
Dr.WEB®
CureNet!
Defend what you create
when your network`s
going up in smoke
CureNet!
Centrally managed
network utility for remote
scanning and curing of local
networks` workstations and servers
under Windows, including those running
other anti-virus software
http://products.drweb.com/curenet/

No viruses in your network? Are you sure?

Better make a quality-test of your anti-virus with Dr.Web CureNet! and be happy!

It has become a common practice for many companies with high information security standards to use anti-virus products from different vendors to protect their workstations, servers and gateways in the corporate networks.

If computers in your network run an anti-virus from another vendor but you doubt its efficiency or you have a comfirmed infection case, run **Dr.Web CureNet!** without removing your main anti-virus. **Dr.Web CureNet!** will scan all hosts in the network and cure them if necessary.

Dr.Web CureNet! comes to the rescue when others fail

Dr.Web CureNet! profile

Product	**Dr.Web CureNet!**
Intended use	1. Remote centralized emergency scan and curing for Windows workstations and servers when other anti-virus software have failed. 2. Quality-test for anti-viruses from other vendors.
Product description	http://products.drweb.com/curenet/
Supported OS	MS Windows 2012 / 8, 8.1 (Professional/Enterprise) / 2008 SP2 / 7 (Professional/Enterprise/Ultimate) / 2008 / Vista SP1 (Business/Enterprise/Ultimate) / 2003 SP1 / XP Professional SP2 (32- and 64-bit architecture)
What is "My Dr.Web"?	This is your personal area where individual **Dr.Web CureNet!** download links are stored as long as your subscription is valid. You can also use "My Dr.Web" to contact the technical support, submit a suspicious file for analysis and use other services.
Licensing	The utility is licensed per number of workstations (at least 5) for 1, 2, or 3 years.
Demo	Apart from being a perfect anti-virus emergency solution **Dr.Web CureNet!** can also be used as a diagnosis tool. A free demo mode allows you to scan computers in the network at any moment to make sure that the installed anti-virus hasn't "overlooked" something. Curing is not available in the demo mode. Ask for demo now! http://download.drweb.com/demoreq/
System requirements	Master ■ Any computer running Windows 2012/8, 8.1 (Professional/Enterprise)/2008 SP2/7 (Professional/Enterprise/Ultimate)/2008/Vista SP1 (Business/Enterprise/Ultimate)/2003 SP1/XP Professional SP2 (32- and 64-bit architecture) ■ Free RAM: at least 360 MB. ■ Free disk space: at least 200 MB. ■ A TCP/IP connection to all target hosts. ■ Internet access: to update the virus databases and components of Dr.Web CureNet!. Scanner ■ Any PC running MS Windows XP Professional and later versions, except for Windows® Server 2003 x64 Edition and Windows® XP Professional SP2 x64 Edition. ■ Free RAM: at least 360 MB. ■ Free disk space: at least 200 MB.
Where to buy?	Off-line: ask your local Dr.Web partner: http://partners.drweb.com Online: http://estore.drweb.com

Benefits

Compliance with corporate security policies

Dr.Web CureNet! doesn't require a running server or any additional software. It doesn't interrupt business routines and conforms to the corparate security policies. Dr.Web scanners for Windows are distributed between target machines. Once the scanning is completed, all files related to the scanners are deleted. As a bonus option, **Dr.Web CureNet!** can be launched even from a USB data-storage device.

Internet connection not required

Dr.Web CureNet! is not a web-service and therefore doesn't use Internet to distribute scanner software between computers. It makes the distribution process and scanning faster and independent from Internet connection bandwidth. **Dr.Web CureNet!** can even be used in networks that do not have access to the Internet.

Complete confidentiality

Dr.Web CureNet! doesn't send or receive data from/to Doctor Web servers and statistics regarding operation of the anti-virus in the corporate network is never sent to the vendor. A report is created on the computer of the system administrator in the network, so the scan information remains strictly confidential.

Easy administration

Even an inexperienced system administrator can work with the program! **Dr.Web CureNet!** Master Interface presents the scanning procedure as a sequence of steps that are very easy to follow. The administrator can monitor the scanning process real-time. Once curing is completed, an extensive report on actions performed by **Dr.Web CureNet!** scanners is generated on the Master computer.

