Dr.WEB® CureNet!

Defend what you create

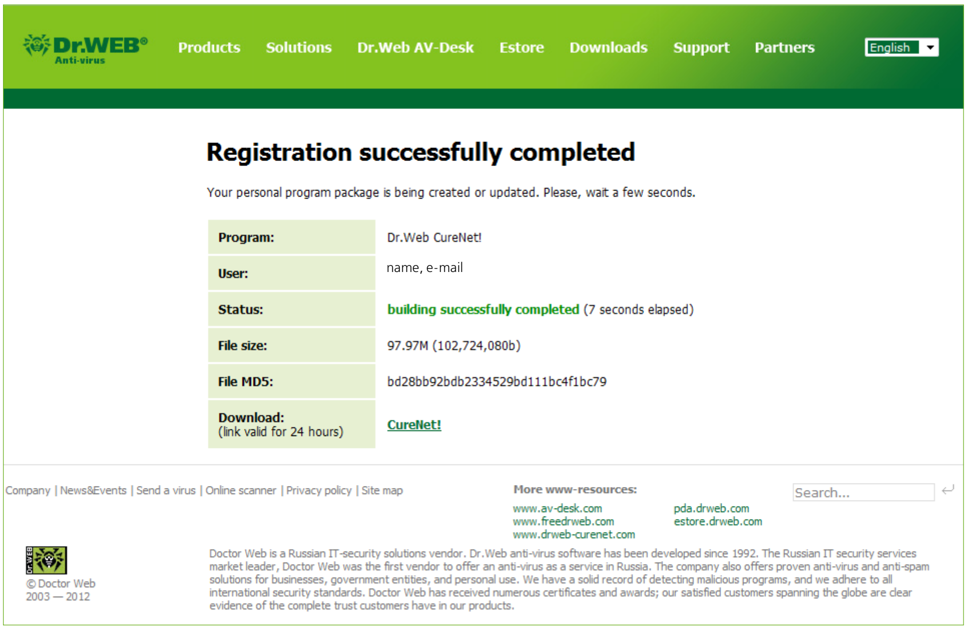
Quick Start

Dr.Web CureNet! performs centrally-managed remote anti-virus scanning of networked computers without installation of anti-virus software on target machines. Dr.Web CureNet! scans personal computers and servers running Microsoft® Windows® in networks of any topology.

Caution! Dr.Web CureNet! doesn't provide resident end-point security . When the solution doesn't scan computers, they may get infected by any malicious program. To establish reliable all-time anti-virus security use such software products as Dr.Web Security Space Pro or Dr.Web Enterprise Suite.

Download Dr.Web CureNet!

To download a distribution file register your serial number at http://products.drweb.com/register/. Your individual distribution file will be generated upon completion of the registration procedure. Download the distribution file from your personal area.



Registration successfully completed

Your personal program package is being created or updated. Please, wait a few seconds.

Program:	Dr.Web CureNet!
User:	name, e-mail
Status:	building successfully completed (7 seconds elapsed)
File size:	97.97M (102,724,080b)
File MD5:	bd28bb92bdb2334529bd111bc4f1bc79
Download: (link valid for 24 hours)	CureNet!

Doctor Web is a Russian IT-security solutions vendor. Dr.Web anti-virus software has been developed since 1992. The Russian IT security services market leader, Doctor Web was the first vendor to offer an anti-virus as a service in Russia. The company also offers proven anti-virus and anti-spam solutions for businesses, government entities, and personal use. We have a solid record of detecting malicious programs, and we adhere to all international security standards. Doctor Web has received numerous certificates and awards; our satisfied customers spanning the globe are clear evidence of the complete trust customers have in our products.

You can use the program's interface to open a personal area page or navigate to your personal area after registering your serial number at http://support.drweb.com/get+cabinet+link/.

If you have already registered your serial number for Dr.Web CureNet!, simply log into your Personal area. and download the latest version of the distribution file.

System requirements

In order to perform a remote scanning of computers by means of DR.Web CureNet!:

- Target machines must be connected to the network.
- an account used by Dr.Web CureNet! to connect to remote computers, must be created with necessary administrative privileges;
- ports 139 and 445 must be open in target systems.

Caution! Before you start scanning, make sure that you have information about all valid administrator accounts created on all target computers.

Windows 2000 system configuration consists of two phases:

1. Enable the administrator account.
2. Configure network components.

Important! The Service Pack 4 Rollup 1 must be installed in the system.

Download Service Pack 4 for Windows 2000:
http://www.microsoft.com/ru-ru/download/details.aspx?id=4127

Download Update Rollup 1 for Windows 2000 SP4:
http://www.microsoft.com/en-us/download/details.aspx?id=18997

1. Enable the administrator account.

Click Start and go to **Settings** → **Control panel** → **Administration** → **Computer Management** → **Local Users** and **Groups** → **Users**. You can adjust required parameters of the **Administrator account** but in it is recommended to create an alternative administrator account. Right-click In the right pane and select **New user** in the context menu.

- Enter DrWebCurenet as a user name.
- Set a strong password In the **Password** and **Confirm password** fields.
- Disable the **User must change password at next logon** option.
- Check the **Password never expires** checkbox.
- Press **Create** and after that press **Close**.

Double-click on the created **DrWebCurenet** account and go to the **Member of** tab. Select **Users** and click **Remove**. Then click **Add**. In the **Select Groups** dialogue, select **Administrators** and click **Add**. And then press **OK**. In the **DrWebCurenet** properties window press **Apply** and **OK**.

2. Configure network components

Click **Start** and go to **Settings** → **Network and Dial-up Connections**. Select a network connection and click the right mouse button. In the context menu select **Properties**.

Make sure that the following components are enabled:

- Client for Microsoft networks
- File and Printer Sharing for Microsoft Networks
- Internet Protocol (TCP/IP)

Click **OK**.

If you use a firewall, open ports 139 and 445.

Windows XP (Windows 2003) system configuration consists of four phases:

1. Enable the administrator account.
2. Configure file sharing (not required for Windows 2003).
3. Configure Local Security Policy.
4. Configure Windows Firewall.
5. Configure network components.

Important! The Service Pack 2 or 3 must be installed for Windows XP.

Download Service Pack 2 for Windows XP: http://www.microsoft.com/en-us/download/details.aspx?id=28

Download Service Pack 3 for Windows XP: http://www.microsoft.com/en-us/download/details.aspx?id=24

Supported versions:

- Windows XP Professional;

Since the following editions do not support remote execution of programs, they can't be used to run Dr.Web CureNet!:

- Windows XP Starter;
- Windows XP Home Edition.

The Service Pack 1 or 2 must be installed for Windows 2003.

