Dr.WEB®
Made in Russia

DEFEND WHAT YOU CREATE

Dr.Web CureNet!

for Windows

Quick Start

https://www.drweb.com

A solution for the remote, centralised curing of Windows PCs and servers, including those running different anti-virus software, regardless of local network size

- Included in the Register of Russian Computer Programs and Databases
- Does not rely on an Internet connection
- Can be launched from any external media or from iPhone/iPod touch

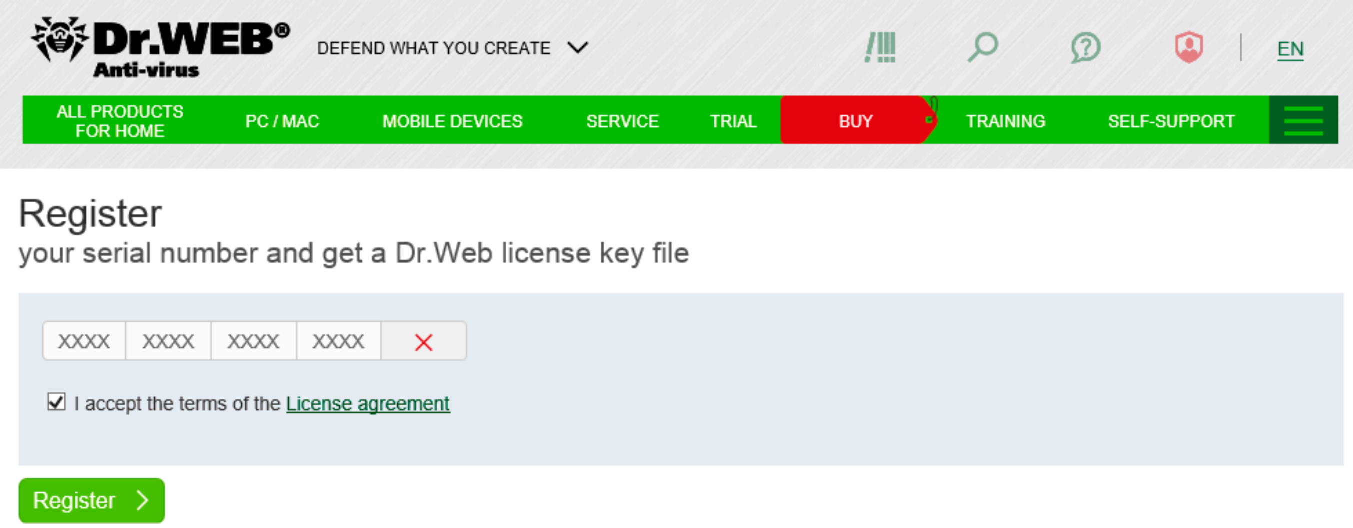
Dr.Web CureNet! Quick Start

With Dr.Web CureNet!, you can perform centrally managed remote anti-virus scanning on your networked computers without installing anti-virus software on the target machines. Dr.Web CureNet! scans personal computers and servers running Microsoft® Windows® in networks of any topology.

Important! Dr.Web CureNet! does not provide resident end-point security. Between scans, computers can get infected by any malicious program. To establish reliable and constant anti-virus security, use software products such as Dr.Web Security Space or Dr.Web Enterprise Security Suite.

Download Dr.Web CureNet!

To download a distribution file, register your serial number at http://products.drweb.com/register.



Register

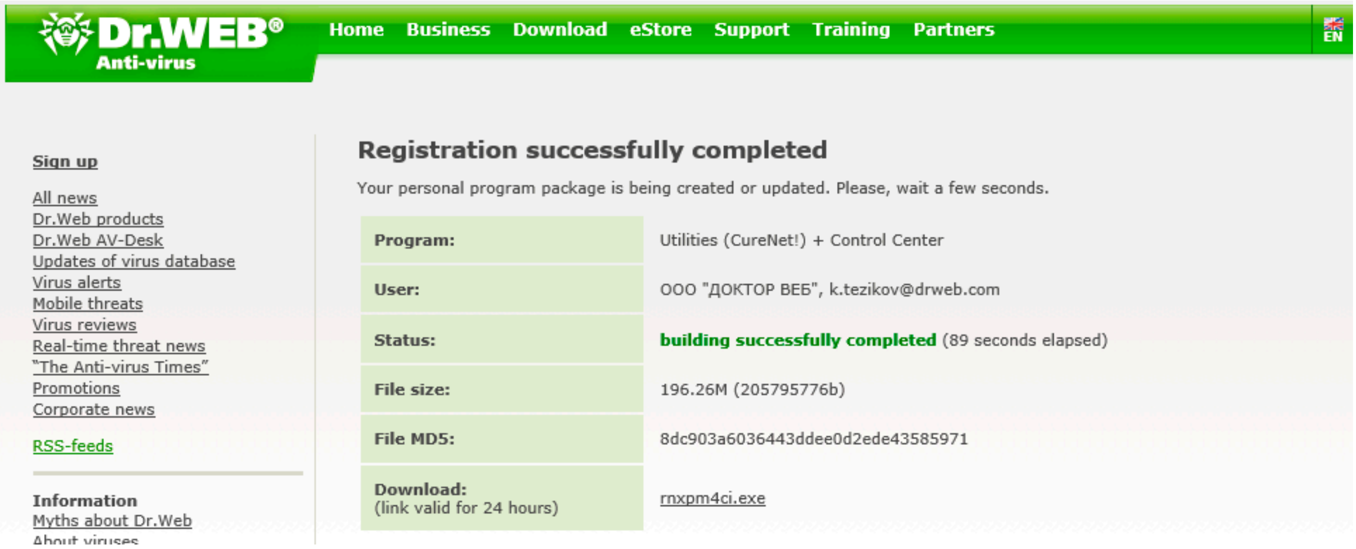
your serial number and get a Dr.Web license key file

XXXX XXXX XXXX XXXX ✕

☑ I accept the terms of the License agreement

Register >

Your individual distribution file will be generated once you complete the registration procedure.



Registration successfully completed

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

Program:	Utilities (CureNet!) + Control Center
User:	ООО "ДОКТОР ВЕБ", k.tezikov@drweb.com
Status:	**building successfully completed** (89 seconds elapsed)
File size:	196.26M (205795776b)
File MD5:	8dc903a6036443ddee0d2ede43585971
Download: (link valid for 24 hours)	rnxpm4ci.exe

Download the created distribution file from your personal account area. From then on, for as long as your license is valid, you will be able to download the latest version of the utility's distribution from your personal account area.

You can get to your personal account area either from the program itself or after entering your serial number at https://support.drweb.com/get+cabinet+link.

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

System requirements

To use Dr.Web CureNet! to scan computers remotely:

- the target machines must be connected to the network;
- there must be an account with the necessary administrative privileges that Dr.Web CureNet! can use to connect to the remote computers;
- ports 139 and 445 must be open in the target systems.

You must have administrator privileges on the applicable PCs and servers to scan your network with the Dr.Web CureNet! anti-virus utility. Remote scanning does not require any additional configuration of your computers provided that they are members of a domain and a domain administrator account is used on them. If a remote computer is not a domain member or a local account is used, for some versions of Windows, remote computers require additional configuration. Detailed configuration information for Windows is described below. You can also watch the video tutorials.

Since changing certain system parameters for remote scanning can lower a remote host's security, it is strongly recommended that you learn how adjusting these parameters affects the system. Otherwise, you should reject the use of remote scanning and launch the anti-virus scanner on the machine locally.

Configuring Windows to launch the Wizard

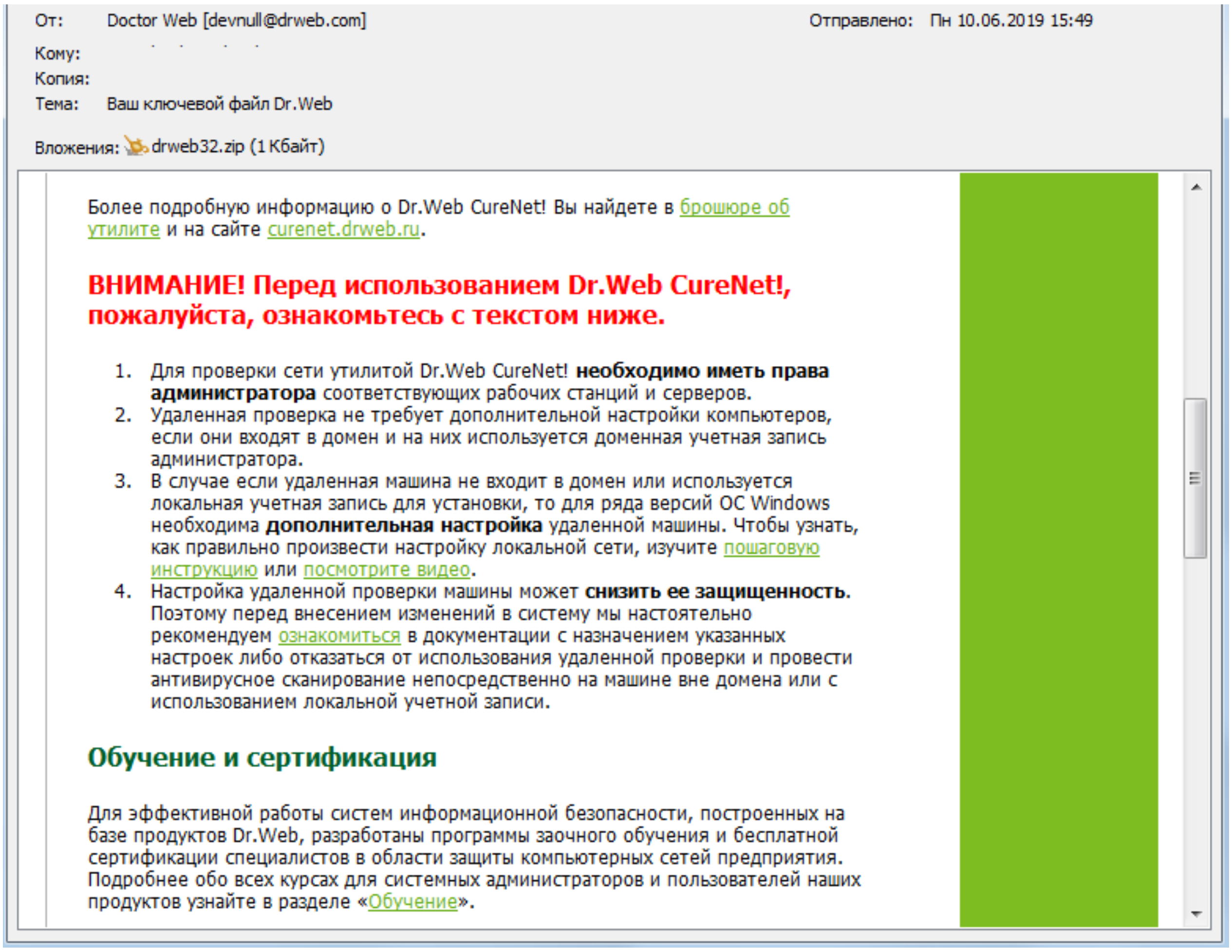
The Wizard incorporated into Dr.Web CureNet! is compatible with the following versions of Windows:

- Windows XP (Professional Service Pack 2 or later)
- Windows Server 2003 Service Pack 1 or later
- Windows Vista (Business, Ultimate, and Enterprise editions) Service Pack 1 or later
- Windows Server 2008
- Windows 7 (Professional, Ultimate, and Enterprise editions)
- Windows Server 2008 R2
- Windows 8 and 8.1 (Professional and Enterprise editions);
- Windows Server 2012
- Windows 10

For the Wizard to be able to operate normally, you must ensure that you have:

1. An Internet connection so that the virus databases and Dr.Web components can be updated.
2. A TCP/IP connection to all the target hosts.

Brief information about Windows' configuration requirements can be found in the letter that was sent to the email address you provided during registration. The full list of requirements is specified in the documentation.



От: Doctor Web [devnull@drweb.com]

Отправлено: Пн 10.06.2019 15:49

Кому:

Копия:

Тема: Ваш ключевой файл Dr.Web

Вложения: drweb32.zip (1 Кбайт)

Более подробную информацию о Dr.Web CureNet! Вы найдете в брошюре об утилите и на сайте curenet.drweb.ru.

ВНИМАНИЕ! Перед использованием Dr.Web CureNet!, пожалуйста, ознакомьтесь с текстом ниже.

1. Для проверки сети утилитой Dr.Web CureNet! **необходимо иметь права администратора** соответствующих рабочих станций и серверов.
2. Удаленная проверка не требует дополнительной настройки компьютеров, если они входят в домен и на них используется доменная учетная запись администратора.
3. В случае если удаленная машина не входит в домен или используется локальная учетная запись для установки, то для ряда версий ОС Windows необходима **дополнительная настройка** удаленной машины. Чтобы узнать, как правильно произвести настройку локальной сети, изучите пошаговую инструкцию или посмотрите видео.
4. Настройка удаленной проверки машины может **снизить ее защищенность**. Поэтому перед внесением изменений в систему мы настоятельно рекомендуем ознакомиться в документации с назначением указанных настроек либо отказаться от использования удаленной проверки и провести антивирусное сканирование непосредственно на машине вне домена или с использованием локальной учетной записи.

Обучение и сертификация

Для эффективной работы систем информационной безопасности, построенных на базе продуктов Dr.Web, разработаны программы заочного обучения и бесплатной сертификации специалистов в области защиты компьютерных сетей предприятия. Подробнее обо всех курсах для системных администраторов и пользователей наших продуктов узнайте в разделе «Обучение».

Configuring Windows to remotely run Dr.Web scanner

General configurations for Windows XP — 10, Windows Server 2003/2008/2012

The system requirements for stations coincide with the requirements for the computer on which the Wizard is run, except for the list of supported operating systems: Windows XP Professional SP2 and later versions, except those listed below for 64-bit systems: Windows Server 2003 x64 Edition and Windows XP Professional SP2 x64 Edition.

- **Windows XP**

  Supported edition — Windows XP Professional. 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

  Versions not supported:

  - Windows XP Starter
  - Windows XP Home Edition

- **Windows 2003**

  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

- **Windows Vista**

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

  Supported versions:

  - Windows Vista Business
  - Windows Vista Enterprise
  - Windows Vista Ultimate

  Versions not supported:

  - Windows Vista Starter
  - Windows Vista Home Basic
  - Windows Vista Home Premium

  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/ru-ru/download/details.aspx?id=15278

- **Windows Server 2008**

  Service Pack 2 must be installed for Windows Server 2008.

  Download Service Pack 2 for Windows 2008:

http://www.microsoft.com/ru-ru/download/details.aspx?id=15278

- **Windows 7**

  Important! Supported versions:

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

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

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

- **Windows Server 2008 R2**

  Service Pack 2 must be installed for Windows 2008.

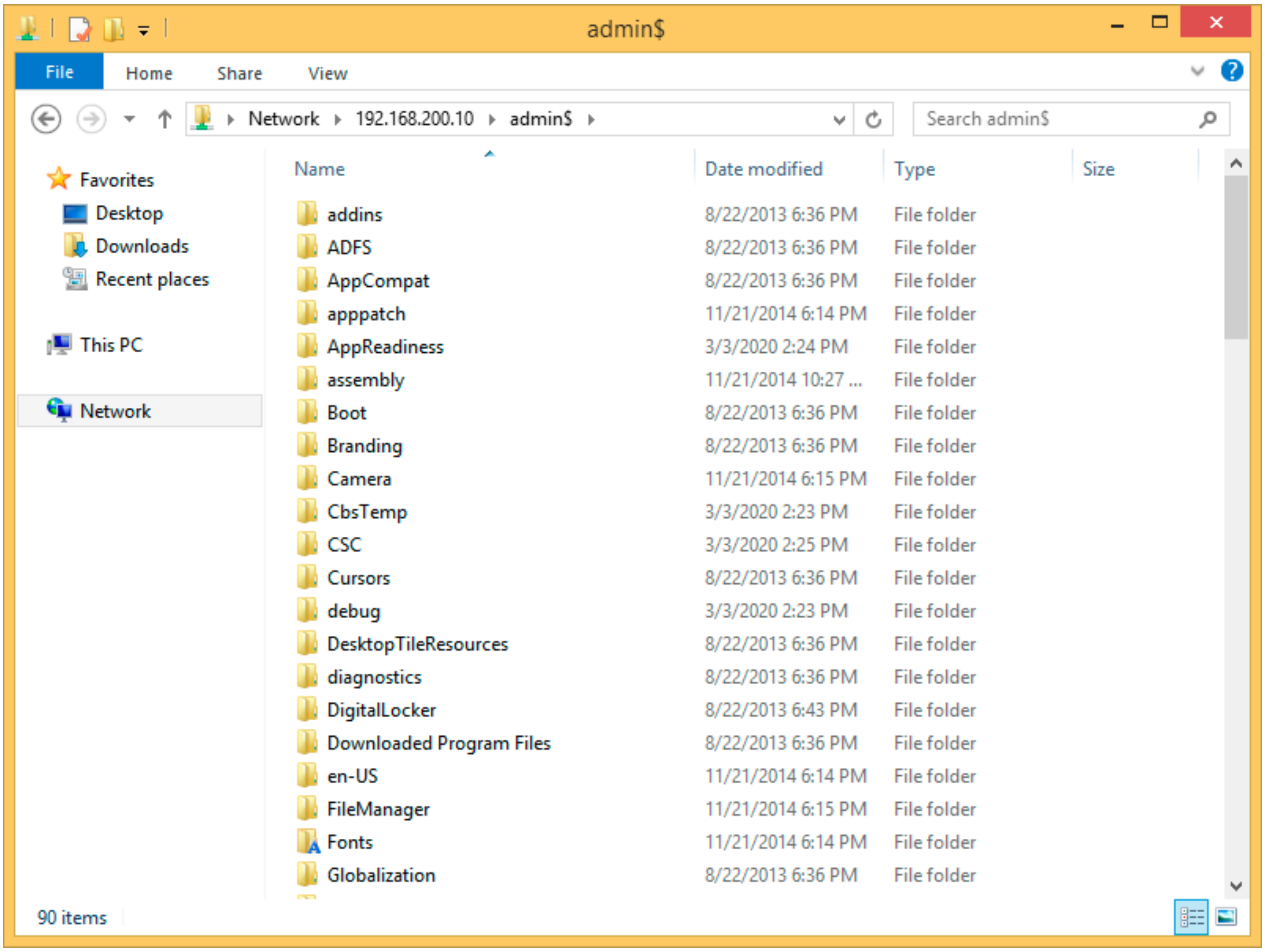
  Download Service Pack 2 for Windows 2008:

  http://www.microsoft.com/ru-ru/download/details.aspx?id=15278

- **Windows 8, 10, Windows 8.1, Windows Server 2012**

Stations do not have to be connected to the Internet.

Make sure that the shared network folder is accessible from the computer. To do this, navigate to the network folder admin$ on the remote computer. Depending on the Windows settings, you may need to enter an administrator login and password. This should open the network folder (see Fig. below).



Name	Date modified	Type	Size
addins	8/22/2013 6:36 PM	File folder	
ADFS	8/22/2013 6:36 PM	File folder	
AppCompat	8/22/2013 6:36 PM	File folder	
apppatch	11/21/2014 6:14 PM	File folder	
AppReadiness	3/3/2020 2:24 PM	File folder	
assembly	11/21/2014 10:27 ...	File folder	
Boot	8/22/2013 6:36 PM	File folder	
Branding	8/22/2013 6:36 PM	File folder	
Camera	11/21/2014 6:15 PM	File folder	
CbsTemp	3/3/2020 2:23 PM	File folder	
CSC	3/3/2020 2:25 PM	File folder	
Cursors	8/22/2013 6:36 PM	File folder	
debug	3/3/2020 2:23 PM	File folder	
DesktopTileResources	8/22/2013 6:36 PM	File folder	
diagnostics	8/22/2013 6:36 PM	File folder	
DigitalLocker	8/22/2013 6:43 PM	File folder	
Downloaded Program Files	8/22/2013 6:36 PM	File folder	
en-US	11/21/2014 6:14 PM	File folder	
FileManager	11/21/2014 6:15 PM	File folder	
Fonts	11/21/2014 6:14 PM	File folder	
Globalization	8/22/2013 6:36 PM	File folder	

If the folder is inaccessible, change the system settings as follows:

In the registry editor (regedit), go to

[HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\LANMANSERVER\PARAMETERS]

Create the 32-bit DWORD value AutoShareWks and assign it a value of 1. Restart the system. The shared folder will become accessible.