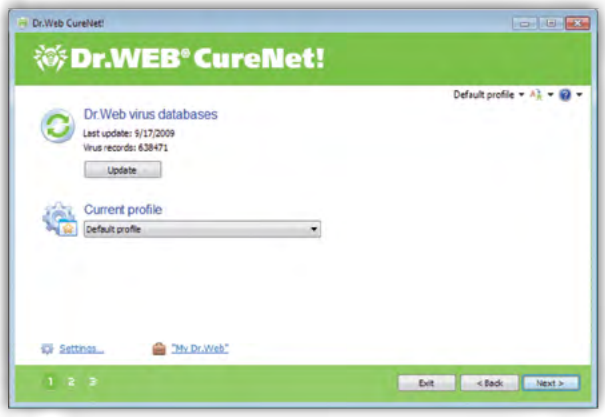
Always up-to-date

The user's individual download link is stored in the "My Dr.Web" area as long as his subscription is valid. Use the link to download the latest version of **Dr.Web CureNet!** any time you need it. You can also launch the updating utility to retrieve the latest updates to the virus database for your running **Dr.Web CureNet!**

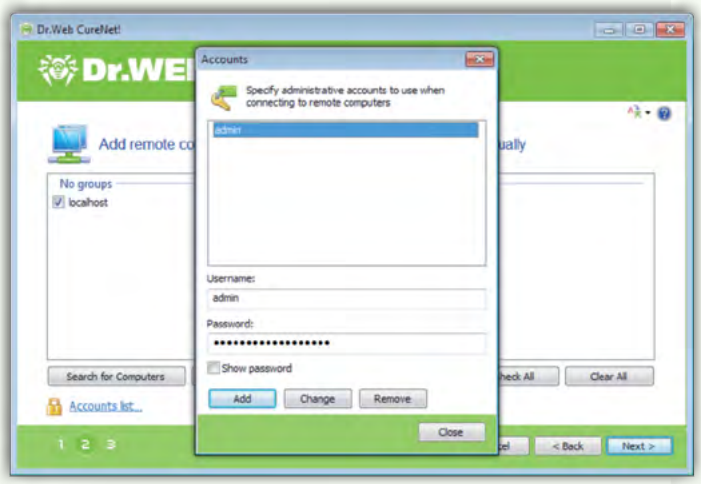
How it works? As simple, as ABCD

A. Download **Dr.Web CureNet!** distribution from your personal area "My Dr.Web ".

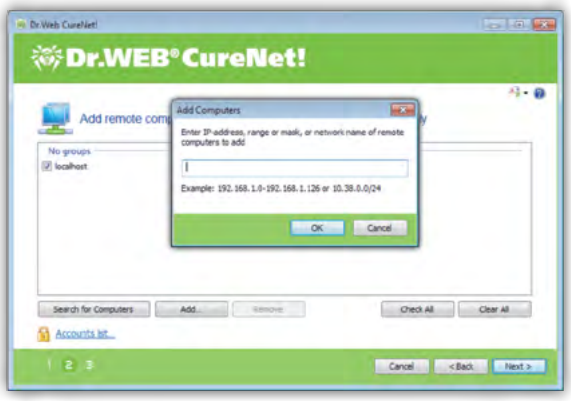
B. The Master package is downloaded with actual virus database, but when using **Dr.Web CureNet!** next time do not forget to update both **Dr.Web CureNet!** and the virus database.



C. Search for stations and launch of Dr.Web for Windows scanners on target hosts is performed remotely using the **Dr.Web CureNet!** Master. The Master is a Windows application that can be launched from any computer connected to the network. User account names and passwords list can be saved in a customized profile to ensure repeated scans of the network if necessary.



D. The Master scans the network for connected hosts before the anti-virus software is distributed to workstations.
You can choose to perform scanning on all available hosts or select workstations and servers that must be checked for viruses. Hosts are selected by their IP addresses, according to a specified IP address range, a mask or NetBIOS name.