Download Service Pack 1 for Windows 2003: http://www.microsoft.com/en-us/download/details.aspx?id=11435

Download Service Pack 2 for Windows 2003 (recommended):
http://www.microsoft.com/en-us/download/details.aspx?id=41

1. Enable the administrator account.

Click **Start** and go to **Control panel** → **Administrative Tools** → **Computer Management** → **Local Users** and **Groups** → **Users**. You can adjust required parameters of the **Administrator account** but in it is recommended to create an alternative administrator account. In the right pane, right-click. In the context menu select **New user**. Enter the user name **Dr.WebCureNET**. In the **Password** and **Confirmation fie**lds Enter a strong password. Disable the **User must change password at next logon** option. Check the **Password never expires** checkbox. Click **Create** and then click **Close**. Double-click on the created **DrWebCurenet account** icon. The **Properties** window will open. Go to the **Member of** tab. In the **Member Of** tab select **Users** and click **Remove**. Then click **Add**. The **Select group** window will open. Click **Advanced** and then click **Find now**. On the resulting list select **Administrators**, press **OK** and press **OK** one more time in the **Select Group** window. In the **DrWebCurenet** properties window press **Apply** and **OK**.

2. Configure file Sharing.

Click Start and go to **Control panel** → **Classical view** → **Folder Options**. The **Folder Options** window will open. Go to the **View** tab. Clear the **Use simple file sharing** checkbox. Press **Apply** and after that press **OK**.

3. Configure the local security policy.

Go to **Control panel** → **Administrative Tools** → **Local Security Policy** → **Local Policies–Security Options**. Hover the mouse cursor over the **Network access: sharing and security model for local accounts** and double-click on the entry. The **Properties** window will open. Select the **Classic** option. Successively press **Apply** and **OK**. Close the **Local Security Settings** window.

4. Configure the firewall.

If you use a third-party firewall, open ports 139 and 445. If you use the Windows Firewall, adjust the following settings. Go to **Start** → **Control panel** → **Windows Firewall**. Go to the **Exceptions** tab. Tick the **File and printer sharing** checkbox. Click **OK**.

5. Configure network components

Go to **Start** → **Control panel** → **Network connections**. Right-click on the network connection. In the context menu select **Properties**. The network connection properties window will open. Go to the **General** tab. Make sure that the following components are enabled:

- Client for Microsoft networks
- File and Printer Sharing for Microsoft Networks
- Internet Protocol (TCP/IP)

Click **OK**.

Windows Vista configuration consists of six stages:

1. Configure User Account Control.
2. Configure file sharing.
3. Enable the administrator account.
4. Configure Windows Firewall.
5. Configure network components.
6. Configure Local Security Policy.

Important! The Service Pack 1 or 2 must be installed for Windows Vista.

Download Service Pack 1 for Windows Vista: http://www.microsoft.com/en-us/download/details.aspx?id=910

Download Service Pack 2 for Windows Vista (recommended): http://www.microsoft.com/en-us/download/details.aspx?id=15278

The following edditions are supported:

- Windows Vista Business;
- Windows Vista Enterprise;
- Windows Vista Ultimate.

Since the following editions do not support remote execution of programs, they can't be used to run Dr.Web CureNet!:

- Windows Vista Starter;
- Windows Vista Home Basic;
- Windows Vista Home Premium.

1. If UAC is enabled, perform the following steps.

- Press **Windows+R**. In the window that opens, type «`Regedit`» without the quotes and press **Enter**. This will open the **Windows Registry Editor**.
- Go to `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]`
- Go to the right side of the **Registry Editor** window, right click and select **Create** in the the context menu and choose **32-bit DWORD value**. Set the name of the parameter «`LocalAccountTokenFilterPolicy`» without the quotes.
- Double-click on the newly created key. The **DWORD** edit window will appear. Set the value to 1 and click **OK**.
- Close the **Registry Editor**.

2. Adjust file sharing settings.

Click **Start** and go to **Control Panel** → **Network and Internet** → **The Network and Sharing Center** → **Sharing and Discovery**. Enable **Network discovery** and **File Sharing**.

3. Enable the administrator account.

Click **Start** and go to **Control panel** → **System and Maintenance** → **Administrative Tools** → **Computer Management** → **Local Users** and **Groups** → **Users**. You can adjust required parameters of the **Administrator account** but in it is recommended to create an alternative administrator account. Right-click In the central pane and select **New user** in the context menu.

- Enter the user name **DrWebCurenet**
- Set a strong password In the **Password** and **Confirm password** fields.
- Disable the **User must change password at next logon** option.
- Check the **Password never expires** checkbox.
- Press **Create** and after that press **Close**.

Double-click on the created **DrWebCurenet account** and go to the **Member of** tab. Select **Users** and click **Remove**. Then click **Add**. The **Select groups** window will open. Click **Advanced** and then click **Find now**. In the search results select **Administrators** and click **OK**. In the **Select groups** window also click **OK**. Click **Apply** and **OK** in the **Properties:DrWebCurenet** window.

4. Configure the firewall.

If you use a third-party firewall, open ports 139 and 445. If you use the Windows Firewall, adjust the following settings. Go to **Start** → **Control panel** → **Security** → **Windows Firewall**. Click **Allow a program through Windows Firewall**. In theWindows Firewall window go to **Exceptions**. Tick the **File and printer sharing** checkbox. Click **OK**.

5. Configure network components

Click **Start** and go to **Control Panel** → **Network and Internet** → **The Network and Sharing Center** → **Network management**. Click on the network connection icon. In the context menu select **Properties**. Make sure that the following components are enabled:

- Client for Microsoft networks
- File and Printer Sharing for Microsoft Networks
- Internet Protocol version 4.

6. Configure the local security policy.

Click **Start** and go to **Control Panel** → **System and Maintenance** → **Administration** → **Local Security Policy** → **Local Policies** → **Security Options**. Hover the mouse cursor over the **Network access: sharing and security model for local accounts** and double-click on the entry. The **Properties** window will open. Select **Classic** and click **OK**.

Windows 7 (Windows 2008, Windows 2008 R2) configuration consists of six stages:

1. Configure User Account Control
2. Configure file sharing
3. Enable the administrator account.
4. Configure Windows Firewall.
5. Configure network components.
6. Configure Local Security Policy.

Important! The following editions are supported:

- Windows 7 Professional
- Windows 7 Enterprise
- Windows 7 Ultimate.

Since the following editions do not support remote execution of programs, they can't be used to run Dr.Web CureNet!:

- Windows 7 Starter
- Windows 7 Home Basic
- Windows 7 Home Premium

For Windows 2008 Service Pack 2 must be installed.

Download Service Pack 2 for Windows 2008: http://www.microsoft.com/en-us/download/details.aspx?id=15278

1. If UAC is enabled, perform the following steps.

- Press **Windows+R**. In the window that opens, type «`Regedit`» without the quotes and press Enter. This will open the **Windows Registry Editor**.
- Go to `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]`
- Go to the right side of the **Registry Editor** window, right click and select **Create** in the the context menu and choose **32-bit DWORD** value. Set the name of the parameter «`LocalAccountTokenFilterPolicy`» without the quotes.
- Double-click on the newly created key. The **DWORD** edit window will appear. Set the value to 1 and click **OK**.
- Close the **Registry Editor**.