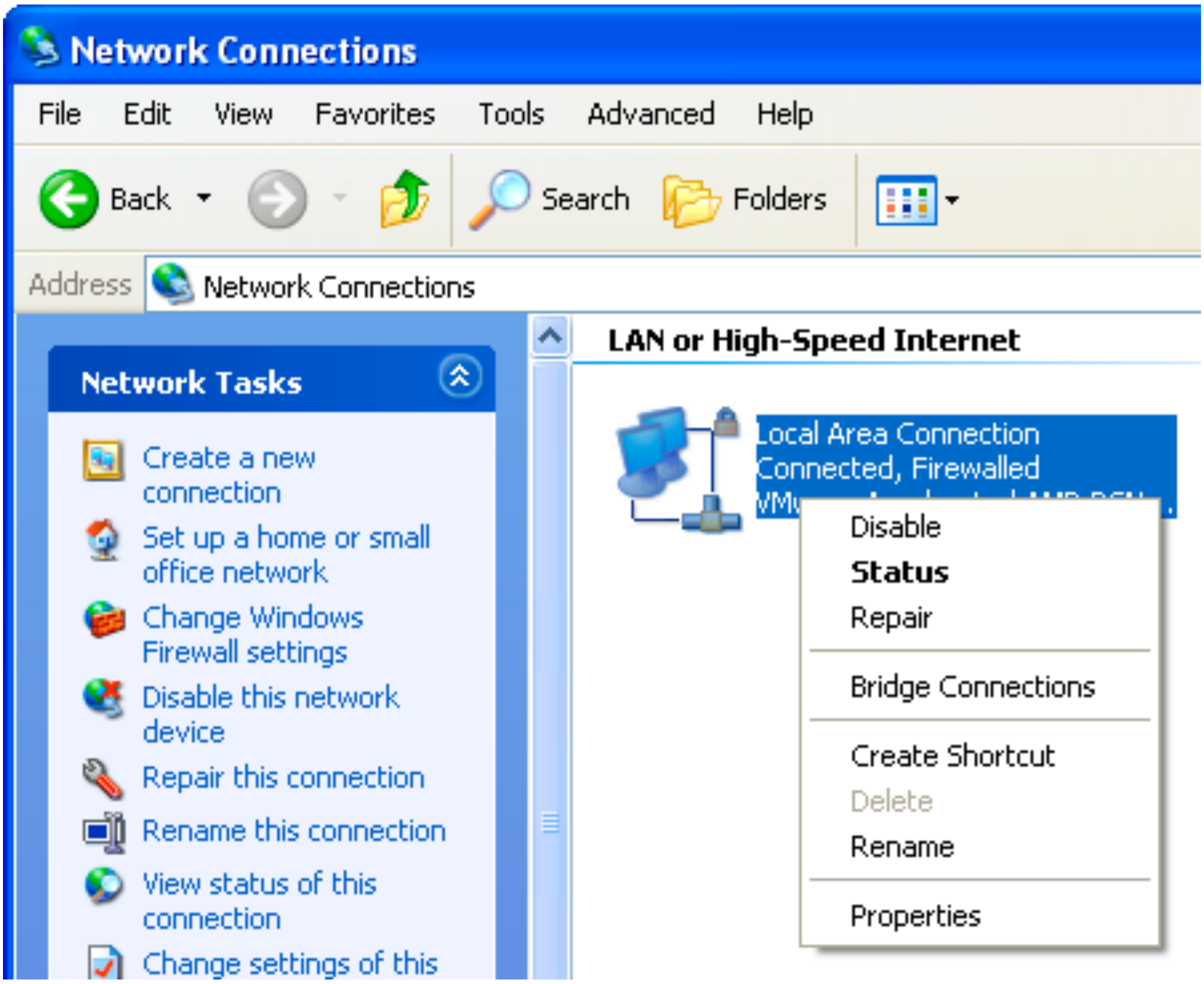
To scan stations, the following conditions must be met simultaneously:

- The **Network discovery** option must be enabled on the station on which the Wizard is launched if you want to use this method to search for stations in the network;
- the station should be accessible over the network;
- the account used for the connection must exist and have sufficient privileges;
- if a firewall is being used to protect the remote computer, you need to specify the additional settings described below;
- UAC restrictions must be disabled if the station is running Windows Vista or a later version of the operating system. If you are using a built-in administrator account, skip this configuration step;
- all the services necessary for the network's operation must be installed and configured.

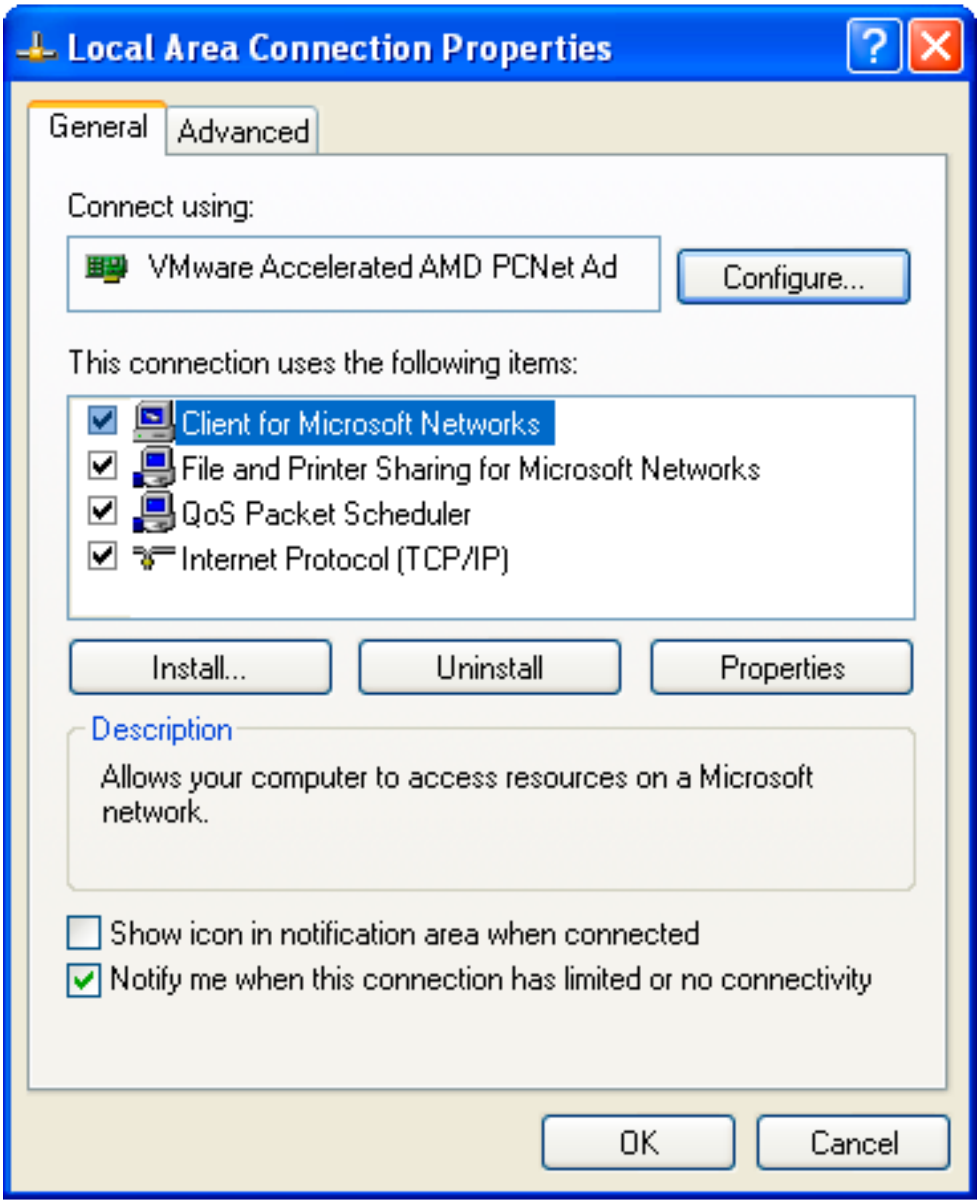
Viewing network settings

1. Start the **Control Panel** on the station, using any of the methods described below:

- for Windows XP/2003Vista, click on **Start** and go to **Control Panel** → **Network Connections** (if this section is not available, click on **Switch to standard view**). Click on the network connection icon. In the drop-down menu, select **Properties**.



Go to the **General** tab.



Local Area Connection Properties

General | Advanced

Connect using:

VMware Accelerated AMD PCNet Ad

This connection uses the following items:

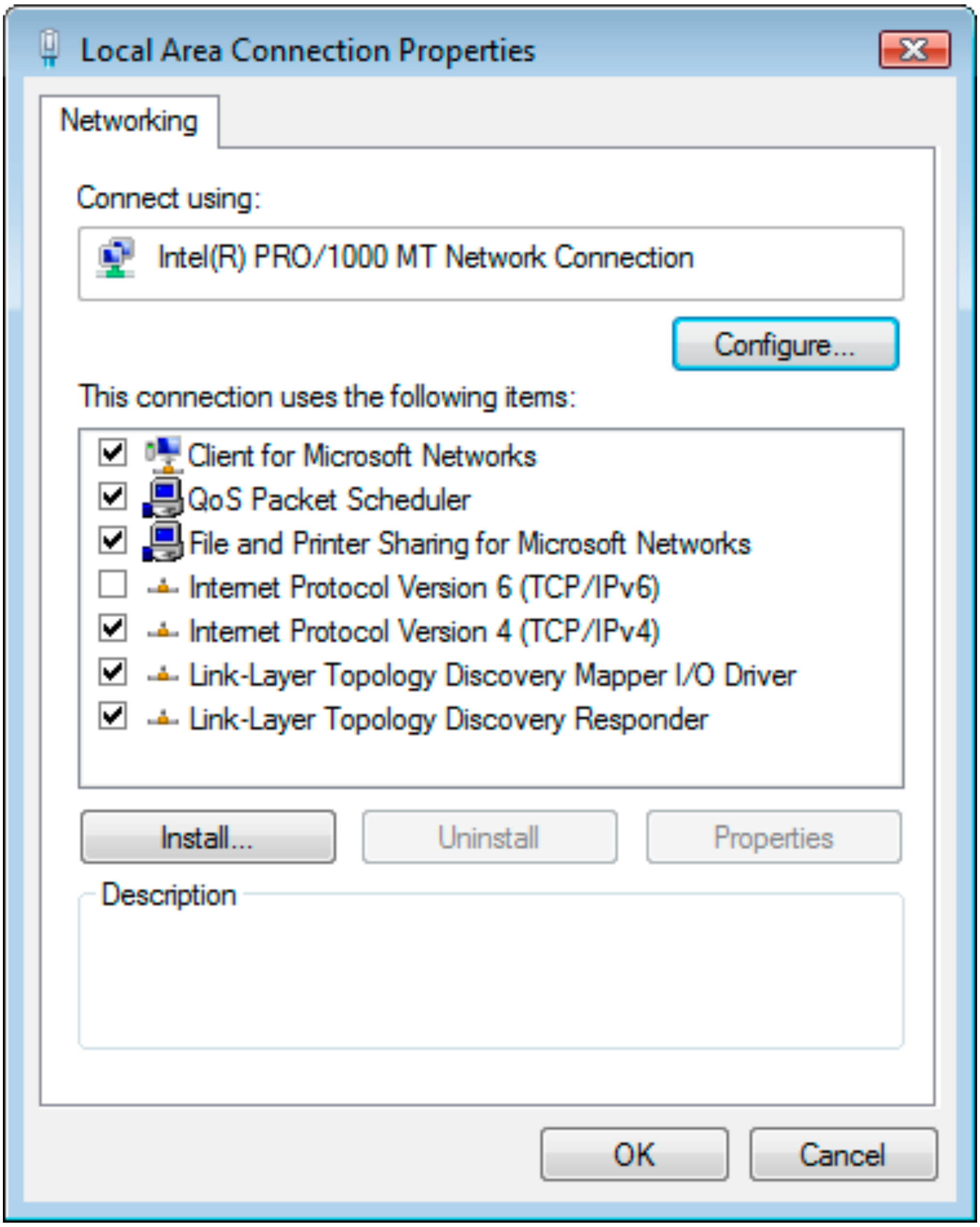
☑ Client for Microsoft Networks
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

Allows your computer to access resources on a Microsoft network.

☐ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

- for Windows Vista, click on **Start** and go to **Control Panel** → **Network and Internet** → **Network and Sharing Center** → **Network management**. Click on the network connection icon. In the drop-down menu, select **Properties**.



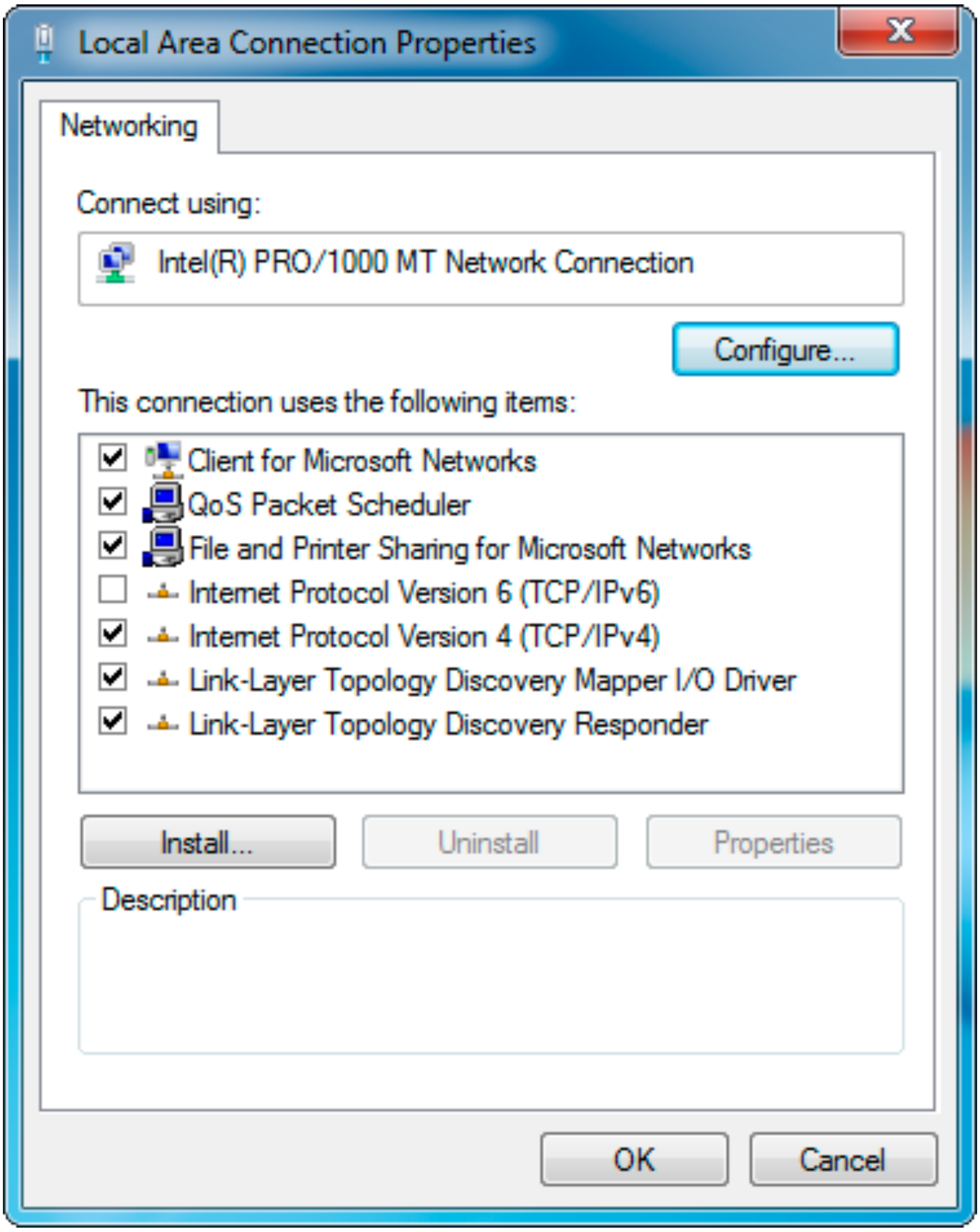
Connect using:

Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☐ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

- for Windows 7 or Windows Server 2008, click on **Start** and go to **Control Panel** → **Network and Internet** → **Network and Sharing Center** → **Change adapter settings**. Right-click on the network connection icon. In the drop-down menu, select **Properties**. Make sure that the following components are enabled:



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
□ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

- for Windows 8, Windows 10 or Windows Server 2012, click on **Windows** + **X**. In the context menu, go to **Control Panel** → **Network and Internet** → **Network and Sharing Center** → **Change adapter settings.** Right-click on the network connection icon. In the drop-down menu, select **Properties**.
- for Windows 10, in the **Network and Internet** category, go to any of the following tabs: **VPN**, **Ethernet** or **Dial**, and select **Network and Sharing Center** → **Change adapter settings**.

2. Make sure that the following services are installed and configured for the connection:
   - Client for Microsoft networks;
   - File and Server sharing for Microsoft networks;
   - Internet Protocol Version 4 (TCP/IPv4) or Internet Protocol Version 6 (TCP/IPv6).
3. Confirm the changes and close the configuration window.

- The sharing parameters should support the advanced configuration described below.
- The standard model of sharing and security should be used for local accounts. Its configuration process is described below.

- If your organisation uses the Active Directory domain controller, you need to configure file-sharing and printer-sharing parameters and security settings. You can create a new Group Policy Object (GPO) to apply these settings or change the settings of an existing object.

Creating a new Group Policy Object

1. In the command prompt, enter **gpmc.msc** in the text field and run the Group Policy Management Console **(GPMC)**.
2. Create a new GPO, for example, **GPO-CureNet**. To do this, in the **GPMC** console tree, right-click on **GPOs** in the appropriate forest and domain. Click on **Create**. In the newly appeared dialogue, specify a new object name and click on **OK**.
3. Bind the created object to the required domain.
4. Right-click on the newly created object, select **Change** and adjust the necessary settings as described below.

If you choose not to create a new object, but to change the parameters of an existing object, open the window with the corresponding settings.

1. On the computer where you installed GPMC, click on **Start** → **Administration** → **Group Policy Management**.
2. If you see the UAC dialogue, check the data, and then click on **Proceed**.
3. In the navigation pane, find and expand the node **Forest: Forest name**. Then expand **GPOs** and right-click on the name of the object for which you want to set the permission.
4. In the newly appeared menu, select **Change**.

Configuring file and printer sharing

Allow incoming requests from client computers to access files. Enabling this firewall exception opens UDP ports 137 and 138, and TCP port 445 for the IP addresses specified in this rule.

Enabling file and printer sharing

1. In the navigation area of the newly appeared window, expand the following nodes: **Computer Configuration → Policies → Administrative Templates → Network → Network connections → Windows Firewall → Domain profile.**
2. In the details pane, double-click on the **Windows Firewall** settings: **Allow inbound file and printer sharing exception** and enable this rule in the settings tab.
3. In the **Allow unsolicited incoming messages from these IP addresses**, select the range.
4. To save the changes, click on **OK**.

Changing security settings

Configure the policy **Network access: Sharing and security model for local accounts** in such a way that when signing in to the network using local account credentials, the authentication will be carried out using those credentials.

Allowing network access for user accounts

1. In the navigation area of the newly appeared window, expand the following options: **Computer Configuration → Policies → Windows Configuration → Security Options → Security settings**.
2. For the policy **Network access: Model Sharing and security for local accounts**, select the **Classic — local users authenticate as themselves** mode.

Applying changes in the domain

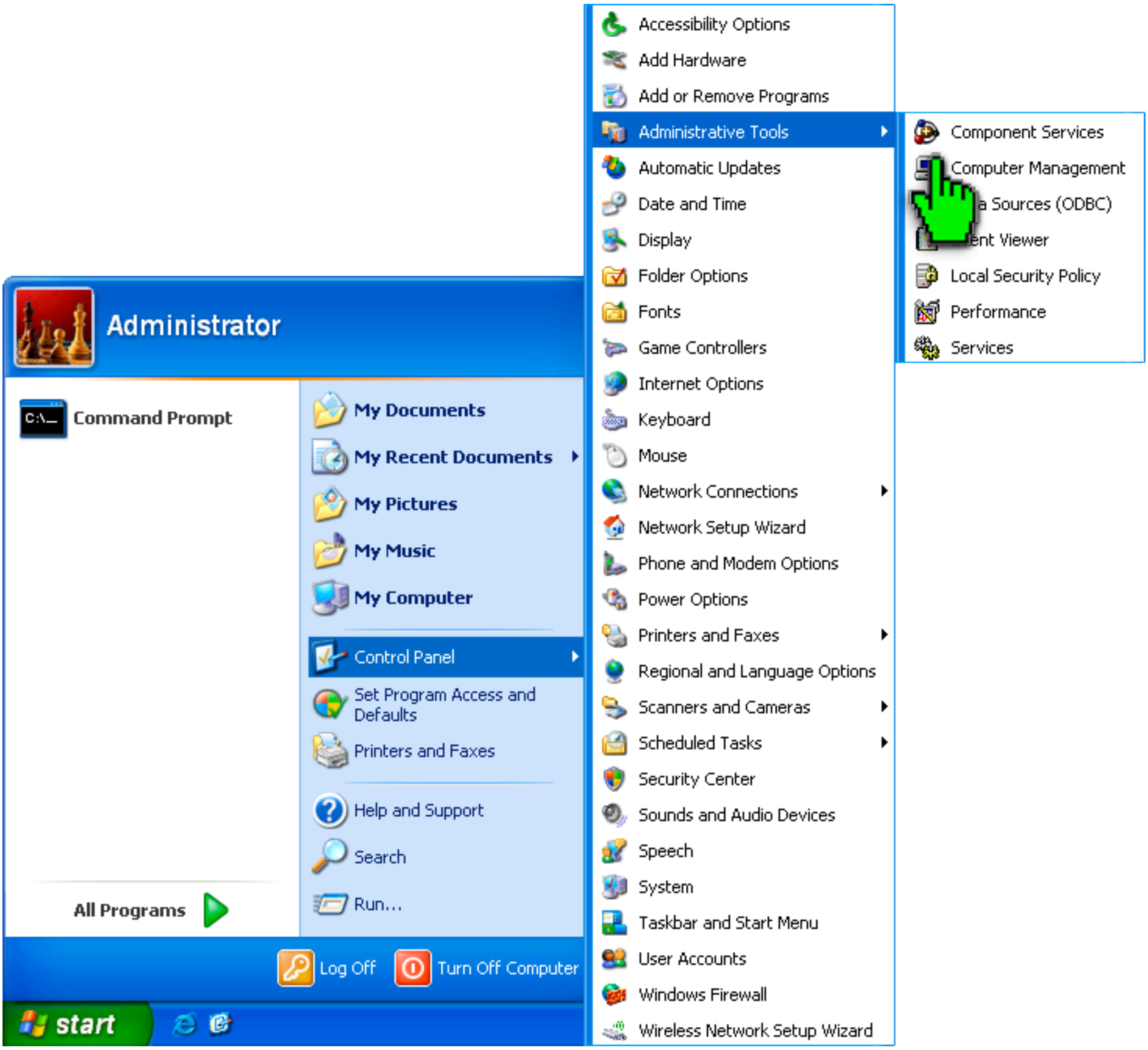
In order to apply the changes of the domain group policies, in both cases (both when creating a new object and when changing the policies of a pre-existing object), specify the **gpupdate /force** command in the command prompt window.