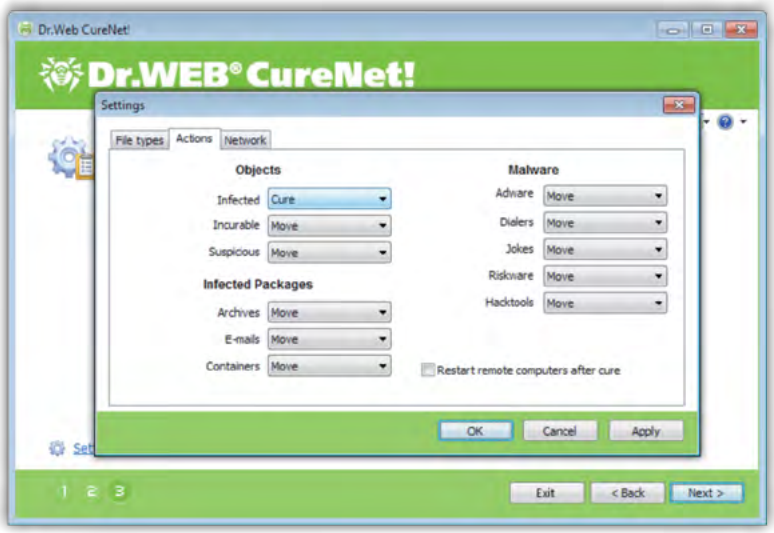


Dr.Web CureIt! is ready to scan and cure your network!

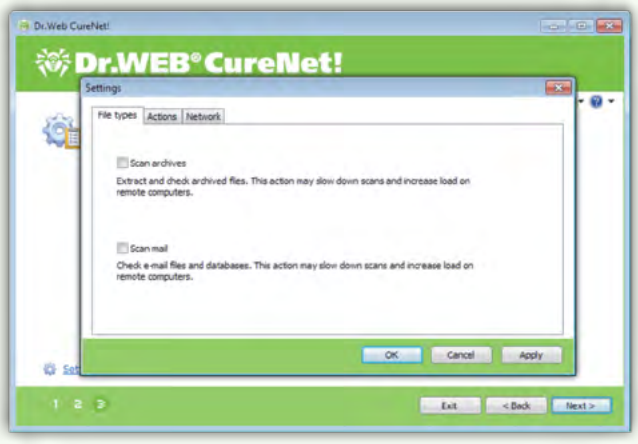
Scan and cure options

Two types of scanning – Express and full – allow specifying the necessary scanning depth. In most cases default settings are an optimum choice.

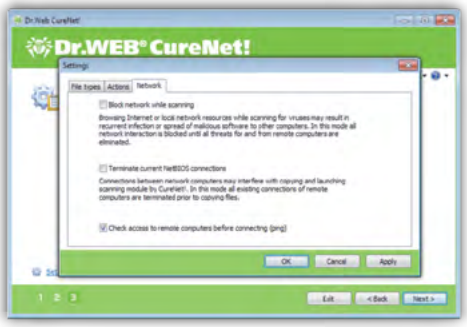
Individual scanning configuration allows setting responses of the scanner software to different events.



You can also choose not to scan archives and e-mail files to speed up the scanning process. Suspicious objects can be moved to the quarantine on local machines.

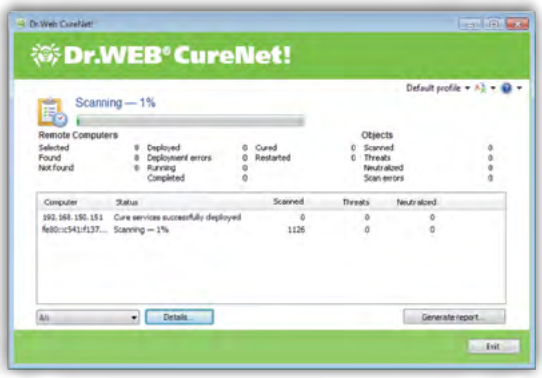


Special network settings allow to block access to workstations being scanned to protect from repeated infections by network worms. This feature does not affect interaction with the Master computer.

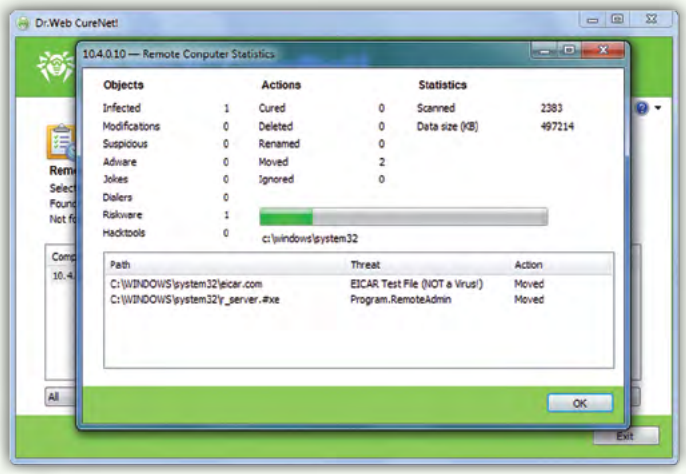


Scanning settings can be saved in XML profiles. You can either use the Default profile, or create your customized ones.

