **Address** and **port** of the proxy server to use. If the proxy server requires authorization, enter **Username** and **Password**.

5.5. Dr.Web Report

This page presents progress and results of anti-virus scans performed by Dr.Web Scanner on all stations. Statistics gathering is independent of the quality of connection between the computer running Administrative Console and remote stations. If a station goes offline during scanning, Dr.Web attempts to re-establish the connection and updates the scanning statistics once the station becomes online again.

The top of the windows displays general information on scanning status and statistics.

The **Stations** section contains the following information:

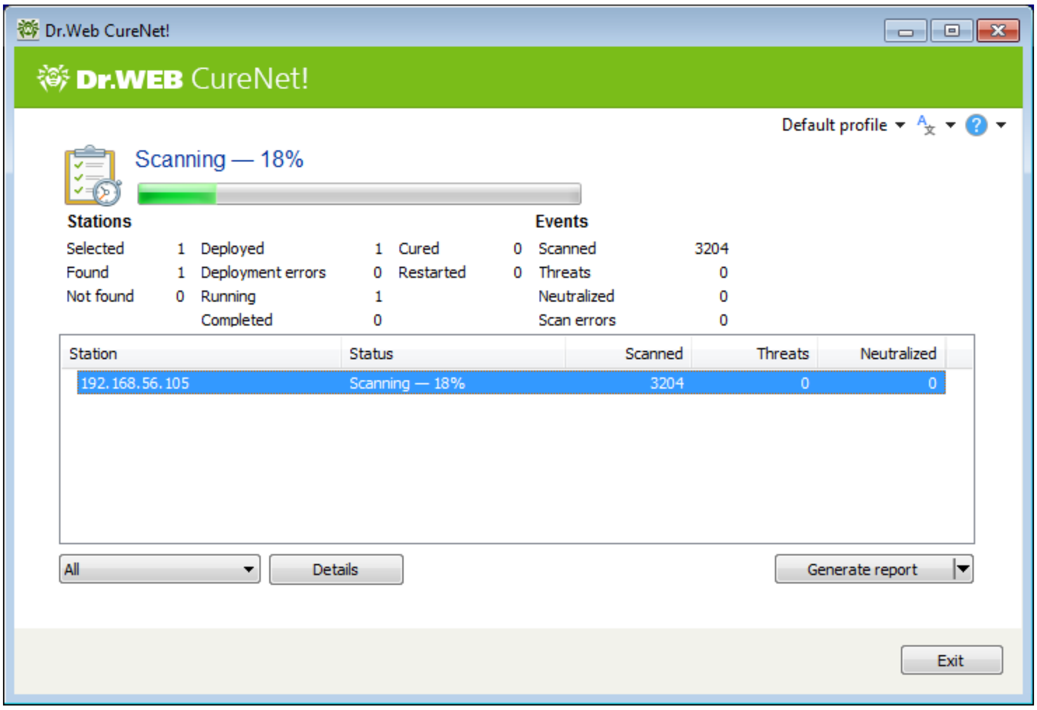
Item	Description
Selected	Total number of stations selected for scanning.
Found	Total number of stations present on the network.
Not found	Total number of stations not found on the network.
Deployed	Total number of stations to which Dr.Web connected and where files were deployed successfully.
Deployment errors	Total number of stations to which Dr.Web failed to connect and/or where Dr.Web failed to deploy files.
Running	Total number of running anti-virus scans.
Completed	Total number of completed anti-virus scans.
Cured	Total number of cured stations where all virus threats were neutralized.
Restarted	Total number of stations restarted to complete curing.

The **Events** section contains the following information:

Item	Description
Scanned	Total number of objects scanned on all stations.
Threats	Total number of virus threats detected on all stations
Neutralized	Total number of objects cured on all stations
Scan errors	Total number of objects Dr.Web Scanner failed to scan on all stations.

General information on scanning is presented as a table with the following data:

Item	Description
Computer	IP address or network name of the station.
Status	Stage of the scanning process on the station (installation, scan progress, error messages, and so on).
Scanned	Total number of objects scanned on the station.
Threats	Total number of virus threats detected on the remote computer.
Neutralized	Total number of virus threats averted on the station (curing is possible only for objects infected with a known and curable virus).



Scanning — 18%

Stations						Events	
Selected	1	Deployed	1	Cured	0	Scanned	3204
Found	1	Deployment errors	0	Restarted	0	Threats	0
Not found	0	Running	1			Neutralized	0
		Completed	0			Scan errors	0

Station	Status	Scanned	Threats	Neutralized
192.168.56.105	Scanning — 18%	3204	0	0

Picture 14. Dr.Web report.