Creating an account that will be used for the connection

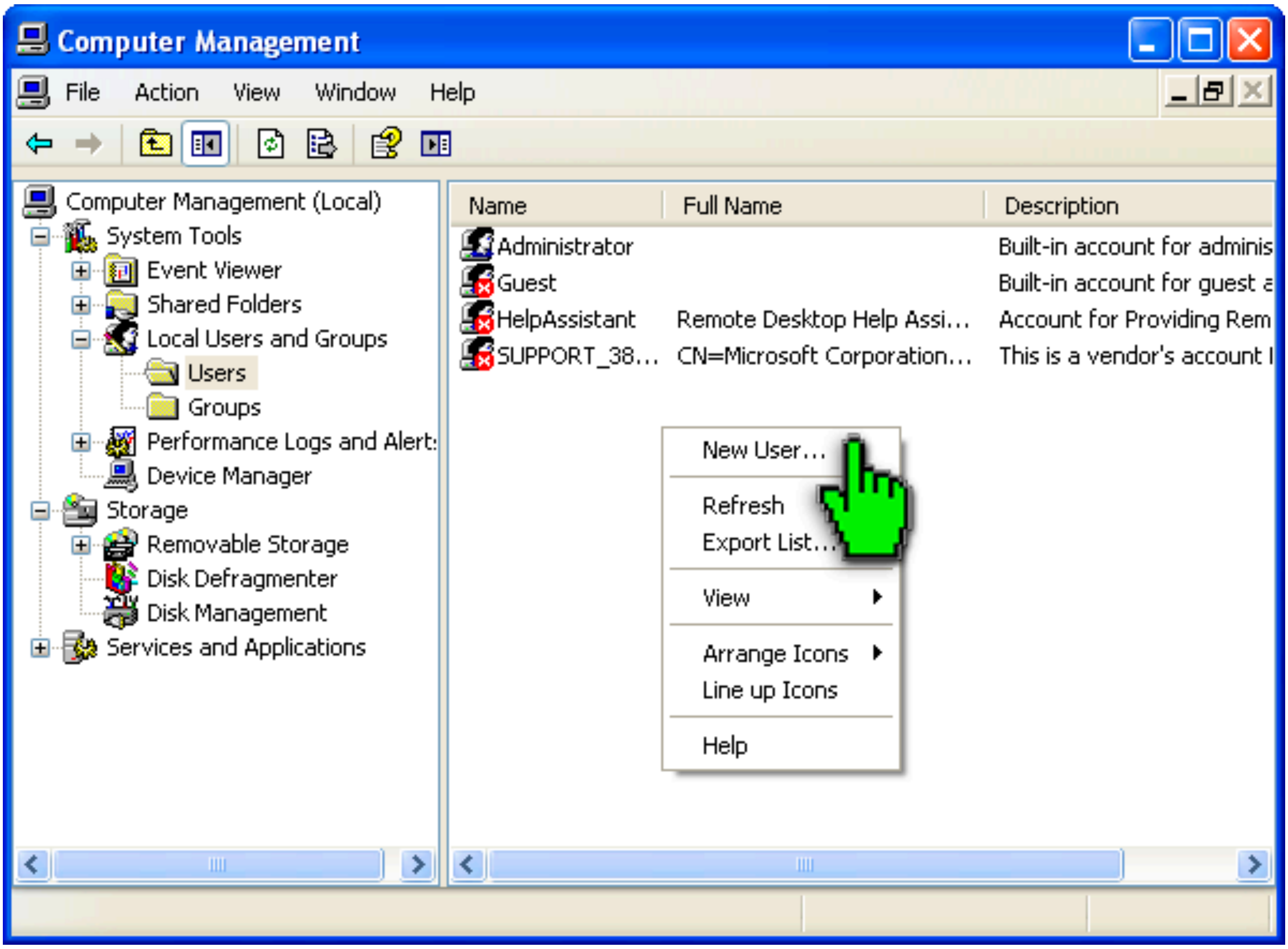
The account used for the connection must exist and have the necessary privileges.

- **Windows XP, Windows 2003**

  Click on **Start** and go to **Control Panel** → **Administrative Tools** → **Computer Management** → **Local Users and Groups** → **Users**.

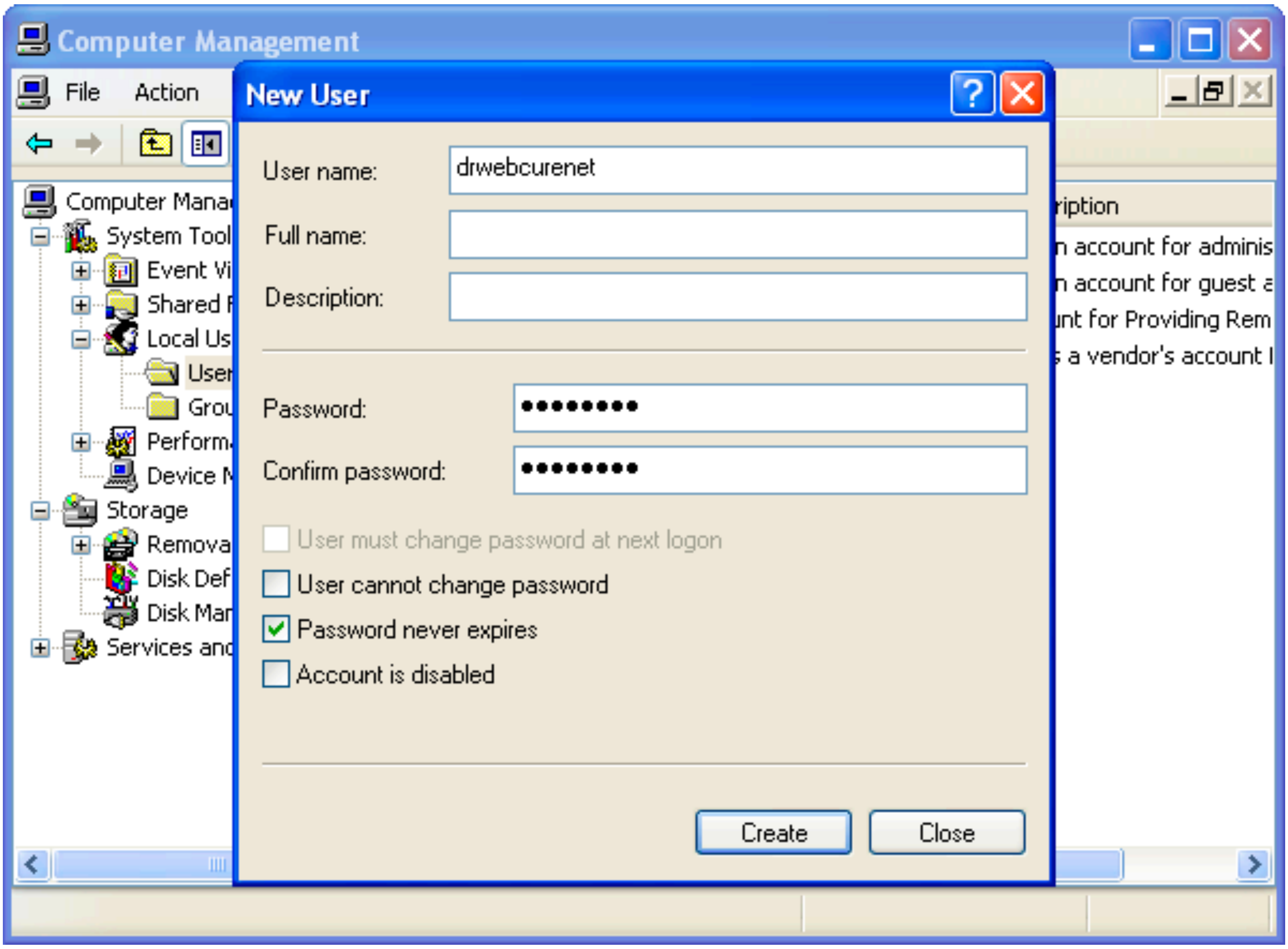


Further adjustments can be made using the standard **Administrator** account, but it is recommended that you create an alternative administrator account. To do this, right-click in the right pane and in the context menu, select **New User**.



Name	Full Name	Description
Administrator		Built-in account for adminis
Guest		Built-in account for guest a
HelpAssistant	Remote Desktop Help Assi...	Account for Providing Rem
SUPPORT_38...	CN=Microsoft Corporation...	This is a vendor's account I

Enter the user name **DrWebCurenet**. In the **Password** and **Confirm password** fields, enter a strong password. Disable the **User must change password at next logon** option. Enable the option **Password never expires**. Click on **Create** and then click on **Close**.



User name: drwebcurenet

Full name:

Description:

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

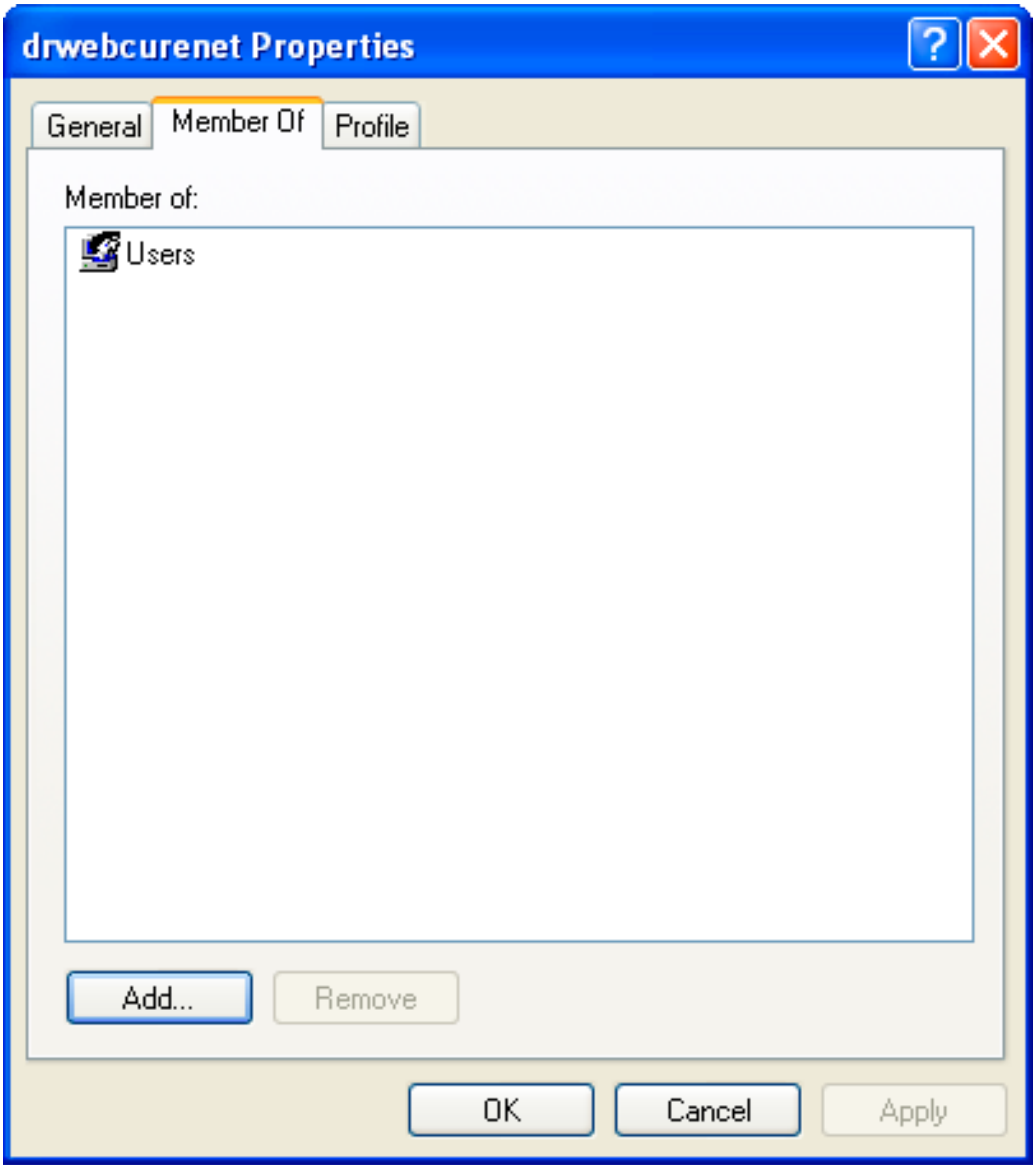
□ User must change password at next logon

□ User cannot change password

☑ Password never expires

□ Account is disabled

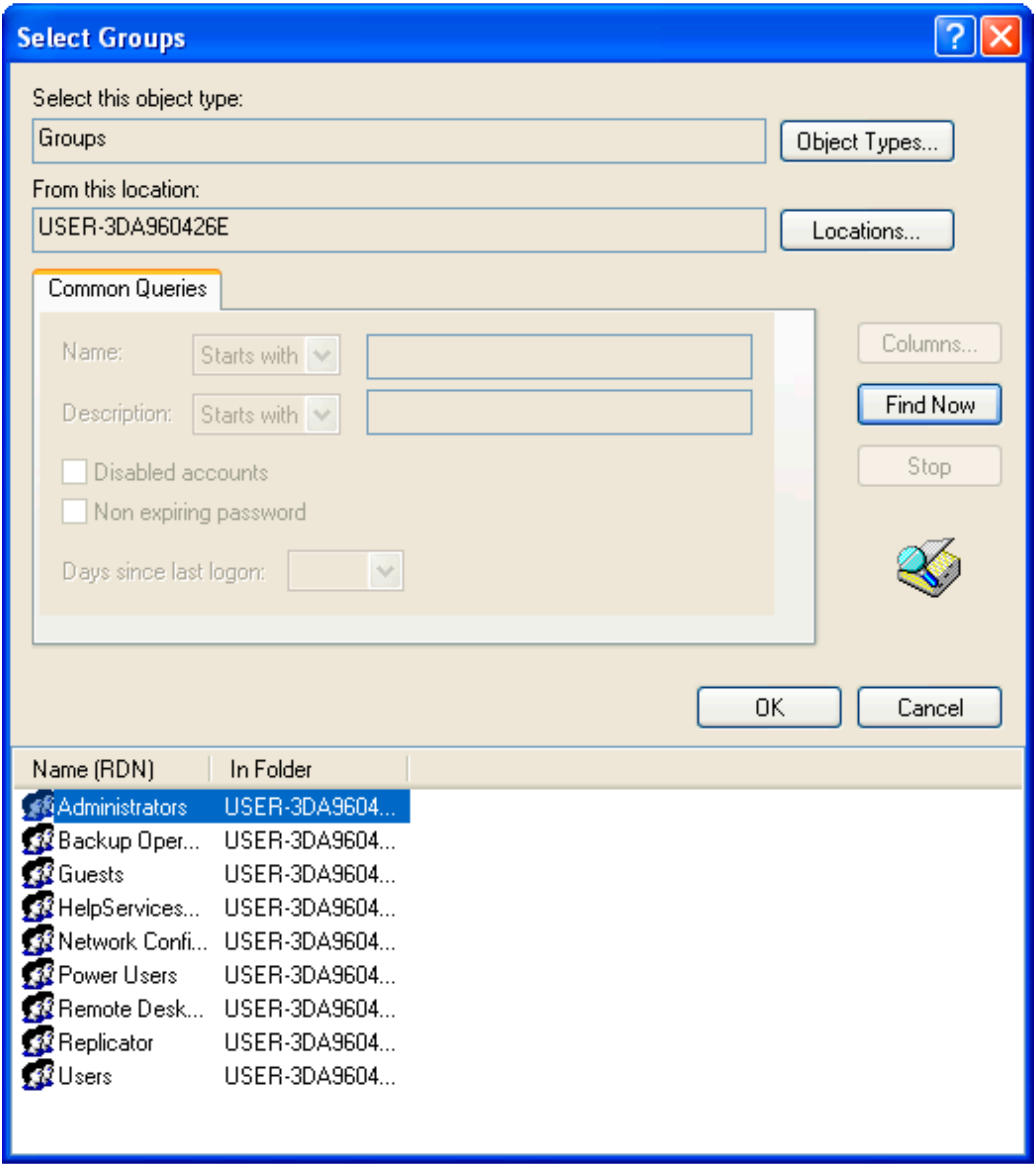
Double-click on the created **DrWebCurenet** account icon. The **DrWebCurenet properties** window will appear. Go to the **Member Of** tab.



Member of:

Users

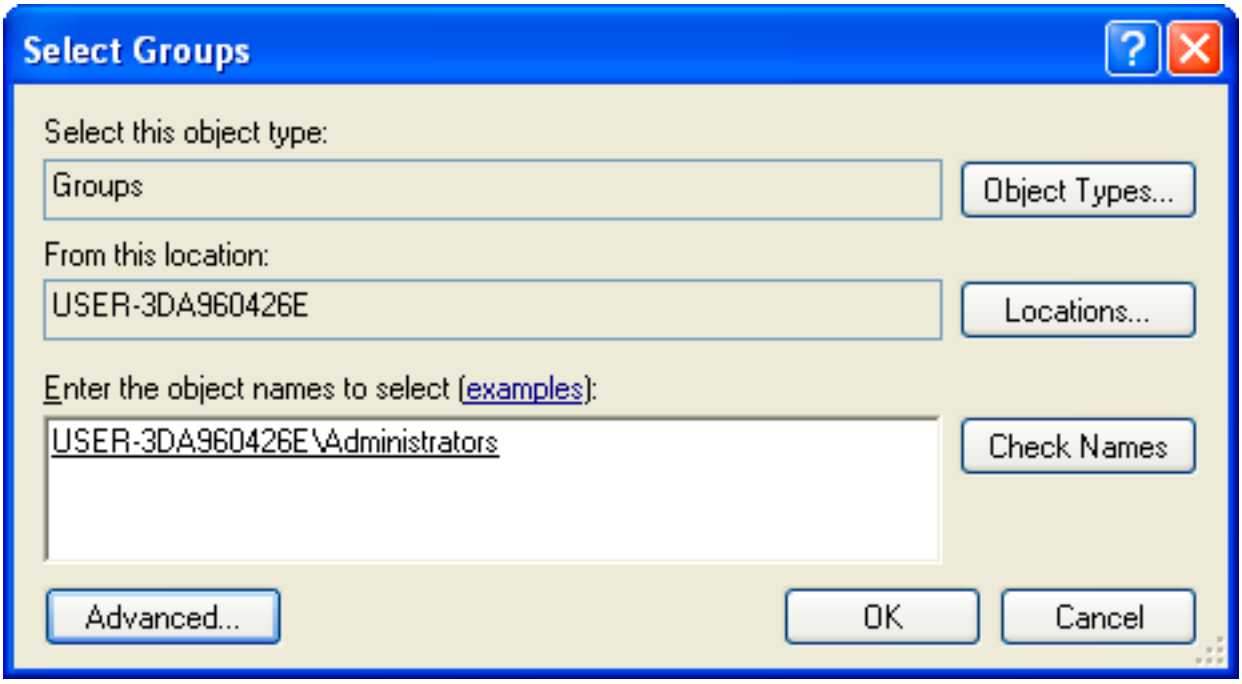
In the **Member Of** tab, select **Users** and click on **Remove**. Then click on **Add**. The **Select Groups** window will open. Click on **Advanced** and then click on **Find Now**. On the resulting list, select **Administrators**, click on **OK**, and then click on **OK** one more time in the **Select Groups** window.



Select this object type:
Groups

From this location:
USER-3DA960426E

Name (RDN)	In Folder
Administrators	USER-3DA9604...
Backup Oper...	USER-3DA9604...
Guests	USER-3DA9604...
HelpServices...	USER-3DA9604...
Network Confi...	USER-3DA9604...
Power Users	USER-3DA9604...
Remote Desk...	USER-3DA9604...
Replicator	USER-3DA9604...
Users	USER-3DA9604...