2. Adjust file sharing settings.

Go to **Start** → **Control panel** → **Network and Internet** → **The Network and Sharing Center** → **Change advanced sharing settings**. In the appropriate network profile choose **Enable network discovery** and **Enable File and Printer sharing**. Click **Save changes**. If you configure Windows 2008 or Windows 2008 R2, do not use the **Enable network discovery** option.

3. Enable the administrator account.

Click **Start** and go to **Control panel** → **System and Security** → **Administrative Tools** → **Computer Management** → **Local Users and Groups–Users**. You can adjust required parameters of the **Administrator account** but in it is recommended to create an alternative administrator account. Right-click In the central pane and select **New user** in the context menu.

Enter the user name **DrWebCurenet**

- Set a strong password In the Password and Confirm password fields.
- Disable the User must change password at next logon option.
- Check the Password never expires checkbox.
- Press Create and after that press Close.

Double-click on the created **DrWebCurenet** account and go to the **Member of** tab. Select **Users** and click **Remove**. Then click **Add**. The **Select groups** window will open. Click **Advanced** and then click **Find now**. In the search results select **Administrators** and click **OK**. In the **Select groups** window also click **OK**. In the **DrWebCurenet** properties window press **Apply** and **OK**.

4. Configure the firewall.

If you use a third-party firewall, open ports 139 and 445. If you use the Windows Firewall, adjust the following settings. Click **Start** and go to **Control Panel** → **System and Security** → **Windows Firewall** → **Allow a program or feature through Windows Firewall**. Click **Change settings**. Tick the **File and printer sharing** checkbox. Click **OK**.

5. Configure network components

Click **Start** and go to **Control Panel** → **Network and Internet** → **The Network and Sharing Center** → **Change adapter settings**. Right-click on the appropriate network connection button. In the context menu select **Properties**. Make sure that the following components are enabled:

- Client for Microsoft networks
- File and Printer Sharing for Microsoft Networks
- Internet Protocol Version 4 (TCP / IP v4).

6. Configure the local security policy.

Click **Start** and go to **Control Panel** → **System and Security** → **Administration** → **Local Security Policy** → **Local Policies** → **Security Options**. Double-click on **Network access: sharing and security model for local accounts**. The **Properties** window will open. Select **Classic** and click **OK**.

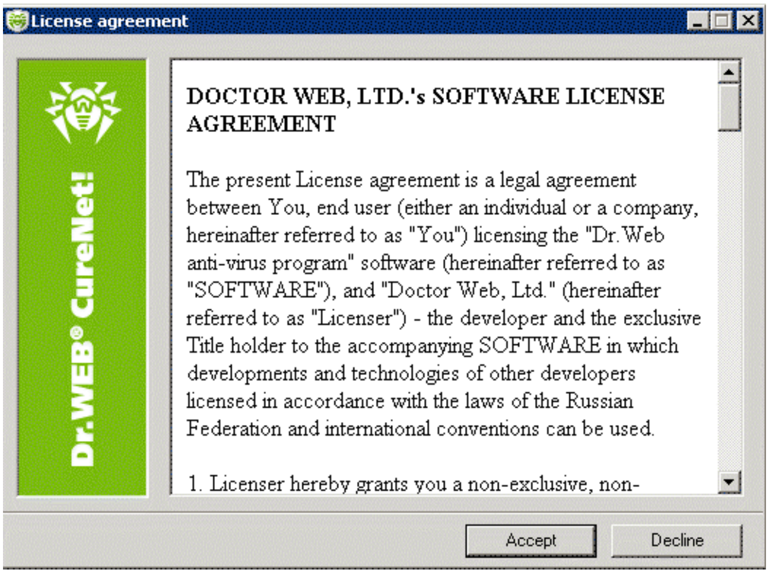
Launch Dr.Web CureNet!

1. Launch the `CureNet!.exe` file you have downloaded.

Caution! The procedure that will be used to start Dr.Web CureNet! after the first launch will be described below.

Catuion! Even though Dr.Web CureNet! is compatible with anti-virus solutions from other vendors, it is recommended to disable them while you are scanning systems with Dr.Web CureNet! to make the scanning process faster.

2. Read the License agreement text and press the **Accept** button to accept its terms.



DOCTOR WEB, LTD.'s SOFTWARE LICENSE AGREEMENT

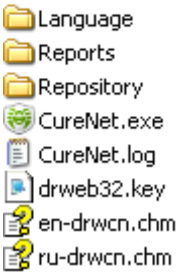
The present License agreement is a legal agreement between You, end user (either an individual or a company, hereinafter referred to as "You") licensing the "Dr.Web anti-virus program" software (hereinafter referred to as "SOFTWARE"), and "Doctor Web, Ltd." (hereinafter referred to as "Licenser") - the developer and the exclusive Title holder to the accompanying SOFTWARE in which developments and technologies of other developers licensed in accordance with the laws of the Russian Federation and international conventions can be used.

1. Licenser hereby grants you a non-exclusive, non-

3. If you want to specify a location to store the Dr.Web CureNet! file for further use rather than save it to the default directory, click on the **Browse** button.

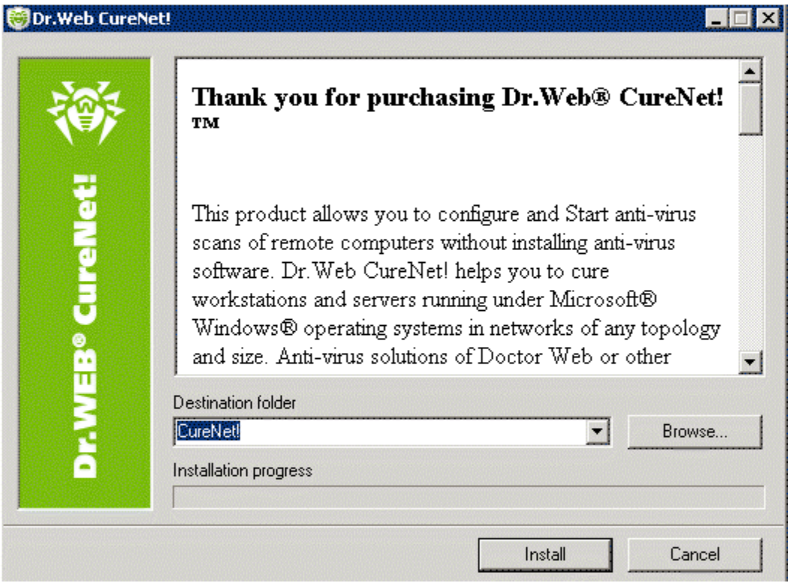
`CureNet!.exe` is a self-extracting archive and it doesn't require installation. All you need to do is to select a location to which the archive's contents will be extracted. The default folder name is CureNet!, but you can change it for a name you like. If you extract the archived files onto a USB flash drive or to any other removable data-storage device, you will be able to carry Dr.Web CureNet! with you wherever you go to come to your aid in emergency situations.