If necessary, use the filter feature to list only the statistics of interest. You can also sort the station list by clicking the heading of the column which you want to order.

Authenticity of the master boot record (MBR) is critical for the operating system security. For this reason, Dr.Web Scanner terminates the anti-virus scan and reboots the remote computer immediately if an MBR virus is detected. This reboot is mandatory to cure an MBR. At that, station scan is terminated prematurely.

In the Dr.Web report, this situation is indicated by earlier completion of anti-virus scans of some computers as compared to the others. Information on MBR virus detection is also provided in the station statistics window.

The anti-virus scanning of stations infected with MBR viruses may be incomplete. To ensure maximum security, run the anti-virus scan on these stations again using Administrative Console.

To add new station to scan

To add new station to scan, if scanning is already started, right-mouse click in the report fie**Add station** and type IP address or network name of the necessary station.

To view statistics of a station

To display detailed statistics on a particular station, do one of the following:

- Double-click an item referring to the remote computer on the list.
- Select an item referring to the station on the list and click **Details**.

Station statistics window opens. If errors occur while copying Dr.Web files to the remote computer, or the remote computers goes offline during scan, this window displays an appropriate warning.

If an infected object is detected within a package (archive, email, or file container), the table lists both the infected object, and the package containing it.

⚠ For details on how to configure actions upon malicious objects, refer to Advanced Settings.

To export report

To save the Dr.Web report, click **Generate report** and select the report format and stations to be included in the report. The report will be automatically saved into the product folder.

5.6. Quarantine Manager

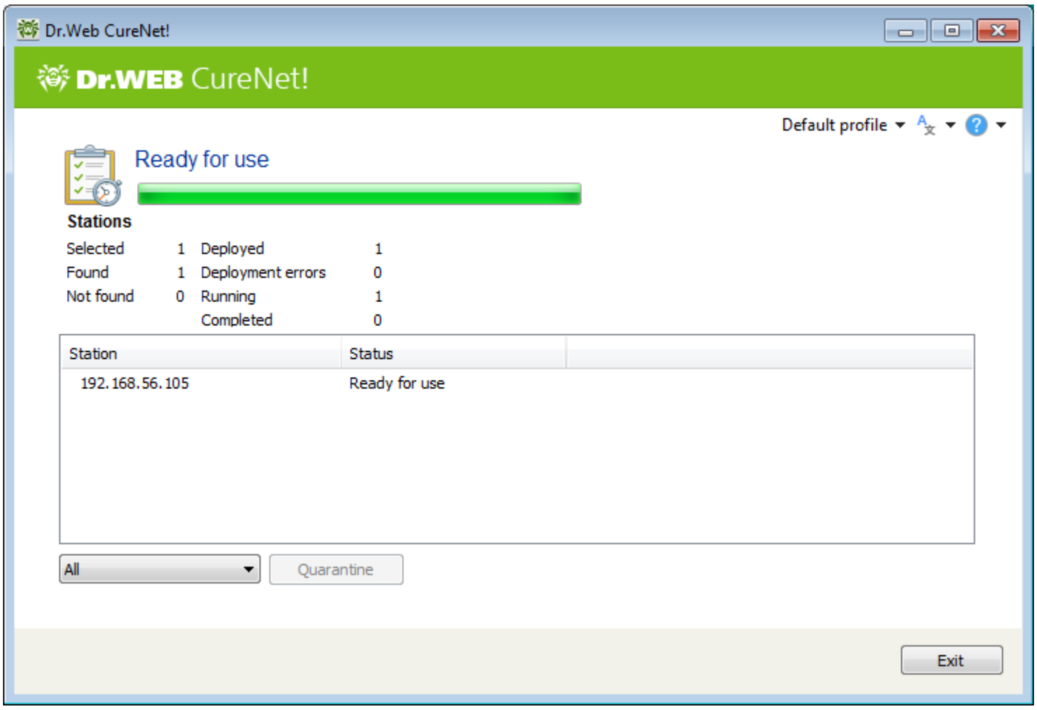
Dr.Web allows you to view and edit quarantine, created on stations, as well as to copy isolated files to your computer for further analysis. Quarantine serves for isolation of files that are suspected to be malicious. Quarantine also stores backup copies of files processed by Dr.Web.

Enabling quarantine mode

1. Specify stations, where you want to view quarantine.
2. On the page, where you can specify operation mode, select **Quarantine Manager**.
3. Click **Start**.