Select Groups

Select this object type:
Groups

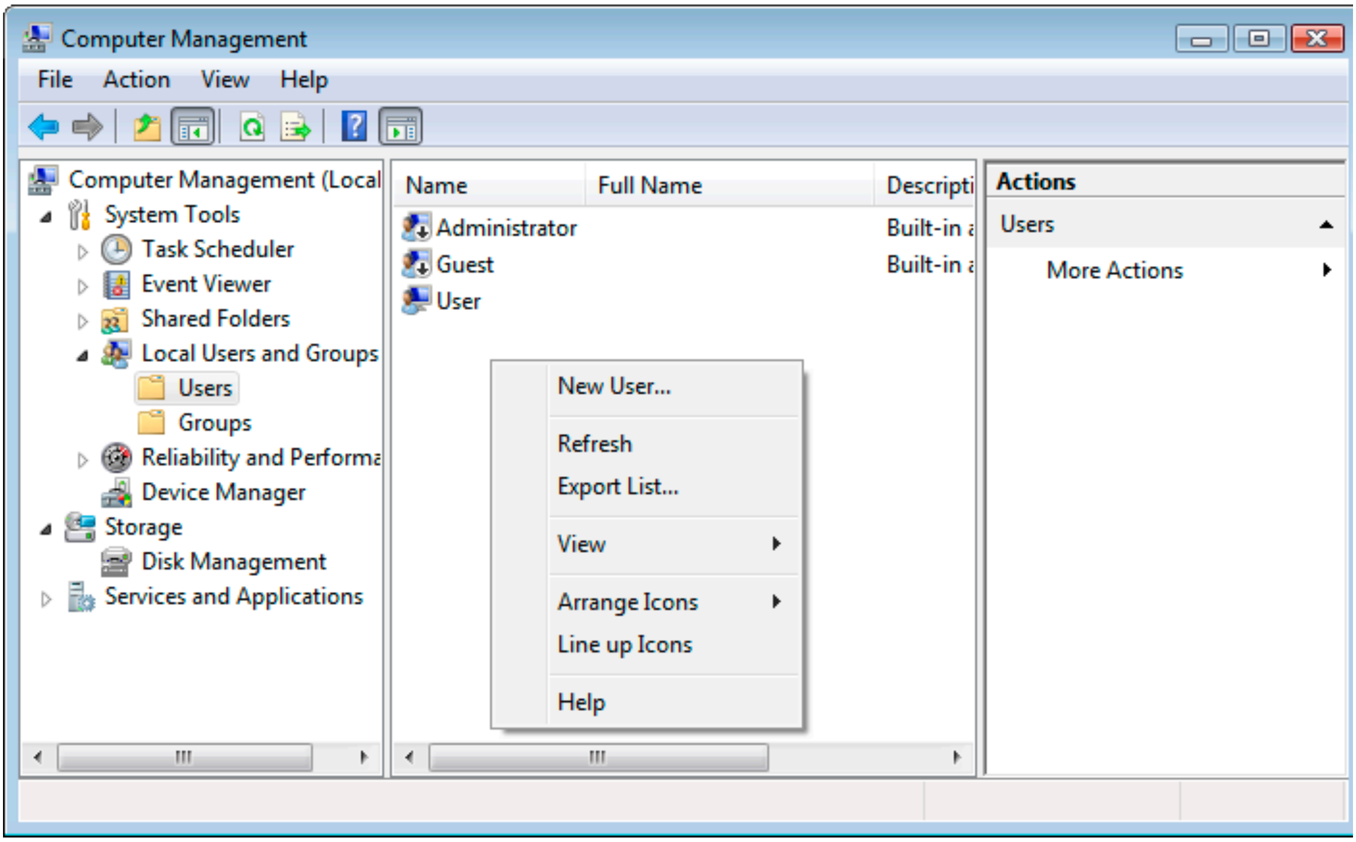
From this location:
USER-3DA960426E

Enter the object names to select (examples):
USER-3DA960426E\Administrators

In the **Dr.WebCureNet properties** window, click on **Apply** and **OK**.

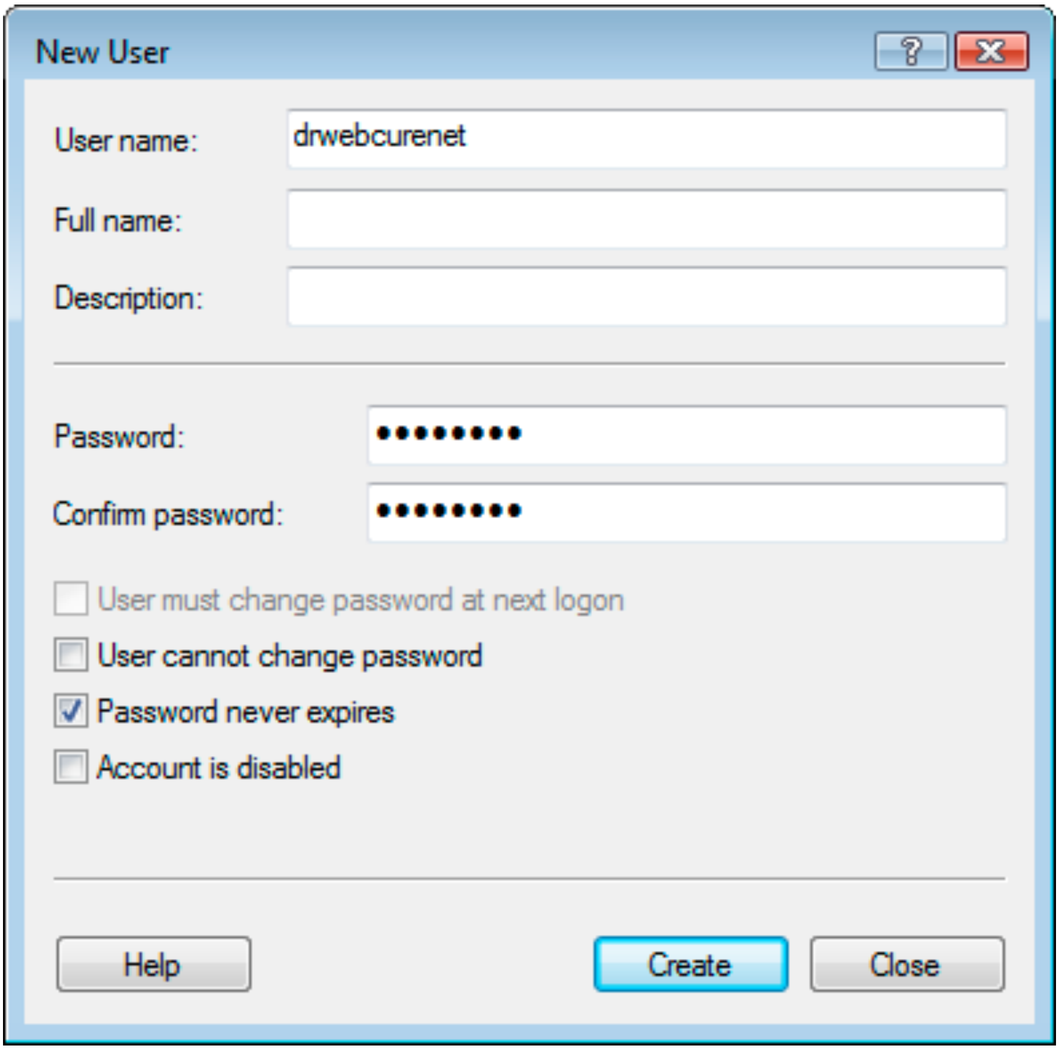
- **Windows Vista and Windows Server 2008**

  Click on **Start** and go to **Control Panel** → **System and Maintenance** → **Administrative Tools** → **Computer Management** → **Local Users and Groups** → **Users**. Further adjustments can be made using the standard Administrator account, but it is recommended that you create an alternative administrator account. Right-click in the middle pane and select New User in the context menu.



Name	Full Name	Descripti
Administrator		Built-in a
Guest		Built-in a
User		

Enter the user name — **DrWebCurenet**. Enter a strong password in the **Password** and **Confirm password** fields. Clear the **User must change password at next logon** check box. Check the **Password never expires** box.



User name: drwebcurenet

Full name:

Description:

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

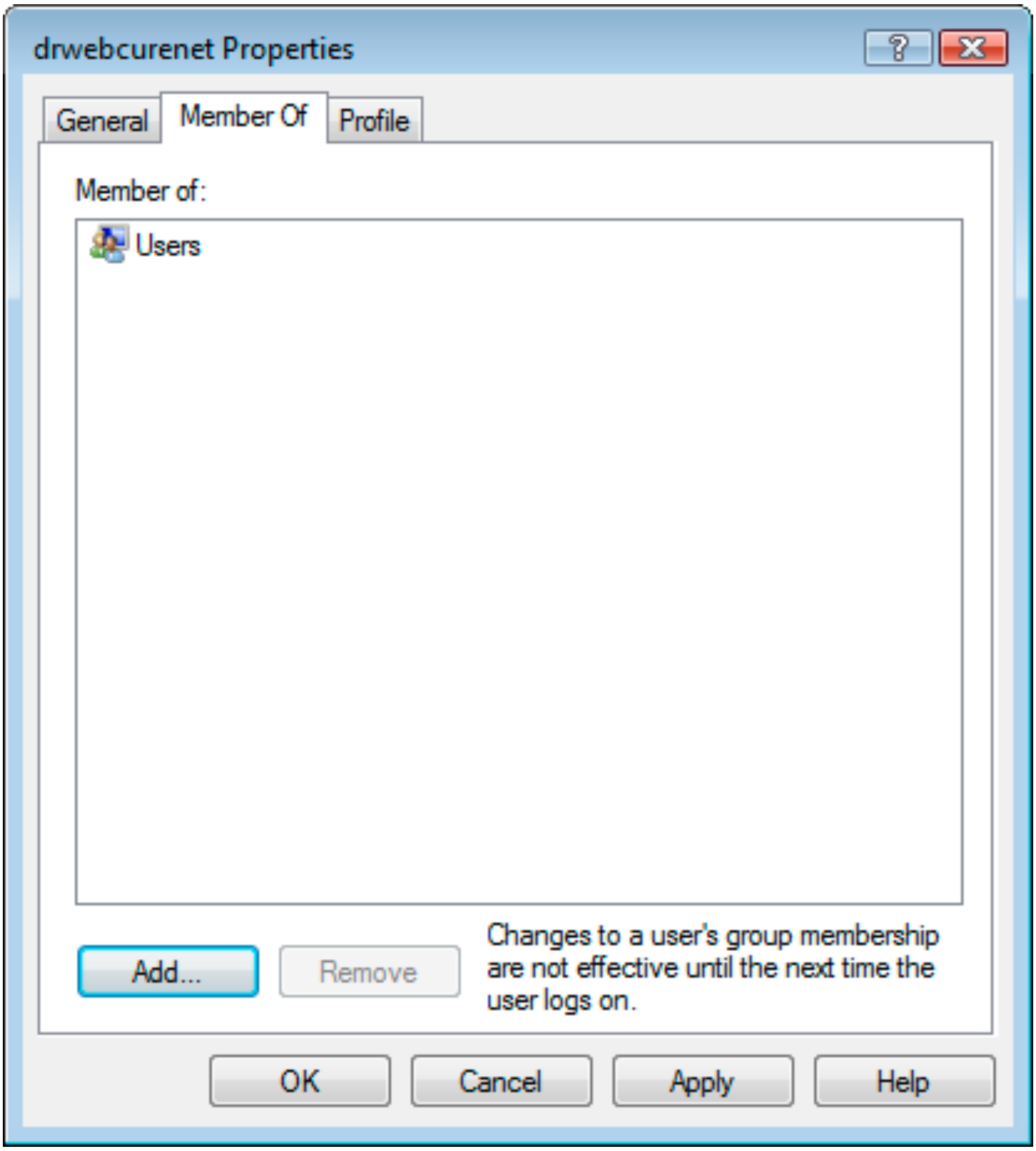
□ User must change password at next logon

□ User cannot change password

☑ Password never expires

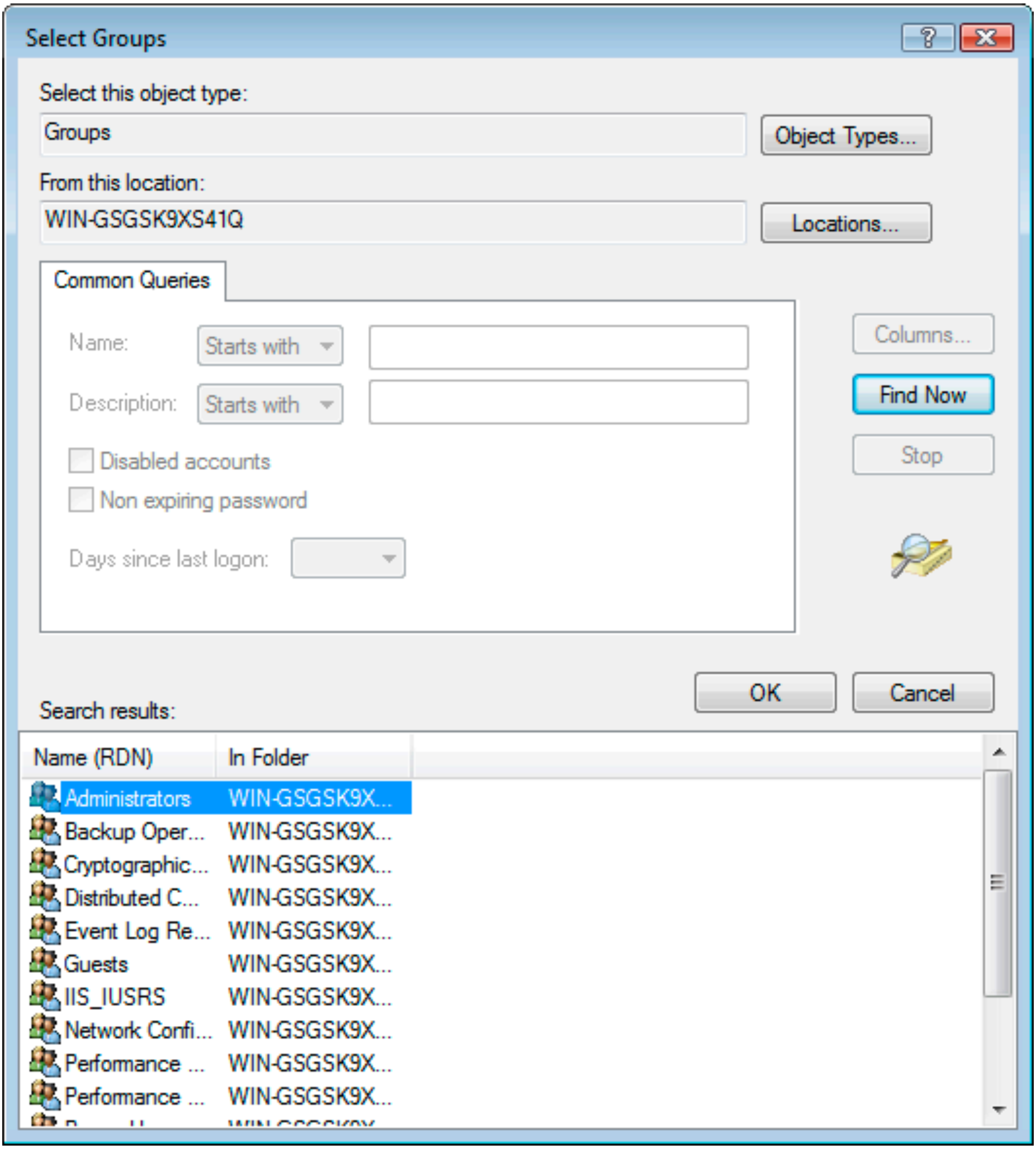
□ Account is disabled

Click in sequence on the **Create** and **Close** buttons. Double-click on the created **DrWebCurenet** account and go to the **Member Of** tab.



Changes to a user's group membership are not effective until the next time the user logs on.

Select **Users** and click on **Remove**. Then click on **Add**. The **Select Groups** window will open. Click on **Advanced** and then click on **Find Now**. In the search results, select **Administrators** and click on **OK**.



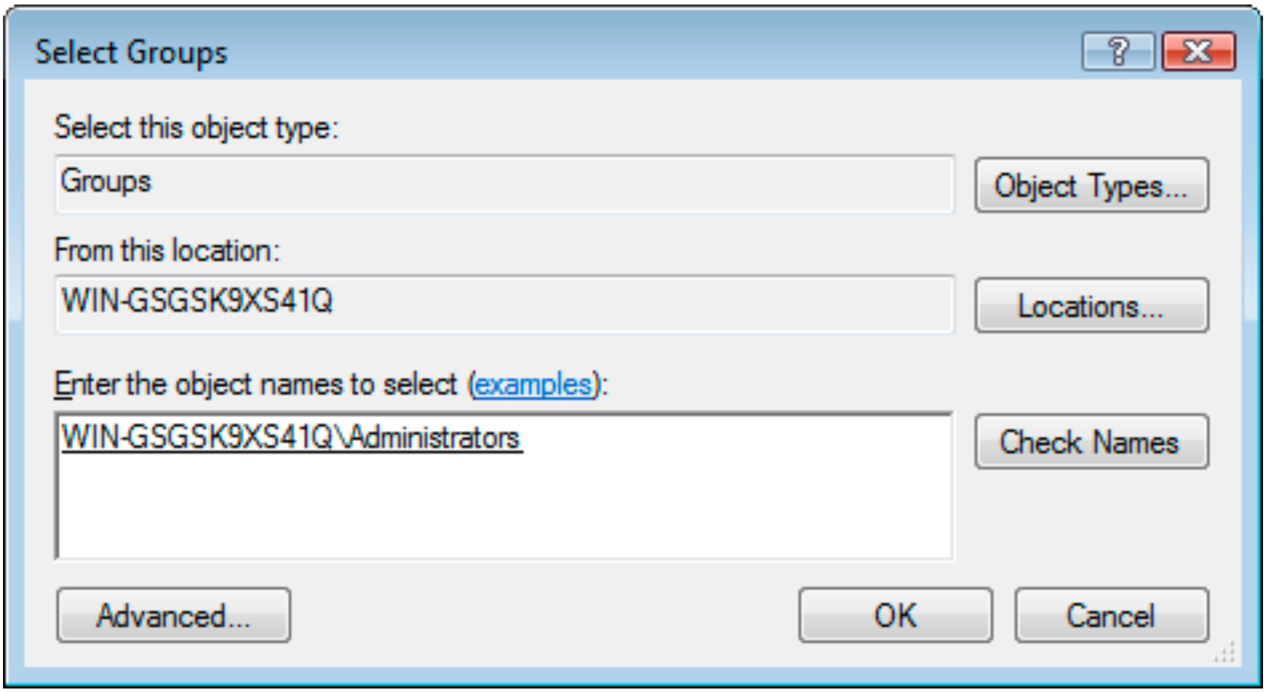
Select this object type:
Groups

From this location:
WIN-GSGSK9XS41Q

Search results:

Name (RDN)	In Folder
Administrators	WIN-GSGSK9X...
Backup Oper...	WIN-GSGSK9X...
Cryptographic...	WIN-GSGSK9X...
Distributed C...	WIN-GSGSK9X...
Event Log Re...	WIN-GSGSK9X...
Guests	WIN-GSGSK9X...
IIS_IUSRS	WIN-GSGSK9X...
Network Confi...	WIN-GSGSK9X...
Performance ...	WIN-GSGSK9X...
Performance ...	WIN-GSGSK9X...

In the **Select Groups** window, also click on **OK**.