Once scanning is launched, its progress can be viewed in real-time in the statistics tab of **Dr.Web CureNet!** Master.



A report is generated upon completion of the scanning.



Features table

Cures computers and servers	Any PC running MS Windows XP Professional and later versions, except for Windows® Server 2003 x64 Edition and Windows® XP Professional SP2 x64 Edition
Curing in networks disconnected from the Internet	Including IPv6
Network size	No limit
Dr.Web CureNet! Master installation	MS Windows 2012 / 8, 8.1 (Professional/Enterprise) / 2008 SP2 / 7 (Professional/Enterprise/Ultimate) / 2008 / Vista SP1 (Business/Enterprise/Ultimate) / 2003 SP1 / XP Professional SP2 (32- and 64-bit architecture)
Distribution of curing scanners from USB-storage device	■
Installation of Dr.Web scanners for Windows	Installation is not required
Remote centralized launch of scanners in an infected system without its preliminary curing	Industry pacesetter!
Custom scan on remote hosts	■
Pause and end scanning on selected hosts	■
Remote centralized launch of scanners on all hosts/on selected hosts	■
Disabling network access on a target machine during scanning to prevent recurring infection	■
Centralized configuration of actions performed to detected malicious objects	■
Centralized collection of statistics	■
Self-removal of scanners after scanning is completed	■
Export scanning reports	■
Hosts search	
Automatic hosts search ■ IP-addresses ■ IP-address range ■ mask ■ network name	■
Scanning	
Customizable scan profiles	■
Customizable actions for different types of malicious objects (spyware, adware, riskware, paid dialers, jokers)	■
Customizable actions for infected and suspicious objects as well as for objects of other types: cure, move to the quarantine, delete	■
Customizable actions sequences performed to a malicious object if one of the actions can't be applied	■
Choice of actions for infected packages (archives, containers, mail files)	■
Scan of archived files at any nesting level	Industry pacesetter!
Quick scan (scan of main memory, boot sectors of all drives, autorun objects, root directory of boot disk, Windows root directory, Windows system directory, My Documents directory, temporary system directory, temporary user directory)	■
Full scan (scan of all hard drives)	■
Heuristic analyzer	■
Non-signature detection technology complementing traditional signature-based scan and heuristic analyzer	Origins Tracing™
Exclusion of archives from scanning	■
Exclusion of mail files from scanning	■

Self-protection from malicious anti-antivirus programs	
Self-protection	Dr.Web SelfPRotect
Curing	
Detection and neutralization of viruses disguised with unknown packers	FLY-CODE
Scan of scripts including VB-Script, Java Script	■
Scan of logical drives	■
Scan of mail files	■
Detection and neutralization of running malicious programs of the following types: ■ worms ■ rootkits ■ File viruses ■ Trojans horses ■ bodiless and stealth-viruses ■ polymorphic viruses ■ macro-viruses and malicious programs infecting MS Office documents ■ script-viruses ■ spyware ■ adware ■ hacking tools ■ paid dialers ■ jokers	Best-of-breed at curing active infections!
Updating	
On-demand updating of virus databases and program modules of **Dr.Web CureNet!** over the Internet	■
Virus database size	Optimized number of entries!!!
Update size	Smallest in the industry!!!
Supported languages	
English interface language	■
User manual in English	■
Support	
Free technical support in English	■
Analysis of viruses unknown to Dr.Web	■

Dr.Web – an industry leader in curing viruses

Dr. Web anti-virus functions on infected computers, exceptional resistance to viruses makes it stand out among other anti-viruses.

- Industry pacesetter! Dr.Web has the highest rate of successful curing of active infections in the industry.
- Industry pacesetter! The unique memory scan technologies and outstanding curing capability allow launching Dr.Web in an infected system (without its preliminary curing).

Anti-virus engine

- Only Dr.Web can scan archived files at any nesting level. Even if a malicious object has been archived many times with different data-compression applications, Dr.Web is sure to detect and neutralize the threat.
- Dr.Web technologies and algorithms allow reliable detection of packed objects, their detailed analysis aimed at exposing hidden threats. Even if an unknown packer has been used to disguise malware, it will be detected by Dr.Web anyway.
- Dr.Web is an unsurpassable leader in detection and neutralization of complex viruses like MaosBoot, Rustock.C, Sector.
- Blocking a virus in the RAM before it replicates itself to a hard drive lowers the probability for malware to exploit a vulnerability of a third-party application or the operating system itself.
- Dr.Web is capable of detecting and neutralizing viruses that can be found only in RAM and do not exist as files on disks, e.g. Slammer or CodeRed. Dr.Web detects and neutralizes viruses that can be found only in the RAM but don't exist as files on a hard drive. July 2001 saw the epidemics of CodeRed virus and Dr.Web turned out to be the only anti-virus capable of detecting it. Even now few anti-viruses can detect malware like CodeRed or Slammer.