Product repository files and the key file will be extracted into the destination folder.



Language
Reports
Repository
CureNet.exe
CureNet.log
drweb32.key
en-drwcn.chm
ru-drwcn.chm

To continue installation press the **Install** button.



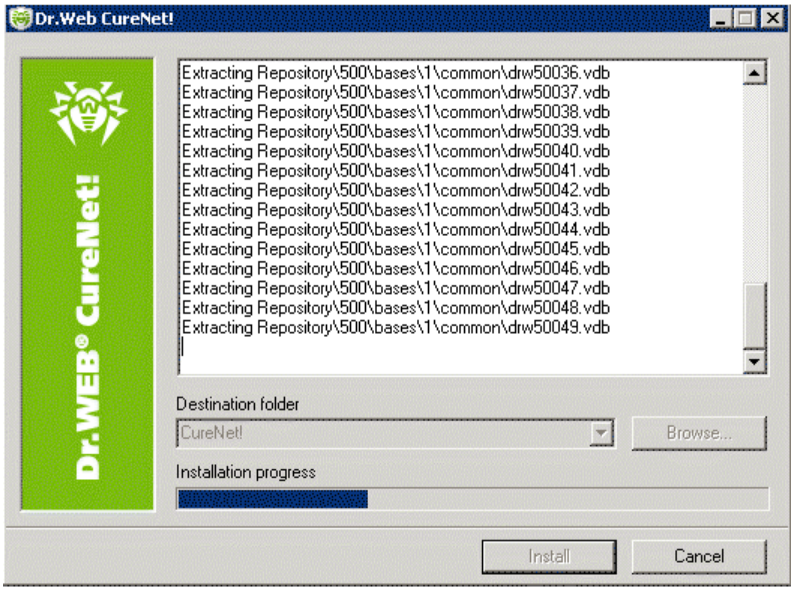
Dr.Web CureNet!

Thank you for purchasing Dr.Web® CureNet! ™

This product allows you to configure and Start anti-virus scans of remote computers without installing anti-virus software. Dr.Web CureNet! helps you to cure workstations and servers running under Microsoft® Windows® operating systems in networks of any topology and size. Anti-virus solutions of Doctor Web or other

Destination folder: CureNet!

Installation progress



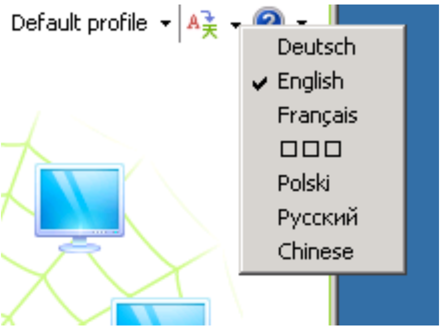
Dr.Web CureNet!

```
Extracting Repository\500\bases\1\common\drw50036.vdb
Extracting Repository\500\bases\1\common\drw50037.vdb
Extracting Repository\500\bases\1\common\drw50038.vdb
Extracting Repository\500\bases\1\common\drw50039.vdb
Extracting Repository\500\bases\1\common\drw50040.vdb
Extracting Repository\500\bases\1\common\drw50041.vdb
Extracting Repository\500\bases\1\common\drw50042.vdb
Extracting Repository\500\bases\1\common\drw50043.vdb
Extracting Repository\500\bases\1\common\drw50044.vdb
Extracting Repository\500\bases\1\common\drw50045.vdb
Extracting Repository\500\bases\1\common\drw50046.vdb
Extracting Repository\500\bases\1\common\drw50047.vdb
Extracting Repository\500\bases\1\common\drw50048.vdb
Extracting Repository\500\bases\1\common\drw50049.vdb
```

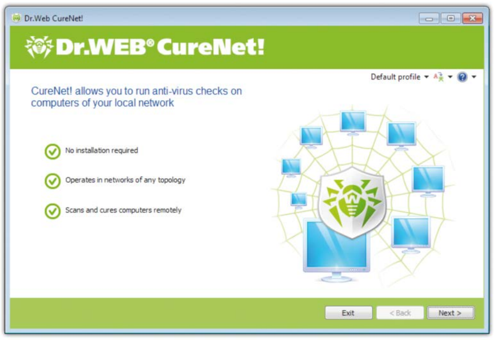
Destination folder: CureNet!

Installation progress

4. Press the button in the right upper corner of the subsequent window to select the localization language.



If you have a configuration file saved from previous scanning sessions and you would like to use it, press the **Standard profile** button in the right upper corner to load it.



CureNet! allows you to run anti-virus checks on computers of your local network

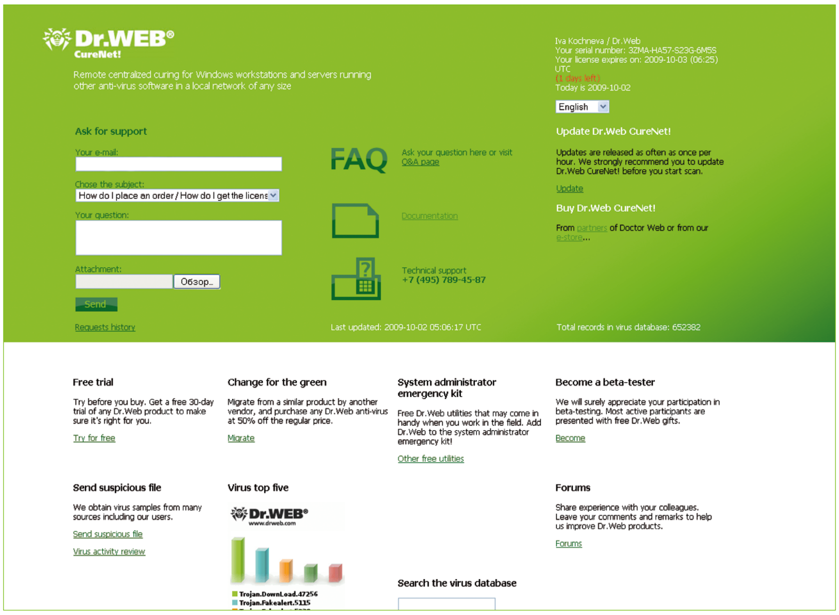
✓ No installation required

✓ Operates in networks of any topology

✓ Scans and cures computers remotely

If you have any questions, press the ? ▾. button. Select **Help** in the context menu to view the **User manual**. Selecting **My Dr.Web** will direct you to your personal page from which you can submit support requests.

Besides, on the personal page you can also select **About** to view information about your license.