Select Groups

Select this object type:

Groups

From this location:

WIN-GSGSK9XS41Q

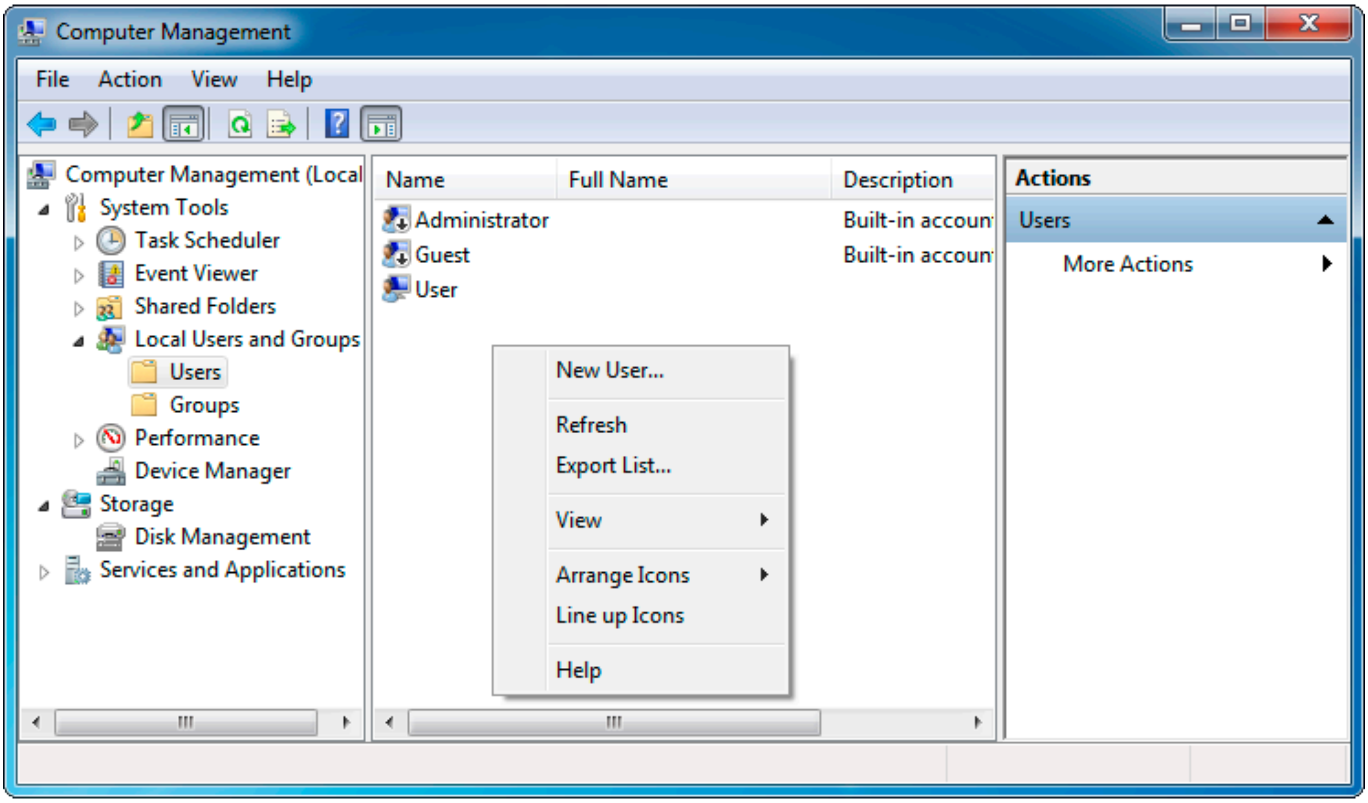
Enter the object names to select (examples):

WIN-GSGSK9XS41Q\Administrators

Click in sequence on **Apply** and **OK** in the **Properties:DrWebCurenet** window.

- **Windows 7, Windows 2008 R2**

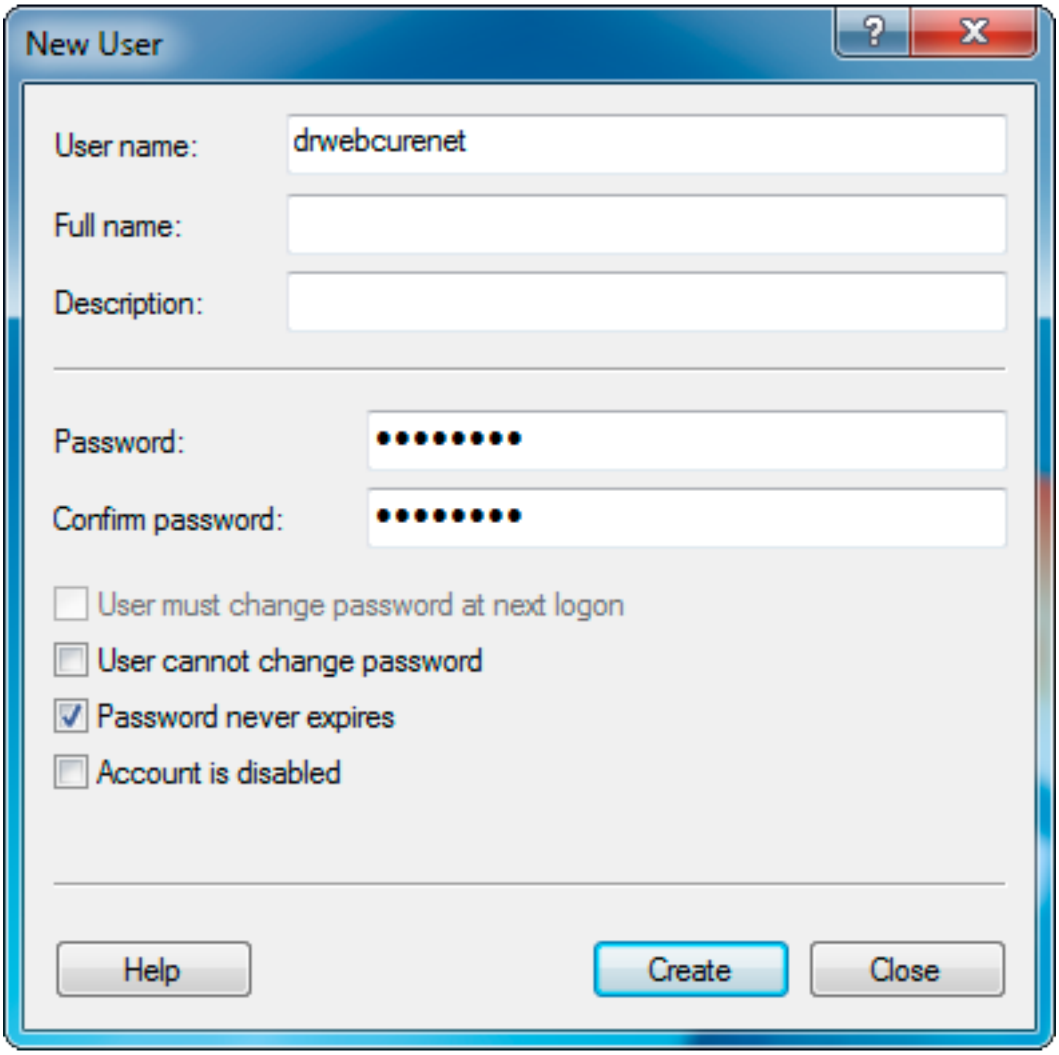
Click on **Start** and go to **Control Panel** → **System and Security** → **Administrative Tools** → **Computer Management** → **Local Users and Groups** → **Users**. Further adjustments can be made using a standard **Administrator** account, but it is recommended that you create an alternative administrator account. Right-click in the middle pane and select **New User** in the context menu.



Computer Management

Name	Full Name	Description
Administrator		Built-in accoun
Guest		Built-in accoun
User		

Enter the user name — **DrWebCurenet**. Enter a strong password in the **Password** and **Confirm password** fields. Clear the **User must change password at next logon** check box. Check the **Password never expires** box. Click in sequence on the **Create** and **Close** buttons.



User name: drwebcurenet

Full name:

Description:

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

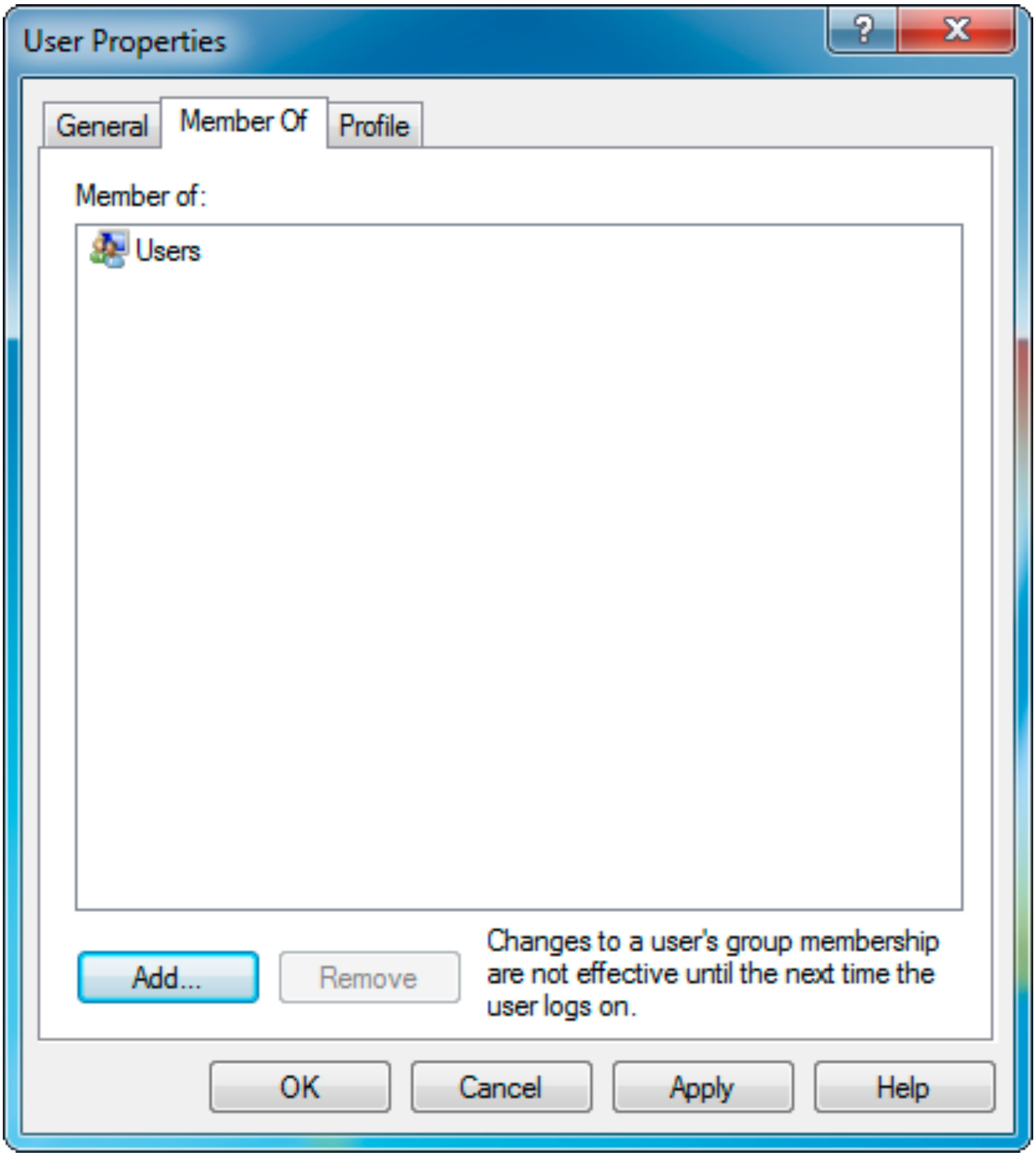
□ User must change password at next logon

□ User cannot change password

☑ Password never expires

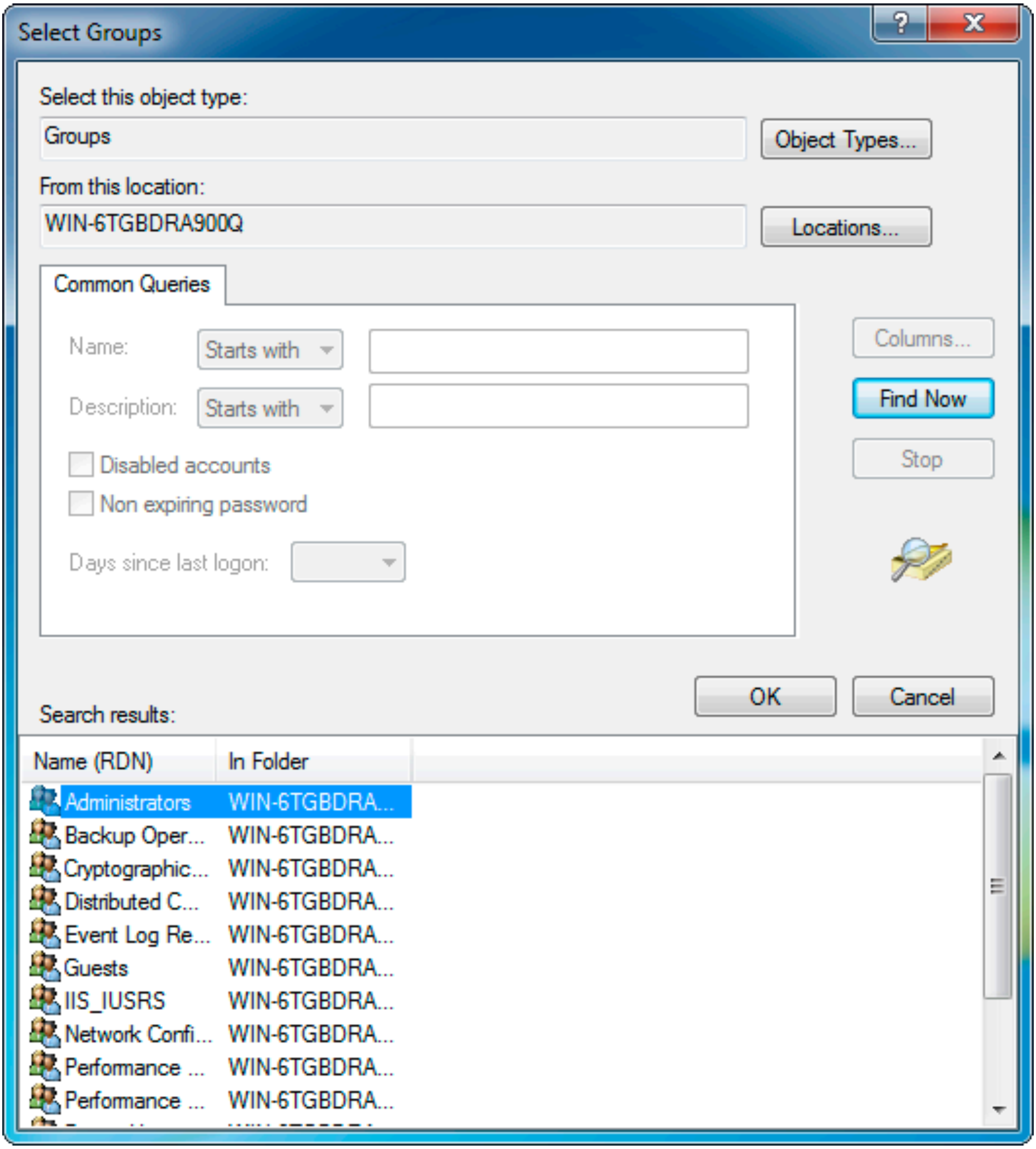
□ Account is disabled

Double-click on the created **DrWebCurenet** account and go to the **Member Of** tab. Select **Users** and click on **Remove**.



Changes to a user's group membership are not effective until the next time the user logs on.

Then click on **Add**. The **Select Groups** window will open. Click on **Advanced** and then click on **Find Now**. In the search results, select **Administrators** and click on **OK**.



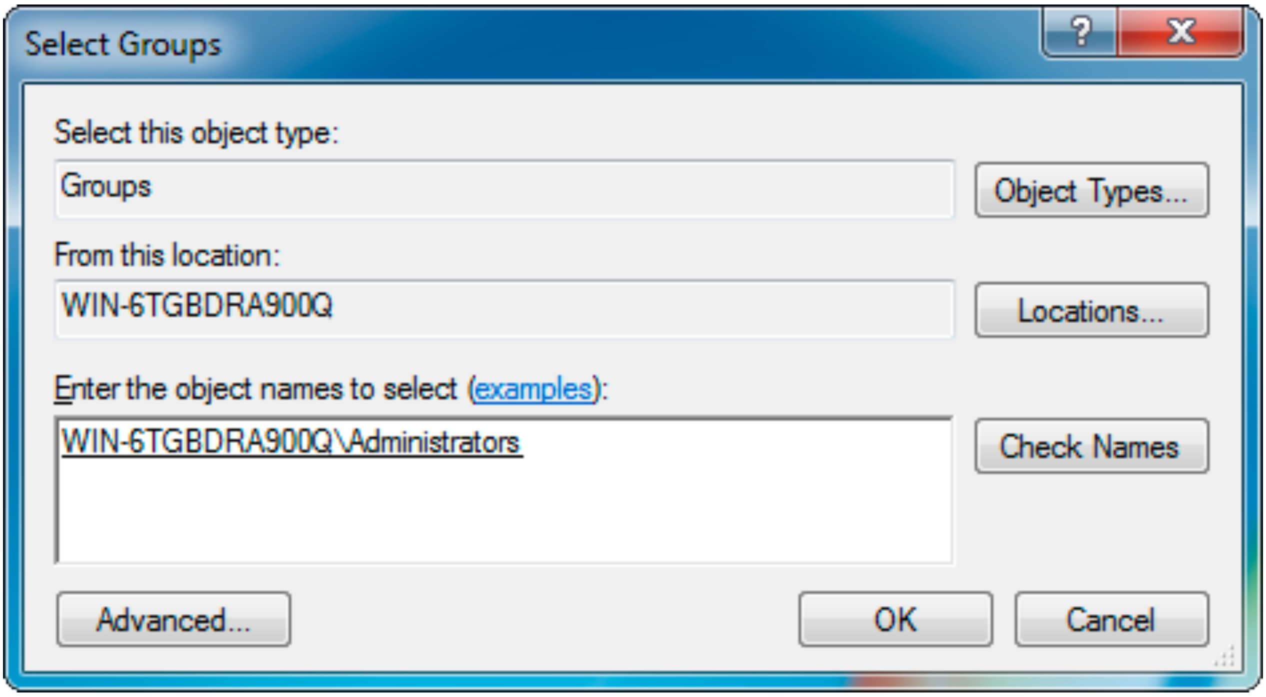
Select this object type:
Groups

From this location:
WIN-6TGBDRA900Q

Search results:

Name (RDN)	In Folder
Administrators	WIN-6TGBDRA...
Backup Oper...	WIN-6TGBDRA...
Cryptographic...	WIN-6TGBDRA...
Distributed C...	WIN-6TGBDRA...
Event Log Re...	WIN-6TGBDRA...
Guests	WIN-6TGBDRA...
IIS_IUSRS	WIN-6TGBDRA...
Network Confi...	WIN-6TGBDRA...
Performance ...	WIN-6TGBDRA...
Performance ...	WIN-6TGBDRA...

In the **Select Groups** window, also click on **OK**.



Select this object type:

Groups

From this location:

WIN-6TGBDRA900Q

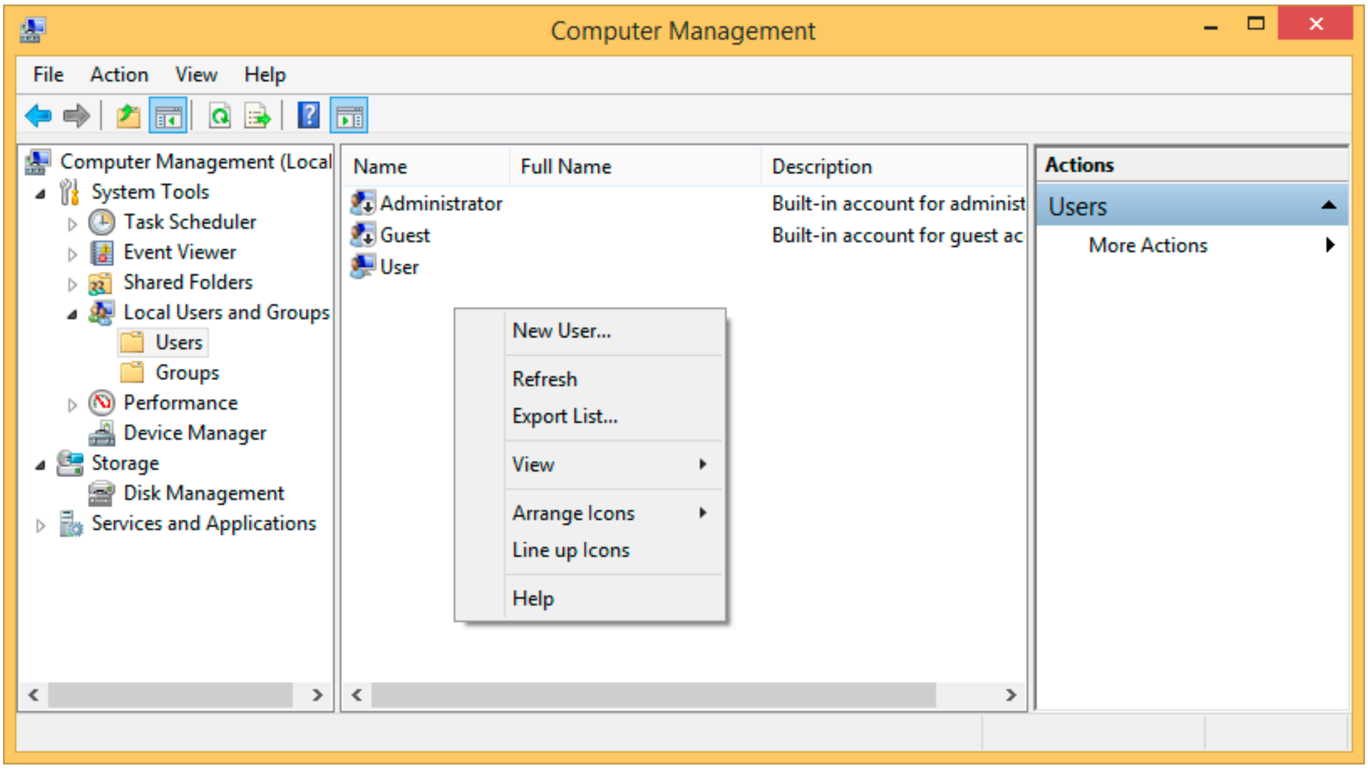
Enter the object names to select (examples):

WIN-6TGBDRA900Q\Administrators

In the **DrWebCurenet** properties window, click in sequence on **Apply** and **OK**.