At the top of the page you will see information about operation of **Quarantine Manager** on the specified stations:

Item	Description
Selected	Total number of selected stations.
Found	Total number of stations present on the network.
Not found	Total number of stations not found on the network.
Deployed	Total number of stations to which Dr.Web connected and where files were deployed successfully.
Deployment errors	Total number of stations to which Dr.Web failed to connect and/or where Dr.Web failed to deploy files.
Running	Number of stations where **Quarantine Manager** is running.
Completed	Number of stations where **Quarantine Manager** completed its operation (for example, because the station was shut down by the user).



Stations

Selected	1	Deployed	1
Found	1	Deployment errors	0
Not found	0	Running	1
		Completed	0

Station	Status
192.168.56.105	Ready for use

Picture 15. Dr.Web Quarantine Manager.

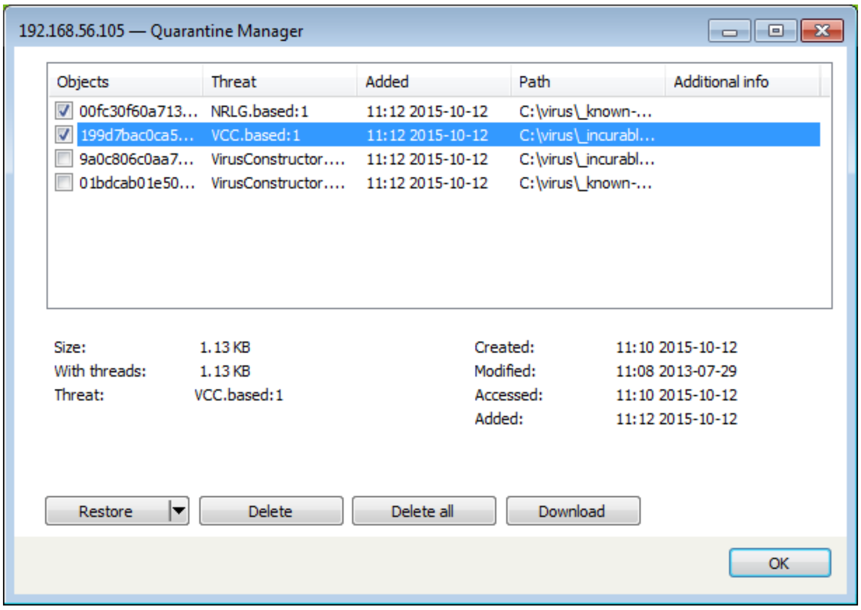
On this page, you can:

- Change account information required for connection to the station. For that, right-click a station on the list and select **Change credentials**.
- Add new stations. For that, right-click anywhere in the table and select **Add station**. In the open window, enter the IP address or network name of the station.

- Filter stations by one of the following parameters: with errors, found, not found, with empty or non-empty quarantine. For that, click the drop-down list below the table and select the required filter.

To view and edit quarantine on a certain station, select it on the list and either click **Quarantine** on the shortcut menu of the station or click the **Quarantine** button at the bottom of the window.

In the open window, you can see the list of objects isolated on this station to quarantine and details on every object: malware class of the object, which is assigned by Dr.Web, date of adding the object to quarantine, full path to the object before it was quarantined, and others.



192.168.56.105 — Quarantine Manager

Objects	Threat	Added	Path	Additional info
☑ 00fc30f60a713...	NRLG.based:1	11:12 2015-10-12	C:\virus_known-...	
☑ 199d7bac0ca5...	VCC.based:1	11:12 2015-10-12	C:\virus_incurabl...	
□ 9a0c806c0aa7...	VirusConstructor....	11:12 2015-10-12	C:\virus_incurabl...	
□ 01bdcab01e50...	VirusConstructor....	11:12 2015-10-12	C:\virus_known-...	

Size:	1.13 KB	Created:	11:10 2015-10-12
With threads:	1.13 KB	Modified:	11:08 2013-07-29
Threat:	VCC.based:1	Accessed:	11:10 2015-10-12
		Added:	11:12 2015-10-12

Picture 16. Viewing quarantine.

On this page, you can:

- Restore certain objects to their original location. For that, select them on the list and click **Restore** at the bottom of the window.
- Restore certain objects to a different location. For that, select them on the list and click **Restore** at the bottom of the window and then select **Restore as**.
- Delete certain objects. For that, select them on the list and click **Remove** at the bottom of the window.
- Delete all objects at once. For that, click **Delete all** at the bottom of the window.
- Download quarantined objects to your computer. For that, select required objects on the list and click **Download** at the bottom of the window. In the open window, specify the folder where you want to save the objects.

6. Appendix A. Technical Support

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

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

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

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

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

7. Appendix B. Detection Methods

Doctor Web anti-virus solutions use several malicious software detection methods simultaneously, which allows them to perform thorough checks on suspicious files and control software behavior.