Remote centralized curing for Windows workstations and servers running other anti-virus software in a local network of any size

Iva Kochneva / Dr.Web
Your serial number: 3ZMA-HA57-S23G-6M5S
Your license expires on: 2009-10-03 (06:25) UTC
(1 days left)
Today is 2009-10-02

Ask for support

Your e-mail:

Chose the subject: How do I place an order / How do I get the licens

Your question:

Attachment:

Requests history

Ask your question here or visit Q&A page

Documentation

Technical support
+7 (495) 789-45-87

Last updated: 2009-10-02 05:06:17 UTC

Update Dr.Web CureNet!

Updates are released as often as once per hour. We strongly recommend you to update Dr.Web CureNet! before you start scan.

Update

Buy Dr.Web CureNet!

From partners of Doctor Web or from our e-store...

Total records in virus database: 652382

Free trial

Try before you buy. Get a free 30-day trial of any Dr.Web product to make sure it's right for you.

Try for free

Change for the green

Migrate from a similar product by another vendor, and purchase any Dr.Web anti-virus at 50% off the regular price.

Migrate

System administrator emergency kit

Free Dr.Web utilities that may come in handy when you work in the field. Add Dr.Web to the system administrator emergency kit!

Other free utilities

Become a beta-tester

We will surely appreciate your participation in beta-testing. Most active participants are presented with free Dr.Web gifts.

Become

Send suspicious file

We obtain virus samples from many sources including our users.

Send suspicious file

Virus activity review

Virus top five

Trojan.DownLoad.47256
Trojan.Fakealert.5115

Search the virus database

Forums

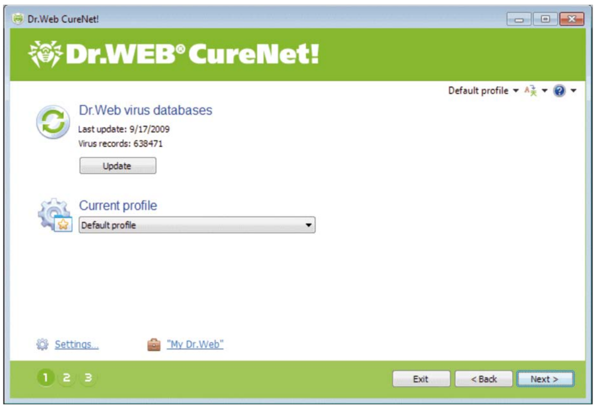
Share experience with your colleagues. Leave your comments and remarks to help us improve Dr.Web products.

Forums

Press **Next** to continue.

5. Press the **Update** button to update virus databases.

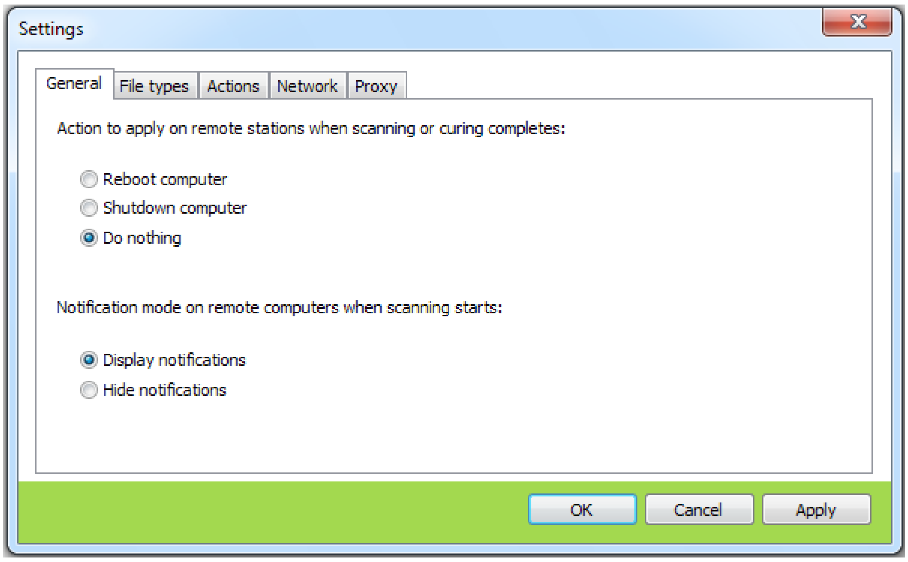
Caution! Success in detection and neutralization of viruses depends greatly on virus definitions in the database, therefore it is strongly recommended to update the databases whenever you launch Dr.Web CureNet!.



Dr.Web virus databases
Last update: 9/17/2009
Virus records: 638471

Current profile: Default profile

If you want to change default settings, click on the **Settings** button.



Action to apply on remote stations when scanning or curing completes:

○ Reboot computer
○ Shutdown computer
● Do nothing

Notification mode on remote computers when scanning starts:

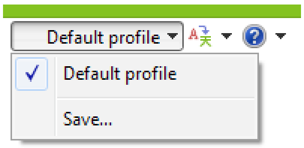
● Display notifications
○ Hide notifications

In the **Actions** tab you can select actions that will be performed with malicious objects of different types. **Move** is set as a default action to be performed upon detection of malicious objects of most types.

It should also be noted that different lists of applicable actions are specified for different types of malicious objects. For example, while the list for infected files contains **Report**, **Cure**, **Delete**, **Rename** and **Move** options, **Cure** won't be available for incurable objects.

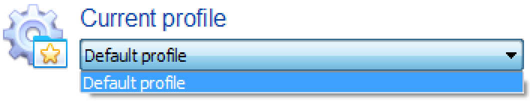
Caution! A system restart is necessary to cure many viruses, however the **Restart** station option (**General** tab) is disabled by default since forced rebooting may interfere with user experience. If a virus is detected in a system, it is recommended to notify users and scan all networked machines.

To save the settings select the **Standard profile** and choose **Save** in the subsequent menu.



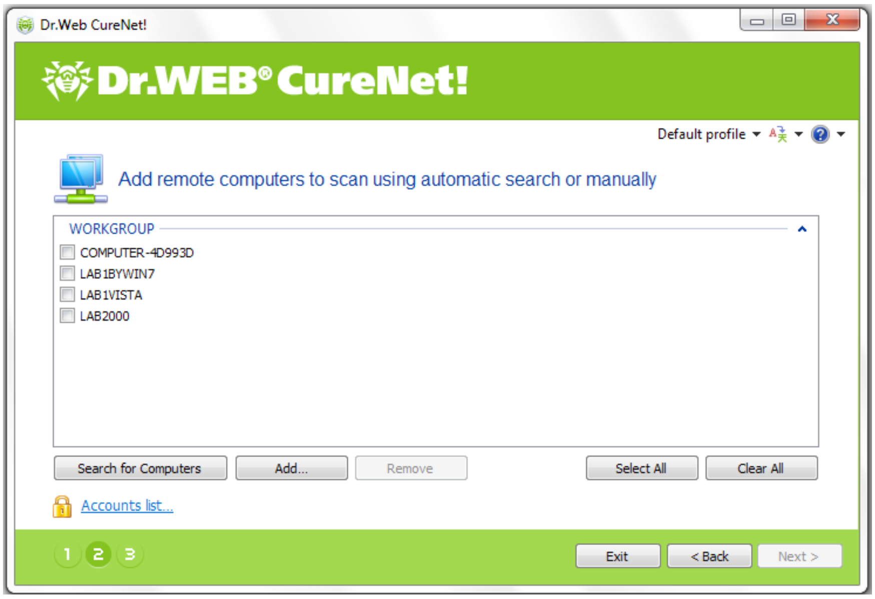
Caution! It is recommended to use default settings since all Doctor Web's products come with settings ensuring optimal performance.