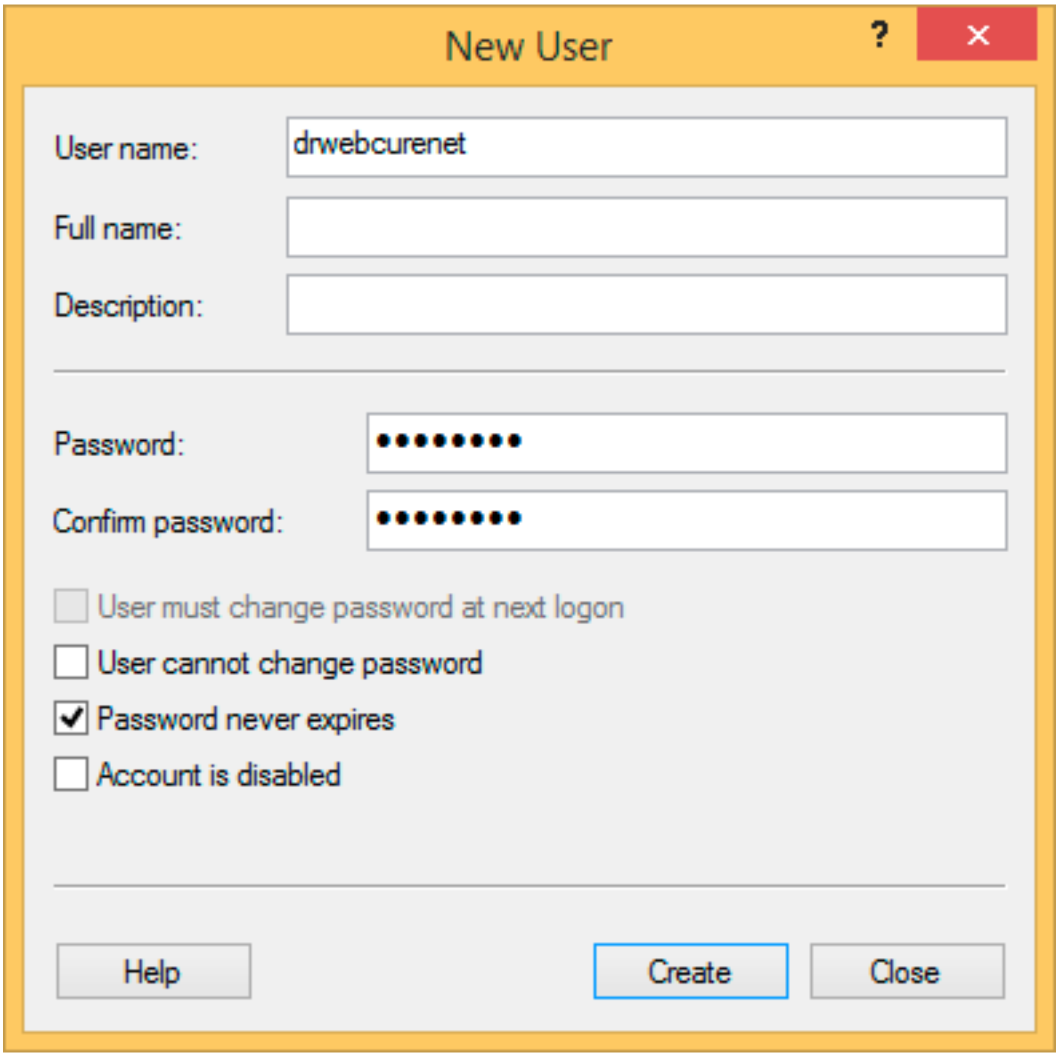
- **Windows 8, 10, Windows 8.1 Windows Server 2012**

Click on the **Windows + X** buttons. In the newly appeared context menu, select **Control Panel** → **System and Security** → **Administration** → **Computer Management** → **Local Users and Groups** → **User**. Further adjustments can be made using a standard **Administrator** account, but it is recommended that you create an alternative administrator account. Right-click in the middle pane and select **New User** in the context menu.



Name	Full Name	Description
Administrator		Built-in account for administ
Guest		Built-in account for guest ac
User		

Enter the user name — **DrWebCurenet**. Enter a strong password in the **Password** and **Confirm password** fields. Clear the **User must change password at next logon** check box. Check the **Password never expires** box.



User name: drwebcurenet

Full name:

Description:

Password: ●●●●●●●●●

Confirm password: ●●●●●●●●●

□ User must change password at next logon

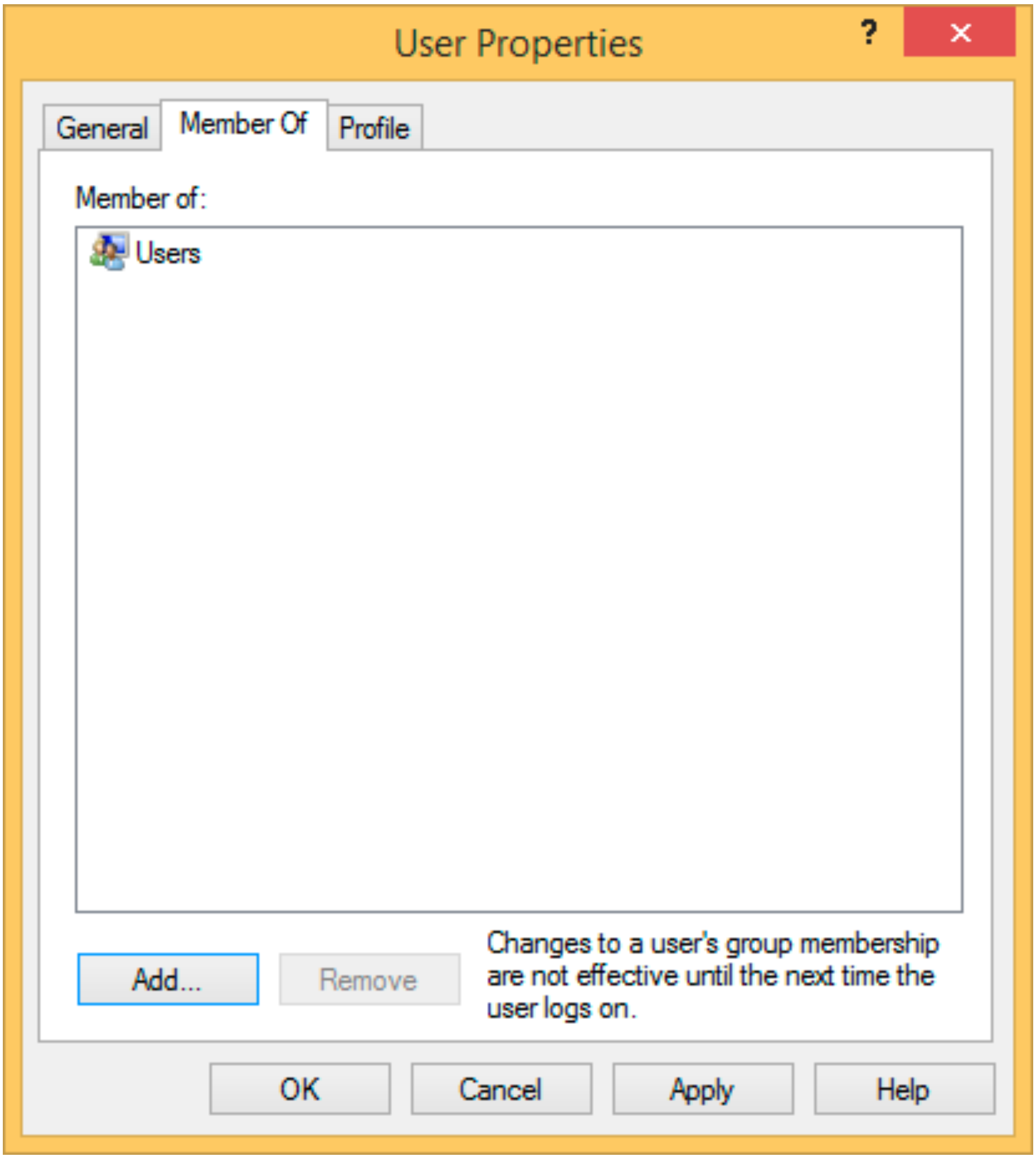
□ User cannot change password

☑ Password never expires

□ Account is disabled

Click on the **Create** and **Close** buttons.

Double-click on the created **DrWebCurenet** account and go to the **Member Of** tab.



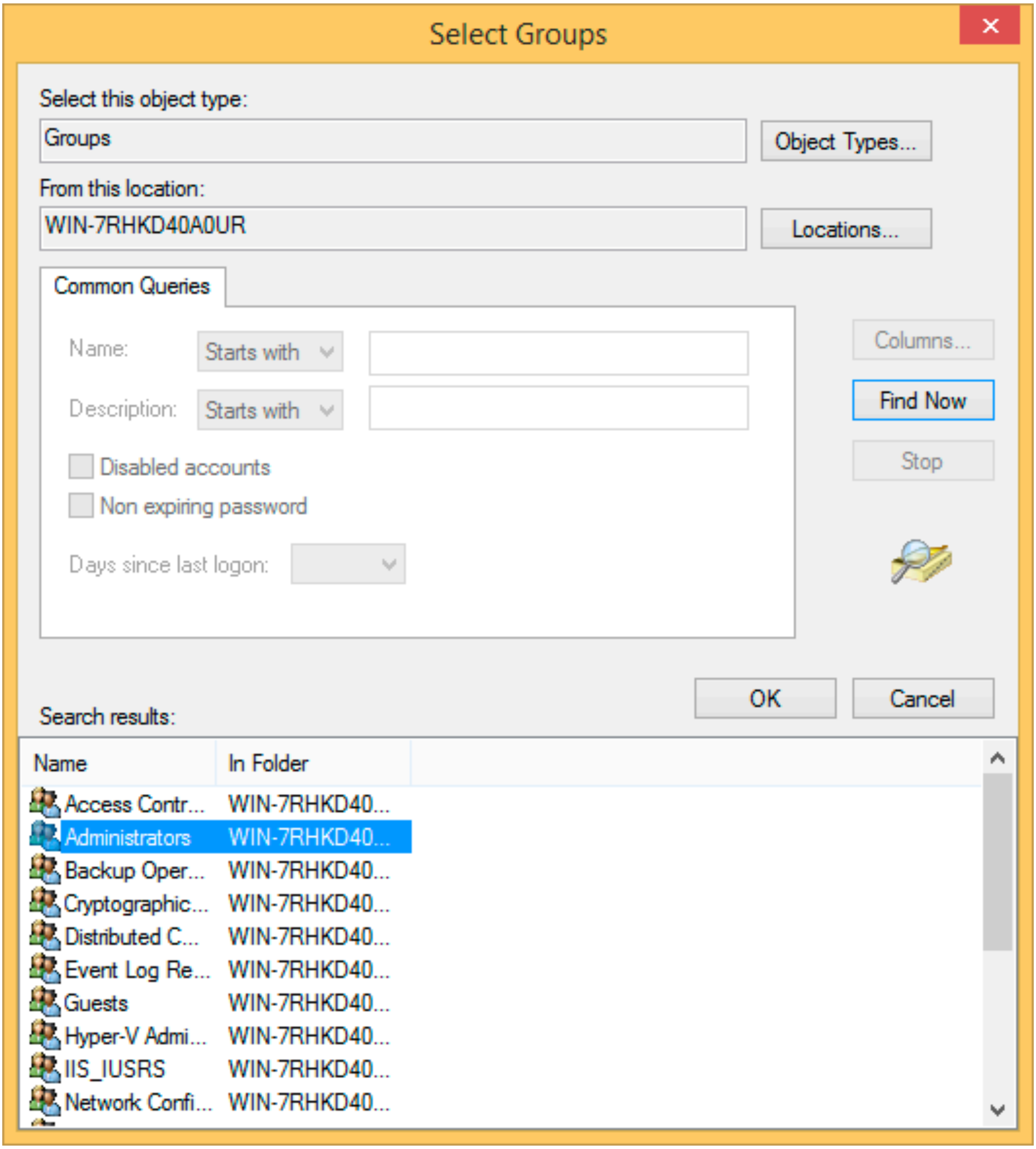
Member of:

Users

Changes to a user's group membership are not effective until the next time the user logs on.

Select **Users** and click on **Remove**.

Then click on **Add**. The **Select group** window will open. Click on **Advanced** and then click on **Find Now**. In the search results, select **Administrators** and click on **OK**.



Select Groups

Select this object type:

Groups

From this location:

WIN-7RHKD40A0UR

Common Queries

Name: Starts with

Description: Starts with

□ Disabled accounts

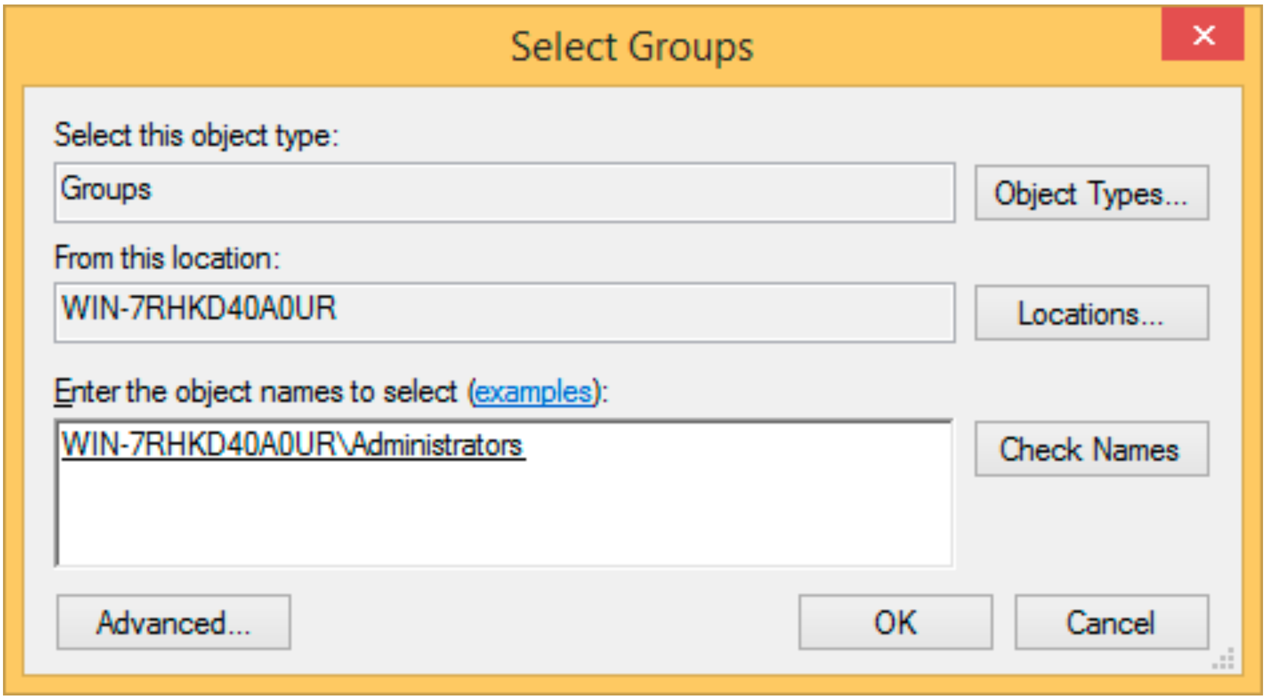
□ Non expiring password

Days since last logon:

Search results:

Name	In Folder
Access Contr...	WIN-7RHKD40...
Administrators	WIN-7RHKD40...
Backup Oper...	WIN-7RHKD40...
Cryptographic...	WIN-7RHKD40...
Distributed C...	WIN-7RHKD40...
Event Log Re...	WIN-7RHKD40...
Guests	WIN-7RHKD40...
Hyper-V Admi...	WIN-7RHKD40...
IIS_IUSRS	WIN-7RHKD40...
Network Confi...	WIN-7RHKD40...

In the **Select Groups** window, also click on **OK**.


Select Groups

Select this object type:

Groups

From this location:

WIN-7RHKD40A0UR

Enter the object names to select (examples):

WIN-7RHKD40A0UR\Administrators

In the **DrWebCurenet** properties window, click in sequence on **Apply** and **OK**.

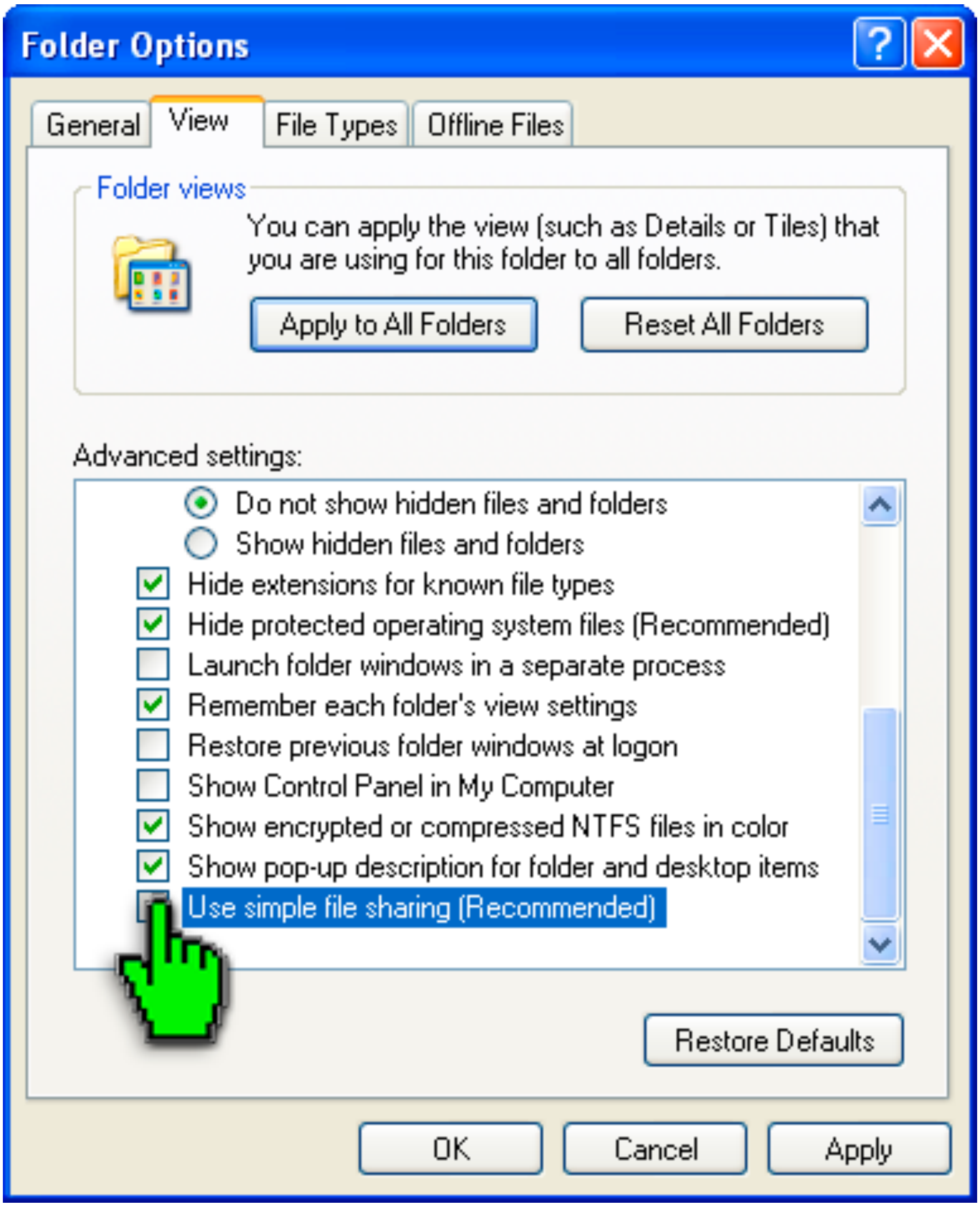
Configuring file sharing

- **Windows XP**

This configuration is not required for Windows 2003.

Click on **Start** and go to **Control Panel** → **Classic view** → **Folder Options**. The **Folder Options** window will open. Go to the **View** tab. Clear the **Use simple file sharing** check box. Click on **Apply** and **OK**.