Detection Methods

Signature analysis

The scans begin with signature analysis that is performed by comparison of file code segments to the known virus signatures. A *signature* is a finite continuous sequence of bytes which is necessary and sufficient to identify a specific virus. To reduce the size of the signature dictionary, Dr.Web anti-virus solutions use signature checksums instead of complete signature sequences. Checksums uniquely identify signatures, which preserves correctness of virus detection and neutralization. Dr.Web virus databases are composed so that some entries can be used to detect not just specific viruses, but whole classes of threats.

Origins Tracing™

On completion of signature analysis, Dr.Web anti-virus solutions use the unique Origins Tracing method to detect new and modified viruses that use the known infection mechanisms. Thus, Dr.Web users are protected against such threats as notorious blackmailer Trojan.Encoder.18 (also known as gpcode). In addition to detection of new and modified viruses, the Origins Tracing mechanism allows to considerably reduce the number of false triggering of the heuristic analyzer. Objects detected using the Origins Tracing algorithm are indicated with the `.Origin` extension added to their names.

Execution emulation

The technology of program code emulation is used for detection of polymorphic and encrypted viruses, when the search against checksums cannot be applied directly, or is very difficult to be performed (due to the impossibility of building secure signatures). The method implies simulating the execution of an analyzed code by an *emulator*—a programming model of the processor and runtime environment. The emulator operates with protected memory area (*emulation buffer*), in which execution of the analyzed program is modelled instruction by instruction. However, none of these instructions is actually executed by the CPU. When the emulator receives a file infected with a polymorphic virus, the result of the emulation is a decrypted virus body, which is then easily determined by searching against signature checksums.

Heuristic analysis

The detection method used by the heuristic analyzer is based on certain knowledge (*heuristics*) about certain features (attributes) that might be typical for the virus code itself, and vice versa, that are extremely rare in viruses. Each attribute has a weight coefficient which determines the level of its severity and reliability. The weight coefficient can be positive if the corresponding attribute is indicative of a malicious code or negative if the attribute is uncharacteristic of a computer threat. Depending on the sum weight of a file, the heuristic analyzer calculates the probability of unknown virus infection. If the threshold is exceeded, the heuristic analyzer generates the conclusion that the analyzed object is probably infected with an unknown virus.

The heuristic analyzer also uses the FLY-CODE™ technology, which is a versatile algorithm for extracting files. The technology allows making heuristic assumptions about the presence of malicious objects in files compressed not only by packagers Dr.Web is aware of, but also by new, previously unexplored programs. While checking packed objects, Dr.Web anti-virus solutions also use structural entropy analysis. The technology detects threats by arranging pieces of code; thus, one database entry allows identification of a substantial portion of threats packed with the same polymorphous packager.

As any system of hypothesis testing under uncertainty, the heuristic analyzer may commit type I or type II errors (omit viruses or raise false alarms). Thus, objects detected by the heuristic analyzer are treated as “suspicious”.

While performing any of the abovementioned checks, Dr.Web anti-virus solutions use the most recent information about known malicious software. As soon as experts of Doctor Web anti-virus laboratory discover new threats, the update for virus signatures, behavior characteristics, and attributes is issued. In some cases, updates can be issued several times per hour. Therefore, even if a brand new virus passes through Dr.Web resident guards and penetrates the system, after an update it is detected on the list of processes and neutralized.

8. Appendix C. Network Masks

A mask determines the sequence of common leading bits in IP addresses of the computers you want to add for scanning. To select a group of IP addresses using masks, specify an IP address of a computer in the subnet and the mask, which determines the rest of the computers by bitwise AND operation.

For example, to add for scanning 254 remote computers with range of IP addresses from 10.30.0.1 to 10.30.0.254, you can use the 10.30.0.0/24 mask:

IP address 10.30.0.1	00001010.00011110.00000000.00000001
Mask 255.255.255.0 (24)	11111111.11111111.11111111.00000000
Minimal IP address 10.30.0.1	00001010.00011110.00000000.00000001
Maximal IP address 10.30.0.254	00001010.00011110.00000000.11111110
Broadcast IP address 10.30.0.255	00001010.00011110.00000000.11111111

Total number of computers in the network: 254

Dr.Web supports the following mask notations:

- Quad-dotted decimal notation, for example, 192.168.0.1/255.255.255.0 where 192.168.0.1 is an IP address and 255.255.255.0 is a mask
- Binary (CIDR) notation which determines the length, in bits, of the mask prefix, for example, 192.168.0.1/24 where 192.168.0.1 is an IP address, 24 is a decimal notation of a bit mask with first 24 bits on

In IPv4 networks both notations can be use. IPv6 networks supports the CIDR notation only.