If you have saved profiles, click on the **Current profile** and choose the profile you need.



Press **Next** to continue.

6. In the subsequent window you need to create a list of networked computers that will be scanned for viruses.

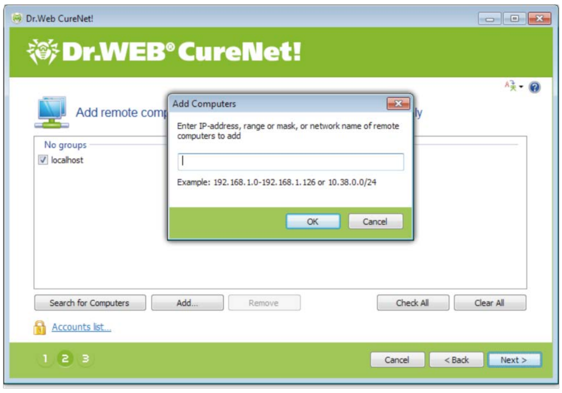


Add remote computers to scan using automatic search or manually

WORKGROUP

- □ COMPUTER-4D993D
- □ LAB1BYWIN7
- □ LAB1VISTA
- □ LAB2000

Click automatic search to **Search for computers** in the network. If you wish to create the list manually, press the **Add** button and enter the address of a target machine or the range of addresses within which systems will be searched for.



Add Computers

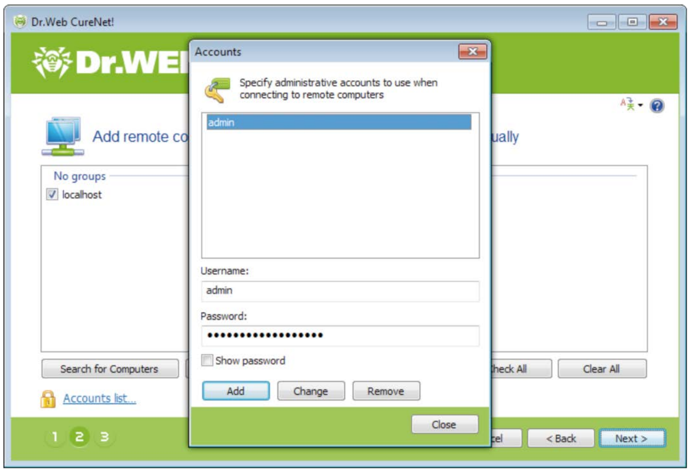
Enter IP-address, range or mask, or network name of remote computers to add

Example: 192.168.1.0-192.168.1.126 or 10.38.0.0/24

No groups

- ☑ localhost

If computers in your network are not in the domain, press the **Connection passwords** button and enter access passwords for respective target machines in the subsequent window.



Accounts

Specify administrative accounts to use when connecting to remote computers

admin

Username: admin

Password: ••••••••••••••••••

□ Show password

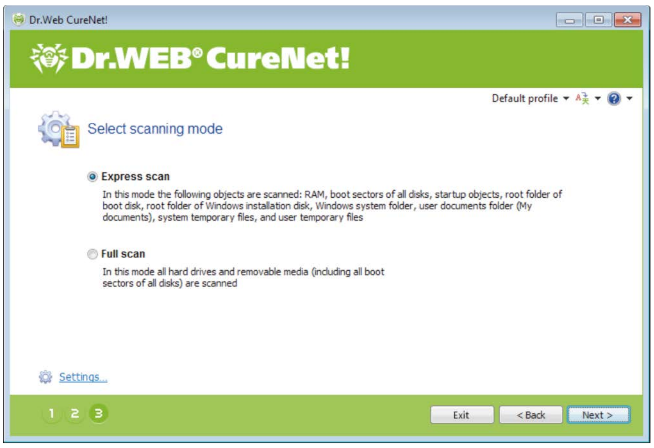
No groups

- ☑ localhost

Press **Next** to continue.

7. In the subsequent window choose the type of scanning: express or full.

Caution! Choosing the **Express scan** will instruct the anti-virus to scan only system directories and running processes which doesn't guarantee that scanning and curing (if infection is detected) will be complete. For example, some viruses running in the system may infect clean files that have already been scanned.



Select scanning mode

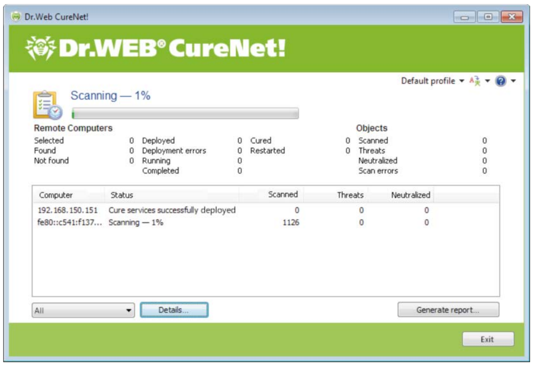
● Express scan

In this mode the following objects are scanned: RAM, boot sectors of all disks, startup objects, root folder of boot disk, root folder of Windows installation disk, Windows system folder, user documents folder (My documents), system temporary files, and user temporary files

○ Full scan

In this mode all hard drives and removable media (including all boot sectors of all disks) are scanned

Press the **Start** button to continue.



Scanning — 1%

Remote Computers

Selected	0	Deployed	0	Cured	0		
Found	0	Deployment errors	0	Restarted	0		
Not found	0	Running	0				
		Completed	0				

Objects

Scanned	0
Threats	0
Neutralized	0
Scan errors	0

Computer	Status	Scanned	Threats	Neutralized
192.168.150.151	Cure services successfully deployed	0	0	0
fe80::c541:f137...	Scanning — 1%	1126	0	0

This window displays the progress of scanning performed on remote computers and its results. The statistics does not depend on the quality of the connection between computers. Even if the connection is interrupted, Dr.Web CureNet! will update statistics upon reconnecting.

Caution! It is not recommended to stop scanning before it is completed.

Running scanning processes feature self-defence mechanisms protecting them against malware.