Anti-rootkit

- Dr.Web Shield™ ensures detection of viruses featuring rootkit-technologies that allow them to hide their presence in the system.
- Dr.Web® Shield™ provides the scanner with privileged access to files, registry and other key system components so it would be able to expose rootkits and block self-protection features of rootkits and stealth-viruses.

Detection of unknown threats

- State-of-the-art Dr.Web technologies allow anti-viruses to detect even unknown threats and save your information.
- FLY-CODE is a universal decompression technology that allows detecting viruses disguised by means of packers unknown to Dr.Web. Special entries n the virus database allow the heuristic analyzer to suggest if a packed file contains malicious code. An object detected in such a way gets "Probably Trojan.Packed" added to its name.
- Origins Tracing™ is the cutting-edge non-signature detection technology that ensures a high probability of detection of malicious code that has not been registered in the Dr.Web virus database. It has already proven its efficiency during epidemics that caused data losses to many users of competitive solutions. Origins Tracing™ is added to traditional signature scan and heuristic analysis which significantly improves detection of unknown malware. The Origins Tracing™ technology allowed reducing the size of Dr.Web signature databases and lowered the number of false positives by the heuristic analyzer.
- The heuristic analyzer detects most known threats with its analysis based on criteria typical of various groups of malicious programs. Even if a signature of a virus is not present in the database, the heuristic analyzer will serve as another barrier in the way of an intruder.

Self-protection

- Dr.Web SelfPROtect makes the anti-virus immune to any attempts of malicious programs to disrupt its operation.
- Dr.Web SelfPROtect is implemented as a driver that runs on the lowest system level. It can't be stopped or disabled unless the system is restarted.
- In order to keep the anti-virus operational Dr.Web SelfPROtect can restrict access to files, folders, removable data storage devices and certain branches of the Windows Registry.
- Some anti-viruses modify the Windows kernel (intercept interrupts, change vector tables or use other undocumented features). It may have a negative impact on the stability of a system and path new ways for malicious programs to get into a system. At the same time Dr.Web SelfPROtect maintains security of the anti-virus and doesn't interfere with routines of the Windows kernel.

About Doctor Web

Doctor Web is a Russian IT-security solutions developer. Dr.Web anti-virus is being developed since 1992. The company offers proven anti-virus and anti-spam solutions for businesses, government entities, and personal use. We have a sound track 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.
Dr.Web anti-virus products, based on the unique technology of detection and curing, have been developed by our company to give you the competitive edge, something very few anti-virus vendors can offer. Doctor Web has its own virus-monitoring service and analytical laboratory, guaranteeing a rapid response to new virus threats. Our customer support staff is standing by to help you solve your problems as quickly as possible.

Russia

Doctor Web
3d street Yamskogo polya 2-12A, Moscow, Russia, 125124
Phone: +7 (495) 789-45-87
Fax: +7 (495) 789-45-97
www.drweb.com | www.av-desk.com | www.freedrweb.com

France

Doctor Web France
10-12, avenue de l'Arche, Faubourg de l'Arche 92419 Courbevoie Cedex
www.drweb.fr

Germany

Doctor Web Deutschland GmbH
Deutschland, 63457 Hanau, Rodenbacher Chaussee 6
Phone: +49 (6181) 9060-1210
Fax: +49 (6181) 9060-1212
www.drweb-av.de

Kazakhstan

Doctor Web – Central Asia
Republic of Kazakhstan, 050009, Almaty, Shevchenko, 165b/72g, 910
Phone: +7 (727) 323-62-30, +7 (727) 323-62-31, +7 (727) 323-62-32
www.drweb.kz

Ukraine

Doctor Web Technical Support Centre
01034, Ukraine, Kiev, Myhailovsky, 17
Тел: +38 (044) 279-20-38
www.drweb.com.ua

Japan

Doctor Web Pacific, Inc.
NKF Kawasaki building 2F, 1-2,
Higashida-cho, Kawasaki-ku,
Kawasaki-shi, Kanagawa-ken 210–0005
Тел.: +81(0) 44–201–7711
www.drweb.co.jp