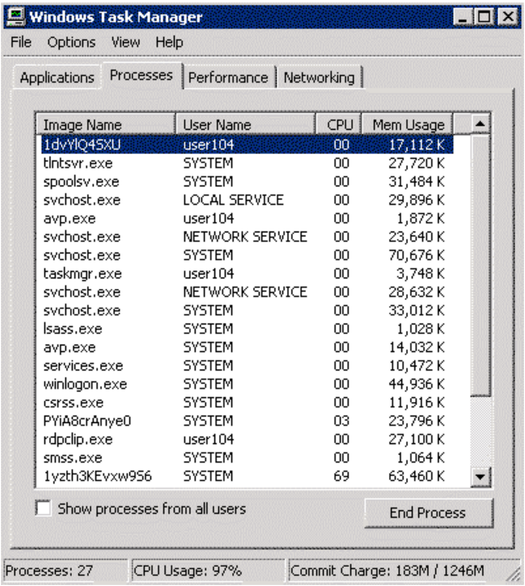
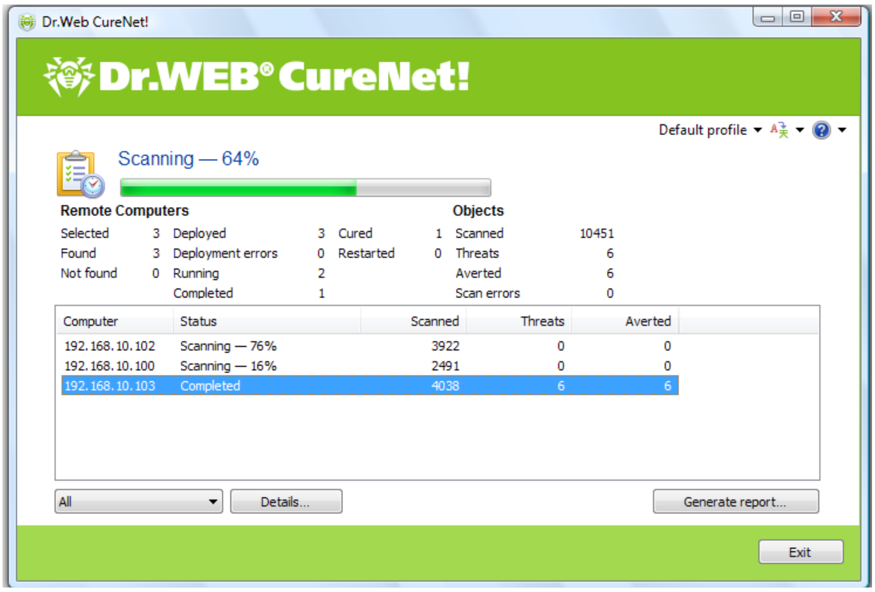


Image Name	User Name	CPU	Mem Usage
1dvYlQ4SXU	user104	00	17,112 K
tlntsvr.exe	SYSTEM	00	27,720 K
spoolsv.exe	SYSTEM	00	31,484 K
svchost.exe	LOCAL SERVICE	00	29,896 K
avp.exe	user104	00	1,872 K
svchost.exe	NETWORK SERVICE	00	23,640 K
svchost.exe	SYSTEM	00	70,676 K
taskmgr.exe	user104	00	3,748 K
svchost.exe	NETWORK SERVICE	00	28,632 K
svchost.exe	SYSTEM	00	33,012 K
lsass.exe	SYSTEM	00	1,028 K
avp.exe	SYSTEM	00	14,032 K
services.exe	SYSTEM	00	10,472 K
winlogon.exe	SYSTEM	00	44,936 K
csrss.exe	SYSTEM	00	11,916 K
PYiA8crAnye0	SYSTEM	03	23,796 K
rdpclip.exe	user104	00	27,100 K
smss.exe	SYSTEM	00	1,064 K
1yzth3KEvxw9S6	SYSTEM	69	63,460 K

Processes: 27 CPU Usage: 97% Commit Charge: 183M / 1246M

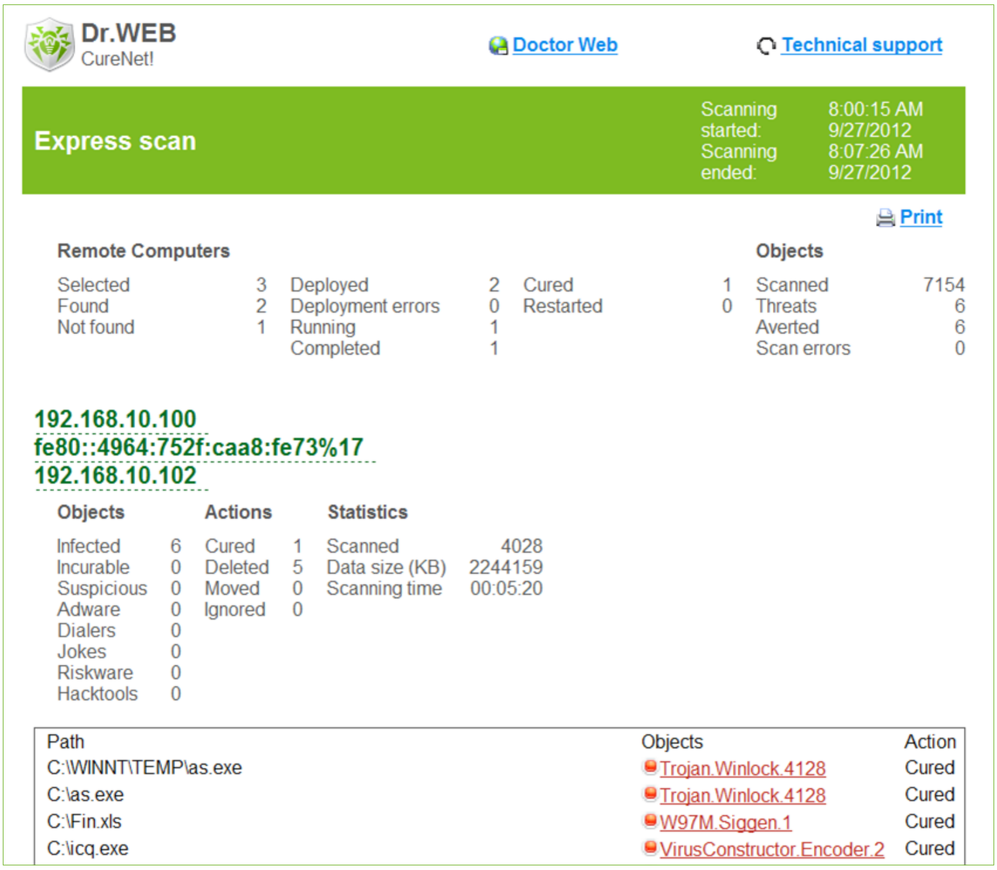


Scanning — 64%

Remote Computers						Objects	
Selected	3	Deployed	3	Cured	1	Scanned	10451
Found	3	Deployment errors	0	Restarted	0	Threats	6
Not found	0	Running	2			Averted	6
		Completed	1			Scan errors	0

Computer	Status	Scanned	Threats	Averted
192.168.10.102	Scanning — 76%	3922	0	0
192.168.10.100	Scanning — 16%	2491	0	0
192.168.10.103	Completed	4038	6	6

Click on the **Generate report** button to create a network scanning report.



Express scan

Scanning started: 8:00:15 AM 9/27/2012
Scanning ended: 8:07:26 AM 9/27/2012

Remote Computers						Objects	
Selected	3	Deployed	2	Cured	1	Scanned	7154
Found	2	Deployment errors	0	Restarted	0	Threats	6
Not found	1	Running	1			Averted	6
		Completed	1			Scan errors	0

192.168.10.100

fe80::4964:752f:caa8:fe73%17

192.168.10.102

Objects		Actions		Statistics	
Infected	6	Cured	1	Scanned	4028
Incurable	0	Deleted	5	Data size (KB)	2244159
Suspicious	0	Moved	0	Scanning time	00:05:20
Adware	0	Ignored	0		
Dialers	0				
Jokes	0				
Riskware	0				
Hacktools	0				

Path	Objects	Action
C:\WINNT\TEMP\as.exe	Trojan.Winlock.4128	Cured
C:\as.exe	Trojan.Winlock.4128	Cured
C:\Fin.xls	W97M.Siggen.1	Cured
C:\icq.exe	VirusConstructor.Encoder.2	Cured

Press **Exit** to close the program.

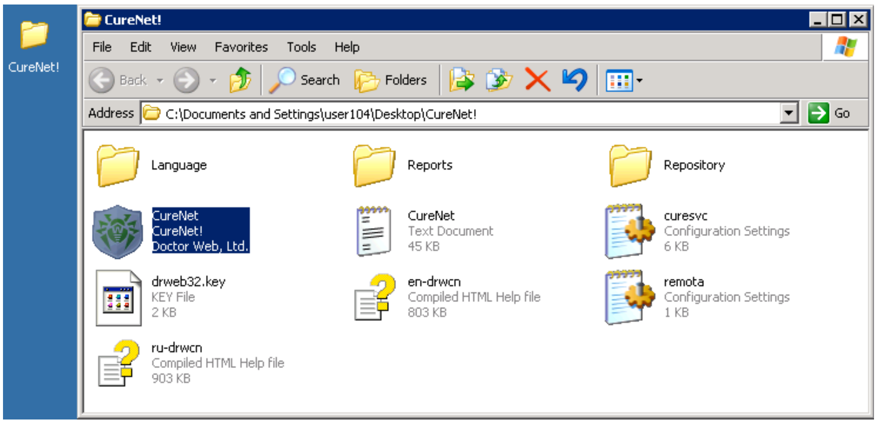
For detailed information about the product, its configuration, scanning, use of profiles refer to the Dr.Web CureNet! administrator manual

Using Dr.Web CureNet!

It is recommended to perform regular anti-virus scans of a system. In particular, files on disks scanned by the file monitor, may contain viruses that weren't known to the anti-virus when it scanned the files.

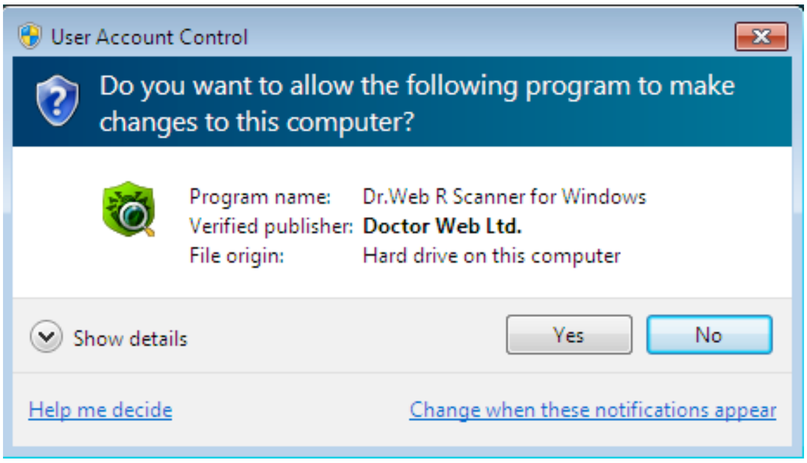
Perform a scan:

1. Open the folder where files of Dr.Web CureNet! were saved when it was launched for the first time. By default the files are saved to the CureNet folder on the desktop.



Address: C:\Documents and Settings\user104\Desktop\CureNet!

2. If you are using Windows 7, you will need to press **Yes** to confirm that you want the program to start.

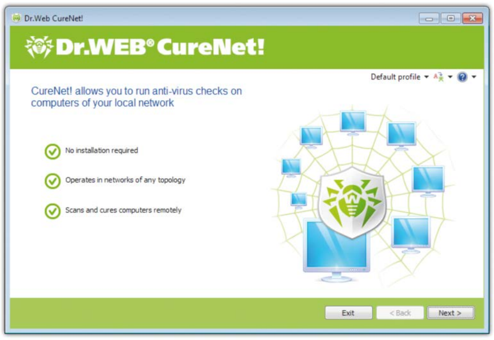


User Account Control

Do you want to allow the following program to make changes to this computer?

Program name: Dr.Web R Scanner for Windows
Verified publisher: **Doctor Web Ltd.**
File origin: Hard drive on this computer

Once you have launched DR.Web CureNet! you may proceed with scanning as described above.



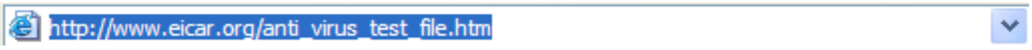
Dr.Web CureNet!

CureNet! allows you to run anti-virus checks on computers of your local network

- No installation required
- Operates in networks of any topology
- Scans and cures computers remotely

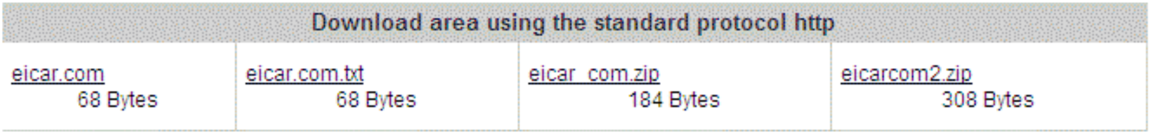
Product operation testing

1. To get a test virus, open your browser and go to



http://www.eicar.org/anti_virus_test_file.htm

2. Scroll down the page until your reach the following text:



Download area using the standard protocol http			
eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

Select any of the files available for downloading, e.g. choose the first one – eicar.com.

3. Save the downloaded file on the desktop of the target machine.

Caution! If you use Dr.Web CureNet! as an addition to an anti-virus from another vendor, disable the anti-virus prior to saving the file.

4. Run Dr.Web CureNet! and perform anti-virus scanning.

125124, Russia, Moscow, 3d street Yamskogo polya 2-12A
Phone: +7 (495) 789-45-87, +7 (495) 789-45-86 (support)
Fax: +7 (495) 789-45-97

www.drweb.com
www.freedrweb.com
www.av-desk.com
www.drweb-curenet.com