You can also configure this setting in the Control Panel. Select **Windows Firewall** (if the item is not available, click on **Switch to standard view**). Go to the **Exceptions** tab and enable **File and Printer Sharing.**



Folder views

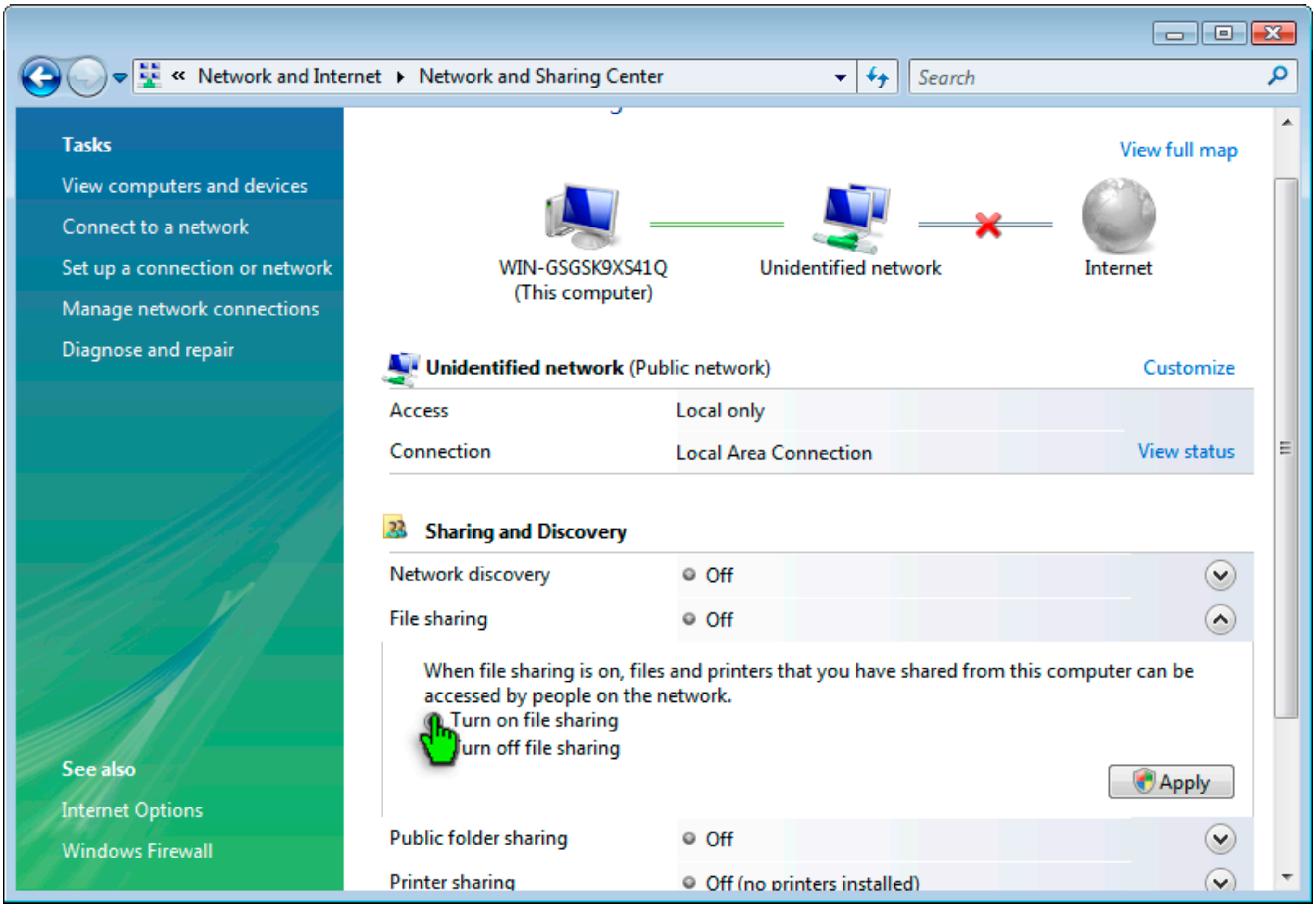
You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Advanced settings:

- ● Do not show hidden files and folders
- ○ Show hidden files and folders
- ☑ Hide extensions for known file types
- ☑ Hide protected operating system files (Recommended)
- □ Launch folder windows in a separate process
- ☑ Remember each folder's view settings
- □ Restore previous folder windows at logon
- □ Show Control Panel in My Computer
- ☑ Show encrypted or compressed NTFS files in color
- ☑ Show pop-up description for folder and desktop items
- □ Use simple file sharing (Recommended)

- **Windows Vista, Windows Server 2008**

Click on **Start** and go to **Control Panel** → **Network and Internet** → **Network and Sharing Center**. Check the **File Sharing** box in the **Sharing and Discovery** section. Click on **Apply**.



Unidentified network (Public network)

Access	Local only
Connection	Local Area Connection

Sharing and Discovery

Network discovery	○ Off
File sharing	○ Off

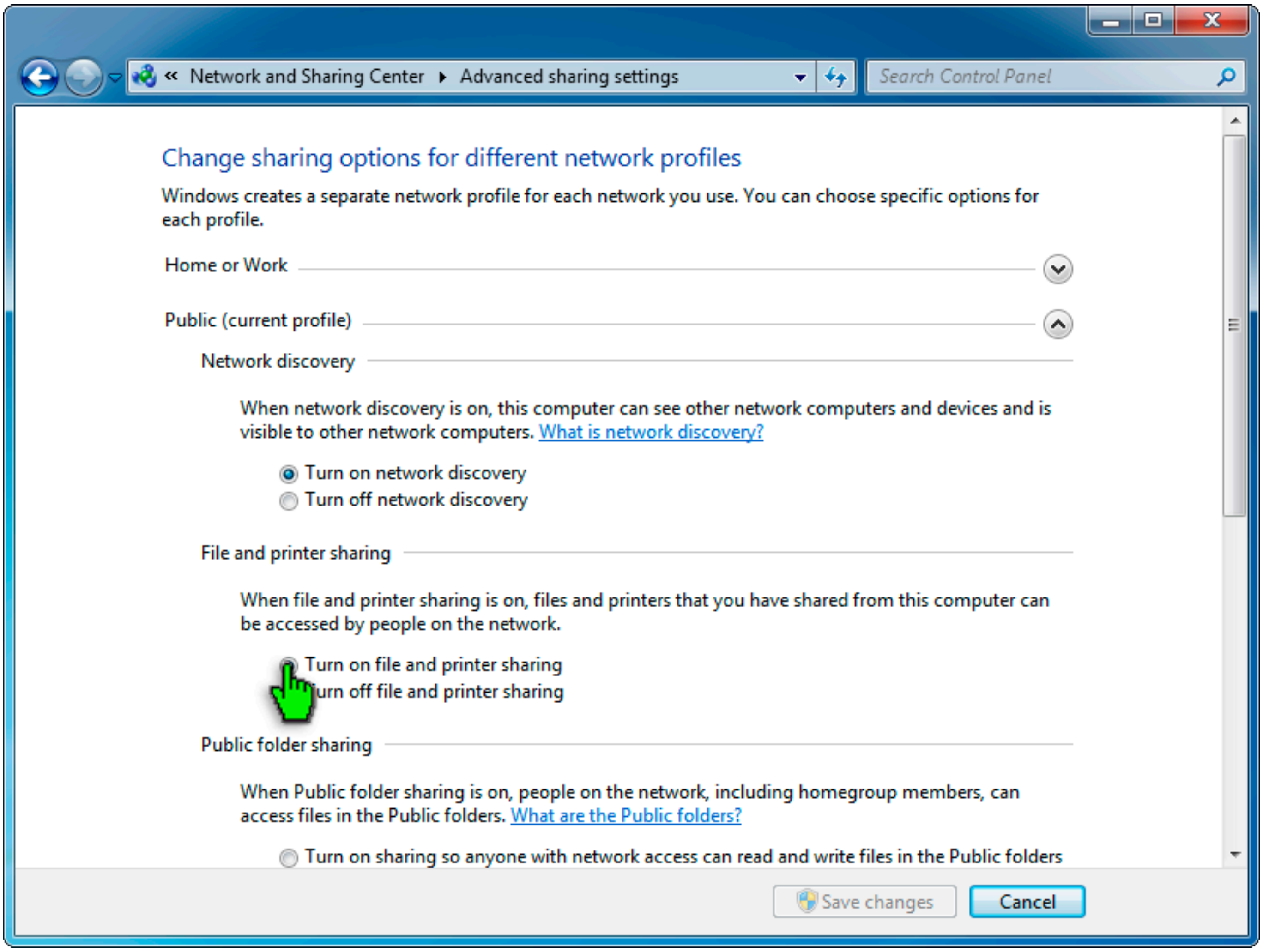
When file sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

○ Turn on file sharing
○ Turn off file sharing

Public folder sharing	○ Off
Printer sharing	○ Off (no printers installed)

- **Windows 7, Windows Server 2008 R2**

Click on Start and go to **Control Panel** → **Network and Internet** → **Network and Sharing Center** → **Change advanced sharing settings**. In the appropriate network profile, enable **Network discovery** and **Turn on file and printer sharing**.



Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Home or Work

Public (current profile)

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers. What is network discovery?

● Turn on network discovery
○ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

○ Turn on file and printer sharing
○ Turn off file and printer sharing

Public folder sharing

When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders. What are the Public folders?

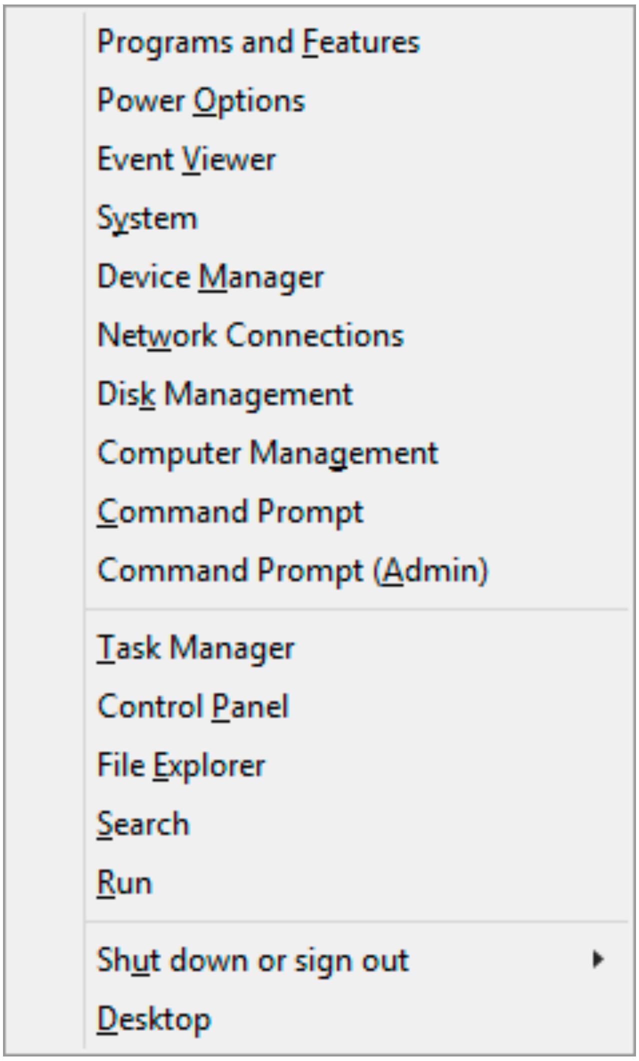
○ Turn on sharing so anyone with network access can read and write files in the Public folders

Click on **Save changes**.

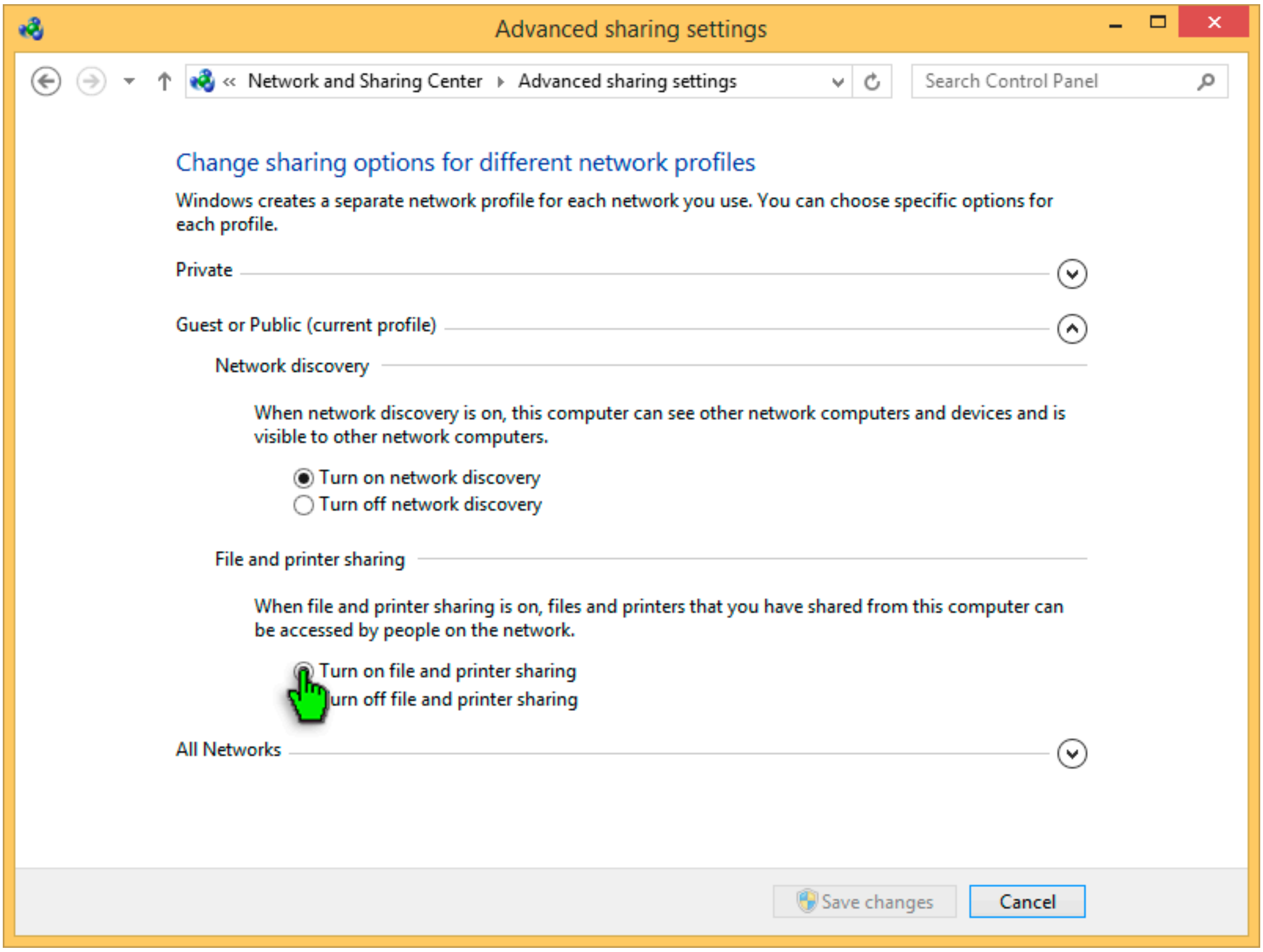
If you configure Windows 2008 or Windows 2008 R2, do not use the **Turn on network discovery** option.

- **Windows 8, 10, Windows 8.1, Windows Server 2012**

Click on the **Windows** + **X** buttons.



In the newly appeared context menu, select **Control Panel → Network and Internet → The Network and Sharing Center → Change advanced sharing settings**. In the network profile, select **Turn on file and printer sharing**.



Advanced sharing settings
Network and Sharing Center › Advanced sharing settings
Search Control Panel

Change sharing options for different network profiles

Windows creates a separate network profile for each network you use. You can choose specific options for each profile.

Private

Guest or Public (current profile)

Network discovery

When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.

● Turn on network discovery
○ Turn off network discovery

File and printer sharing

When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.

● Turn on file and printer sharing
○ Turn off file and printer sharing

All Networks

Click on **Save changes**.

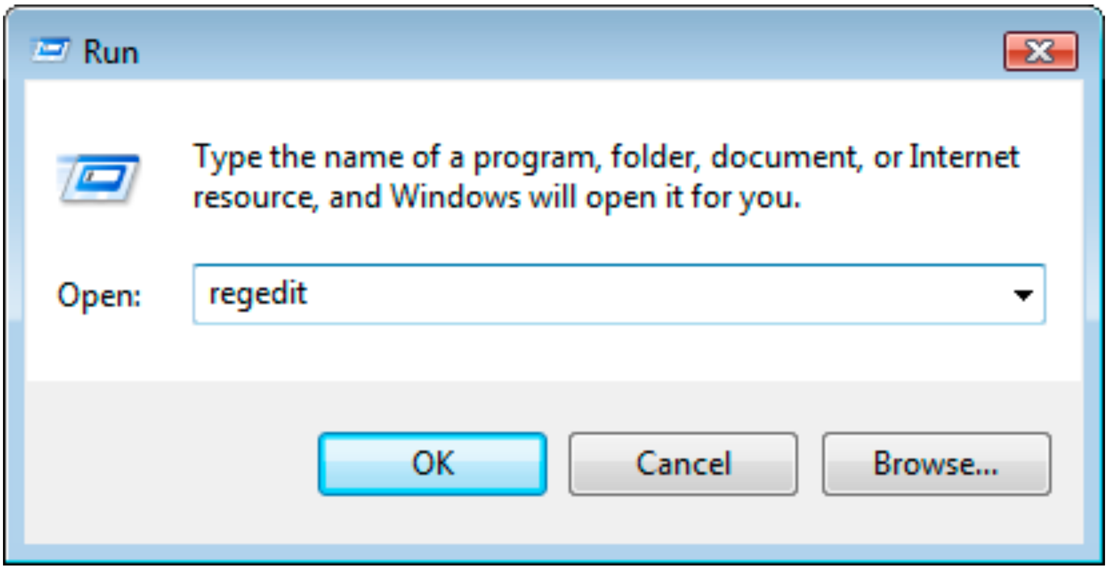
Configuring User Account Control (UAC)

Restrictions should be disabled if the station is running Windows Vista or later versions of the operating system. If you are using a built-in administrator account, skip this configuration step.

- **Windows Vista**

Open the Registry Editor on all the stations to be checked.

Click on the **Windows** + **R** buttons.


Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
OK
Cancel
Browse...

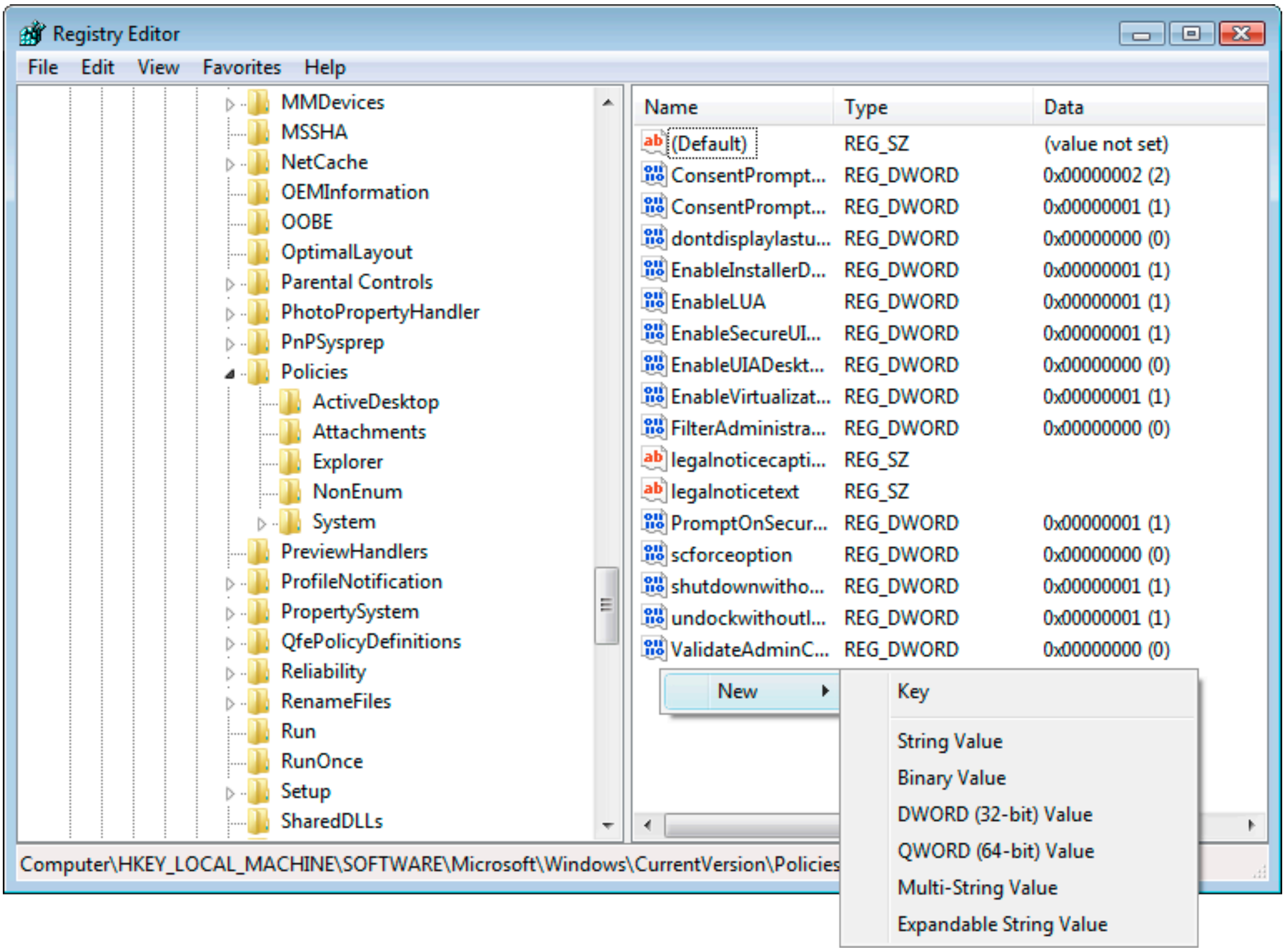
Open: regedit

In the newly appeared window, enter Regedit. Windows Registry Editor will open. Navigate to the following registry branch:

[HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM]

If the **LocalAccountTokenFilterPolicy** key does not exist, create it:

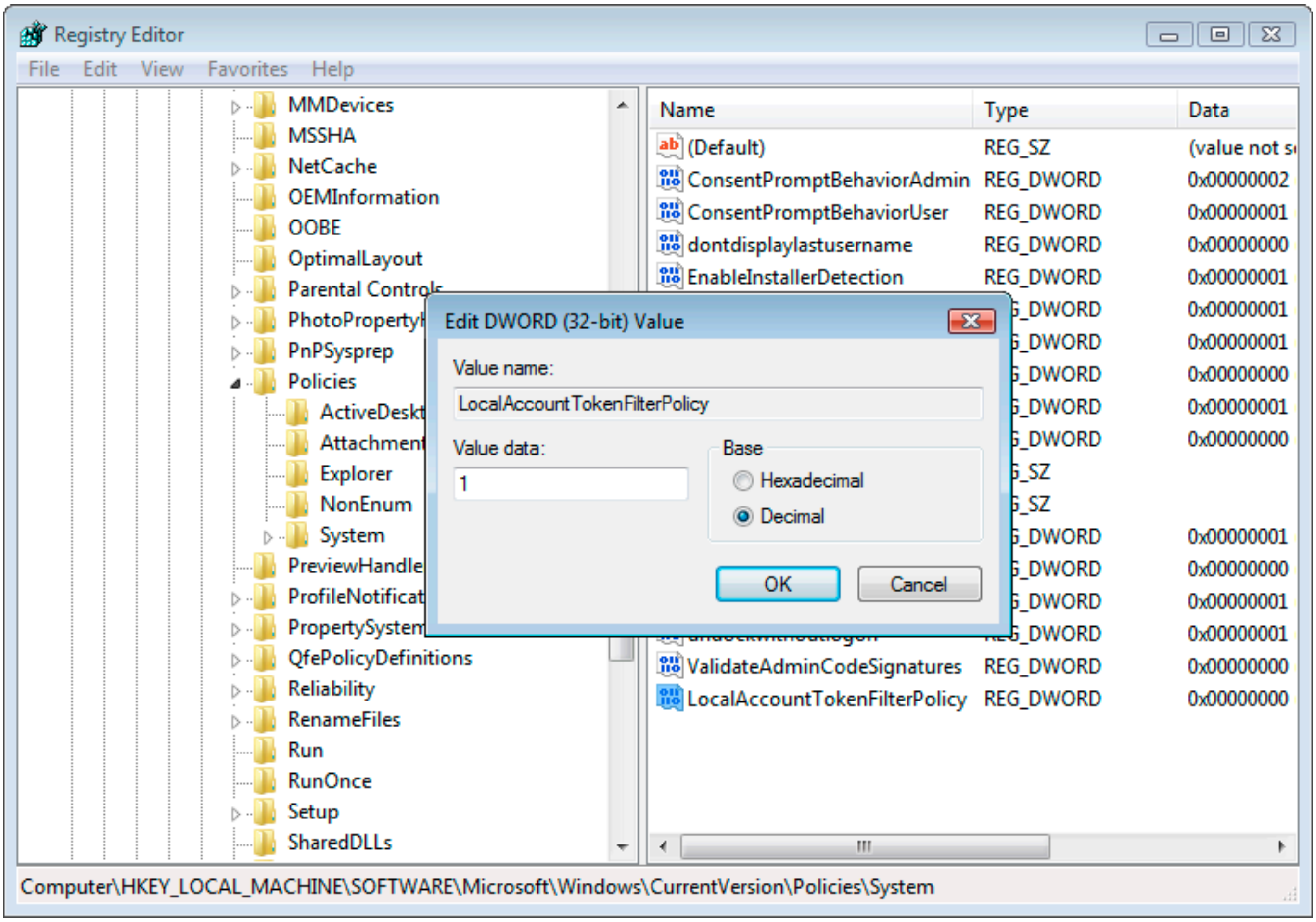
Go to the right pane of the Registry Editor window, right click your mouse and in the context menu, select the option **New** → **DWORD (32-bit) Value**.



Name	Type	Data
(Default)	REG_SZ	(value not set)
ConsentPrompt...	REG_DWORD	0x00000002 (2)
ConsentPrompt...	REG_DWORD	0x00000001 (1)
dontdisplaylastu...	REG_DWORD	0x00000000 (0)
EnableInstallerD...	REG_DWORD	0x00000001 (1)
EnableLUA	REG_DWORD	0x00000001 (1)
EnableSecureUI...	REG_DWORD	0x00000001 (1)
EnableUIADeskt...	REG_DWORD	0x00000000 (0)
EnableVirtualizat...	REG_DWORD	0x00000001 (1)
FilterAdministra...	REG_DWORD	0x00000000 (0)
legalnoticecapti...	REG_SZ	
legalnoticetext	REG_SZ	
PromptOnSecur...	REG_DWORD	0x00000001 (1)
scforceoption	REG_DWORD	0x00000000 (0)
shutdownwitho...	REG_DWORD	0x00000001 (1)
undockwithoutl...	REG_DWORD	0x00000001 (1)
ValidateAdminC...	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies

Set the name of the parameter LocalAccountTokenFilterPolicy. Double-click on the newly created parameter. The **Edit DWORD (32-bit) Value** window will appear. Set the value to 1 and click on **OK**.



Name	Type	Data
(Default)	REG_SZ	(value not s
ConsentPromptBehaviorAdmin	REG_DWORD	0x00000002
ConsentPromptBehaviorUser	REG_DWORD	0x00000001
dontdisplaylastusername	REG_DWORD	0x00000000
EnableInstallerDetection	REG_DWORD	0x00000001
	_DWORD	0x00000001
	_DWORD	0x00000001
	_DWORD	0x00000000
	_DWORD	0x00000001
	_DWORD	0x00000000
	_SZ	
	_SZ	
	_DWORD	0x00000001
	_DWORD	0x00000000
	_DWORD	0x00000001
undockwithoutlogon	REG_DWORD	0x00000001
ValidateAdminCodeSignatures	REG_DWORD	0x00000000
LocalAccountTokenFilterPolicy	REG_DWORD	0x00000000

Edit DWORD (32-bit) Value

Value name: LocalAccountTokenFilterPolicy

Value data: 1

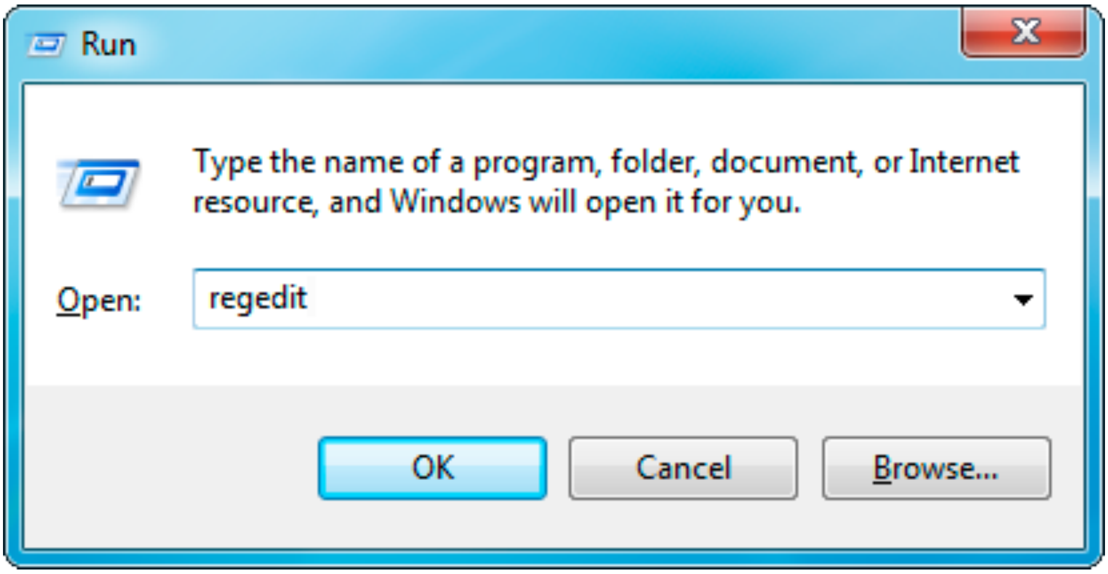
Base: ○ Hexadecimal ● Decimal

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Close the Windows Registry Editor. Change the remaining settings and restart the system.

- **Windows 7**

Click on the **Windows** + **R** buttons.



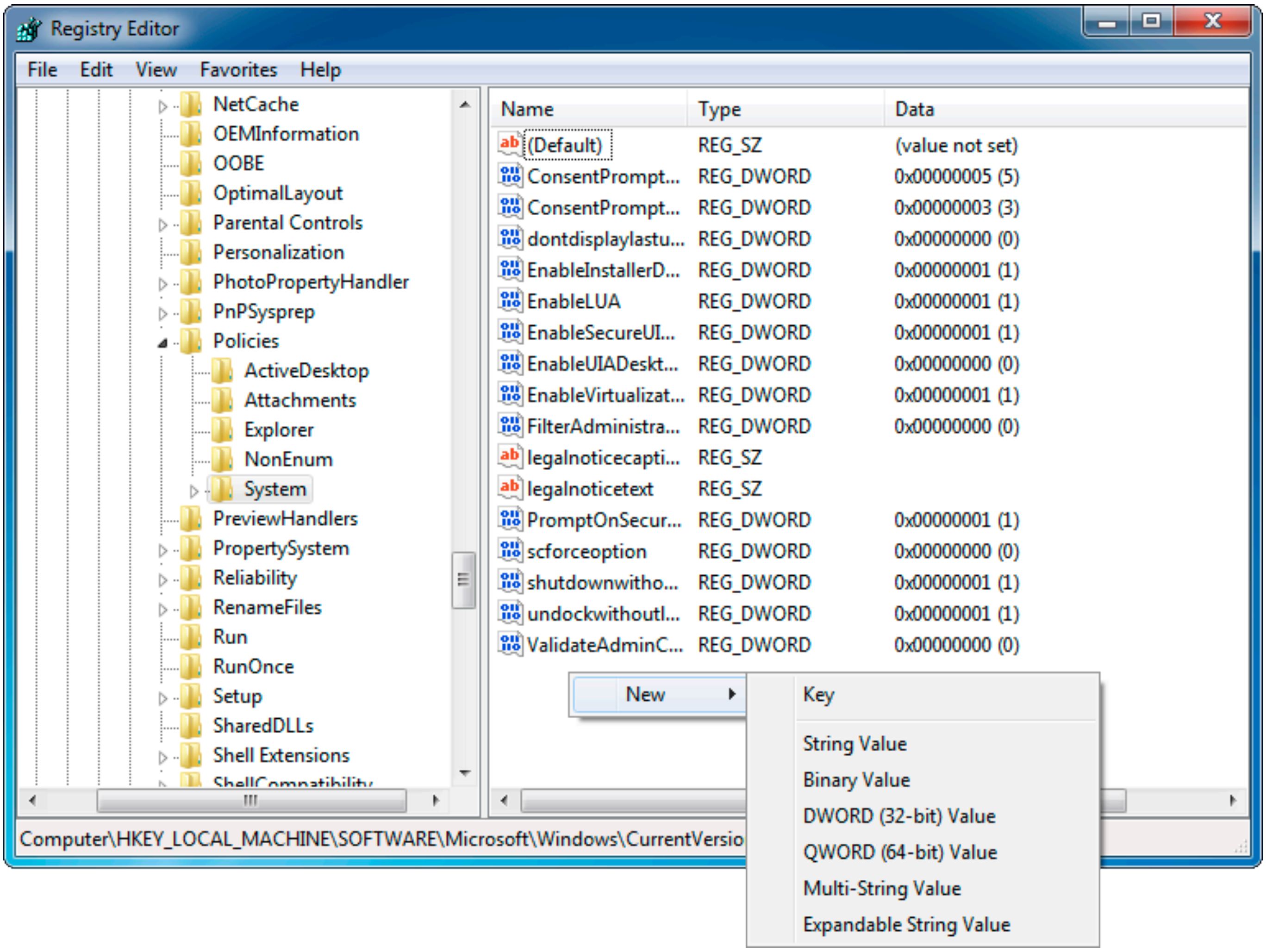
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

In the newly appeared window, enter **Regedit**. The Windows Registry Editor will open. Navigate to the following registry branch:

[HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM]

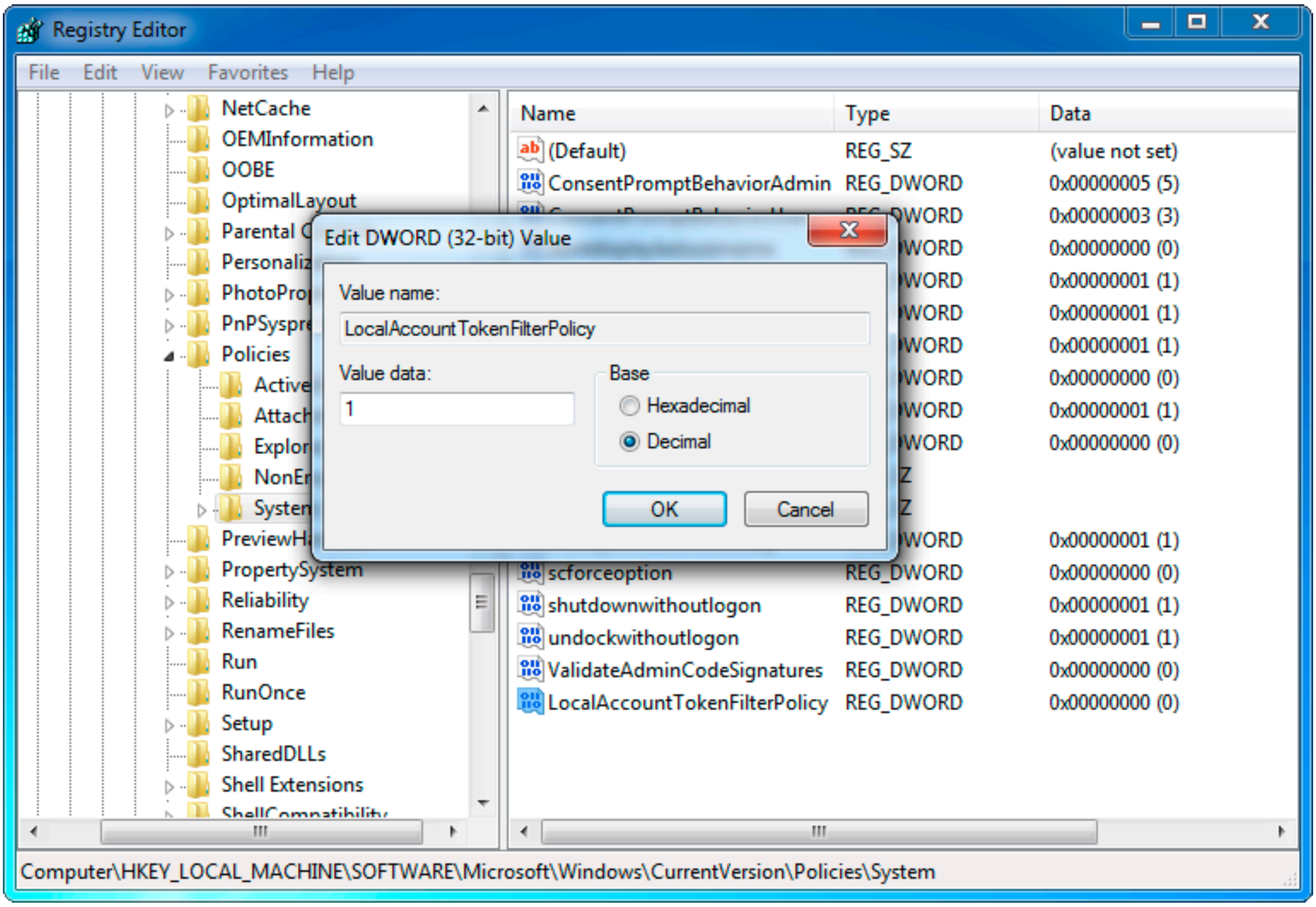
In the right pane of the Registry Editor window, right click on your mouse, and in the context menu, select **DWORD (32-bit) Value**.



Name	Type	Data
(Default)	REG_SZ	(value not set)
ConsentPrompt...	REG_DWORD	0x00000005 (5)
ConsentPrompt...	REG_DWORD	0x00000003 (3)
dontdisplaylastu...	REG_DWORD	0x00000000 (0)
EnableInstallerD...	REG_DWORD	0x00000001 (1)
EnableLUA	REG_DWORD	0x00000001 (1)
EnableSecureUI...	REG_DWORD	0x00000001 (1)
EnableUIADeskt...	REG_DWORD	0x00000000 (0)
EnableVirtualizat...	REG_DWORD	0x00000001 (1)
FilterAdministra...	REG_DWORD	0x00000000 (0)
legalnoticecapti...	REG_SZ	
legalnoticetext	REG_SZ	
PromptOnSecur...	REG_DWORD	0x00000001 (1)
scforceoption	REG_DWORD	0x00000000 (0)
shutdownwitho...	REG_DWORD	0x00000001 (1)
undockwithoutl...	REG_DWORD	0x00000001 (1)
ValidateAdminC...	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersio

Set the name of the parameter LocalAccountTokenFilterPolicy. Double-click on the newly created parameter. The **Edit DWORD (32-bit) Value** window will appear. Set the value to 1 and click on **OK**.



Name	Type	Data
(Default)	REG_SZ	(value not set)
ConsentPromptBehaviorAdmin	REG_DWORD	0x00000005 (5)
	REG_DWORD	0x00000003 (3)
	WORD	0x00000000 (0)
	WORD	0x00000001 (1)
	WORD	0x00000001 (1)
	WORD	0x00000001 (1)
	WORD	0x00000000 (0)
	WORD	0x00000001 (1)
	WORD	0x00000000 (0)
	Z	
	Z	
	WORD	0x00000001 (1)
scforceoption	REG_DWORD	0x00000000 (0)
shutdownwithoutlogon	REG_DWORD	0x00000001 (1)
undockwithoutlogon	REG_DWORD	0x00000001 (1)
ValidateAdminCodeSignatures	REG_DWORD	0x00000000 (0)
LocalAccountTokenFilterPolicy	REG_DWORD	0x00000000 (0)

Edit DWORD (32-bit) Value

Value name:

LocalAccountTokenFilterPolicy

Value data:

1

Base

○ Hexadecimal

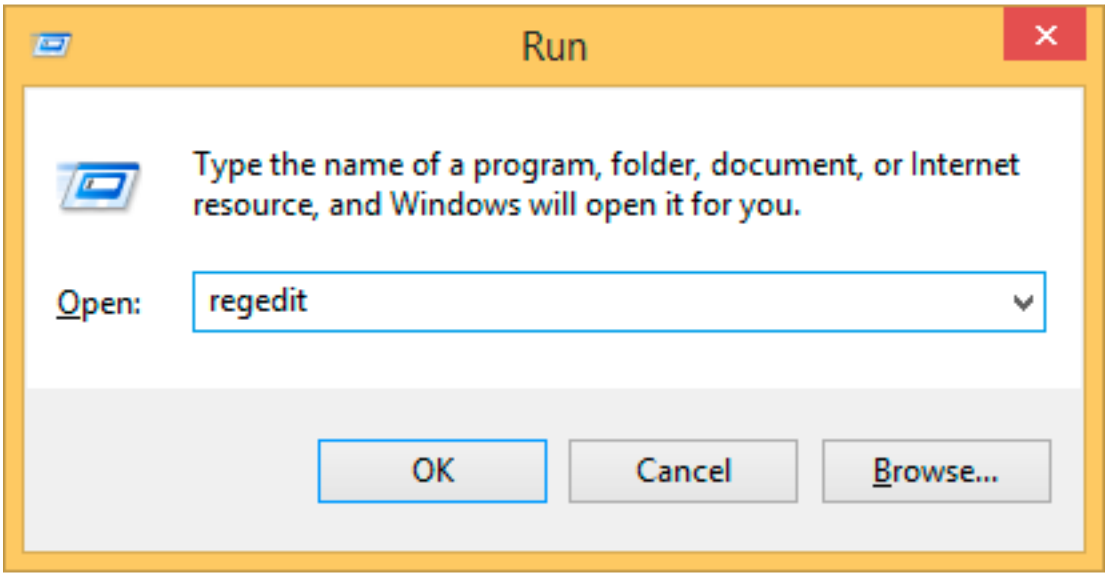
● Decimal

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Quit the Registry Editor. Change the remaining settings and restart the system.

- **Windows 8, 10, Windows 8.1, Windows Server 2012**

Click on the **Windows** + **R** buttons.



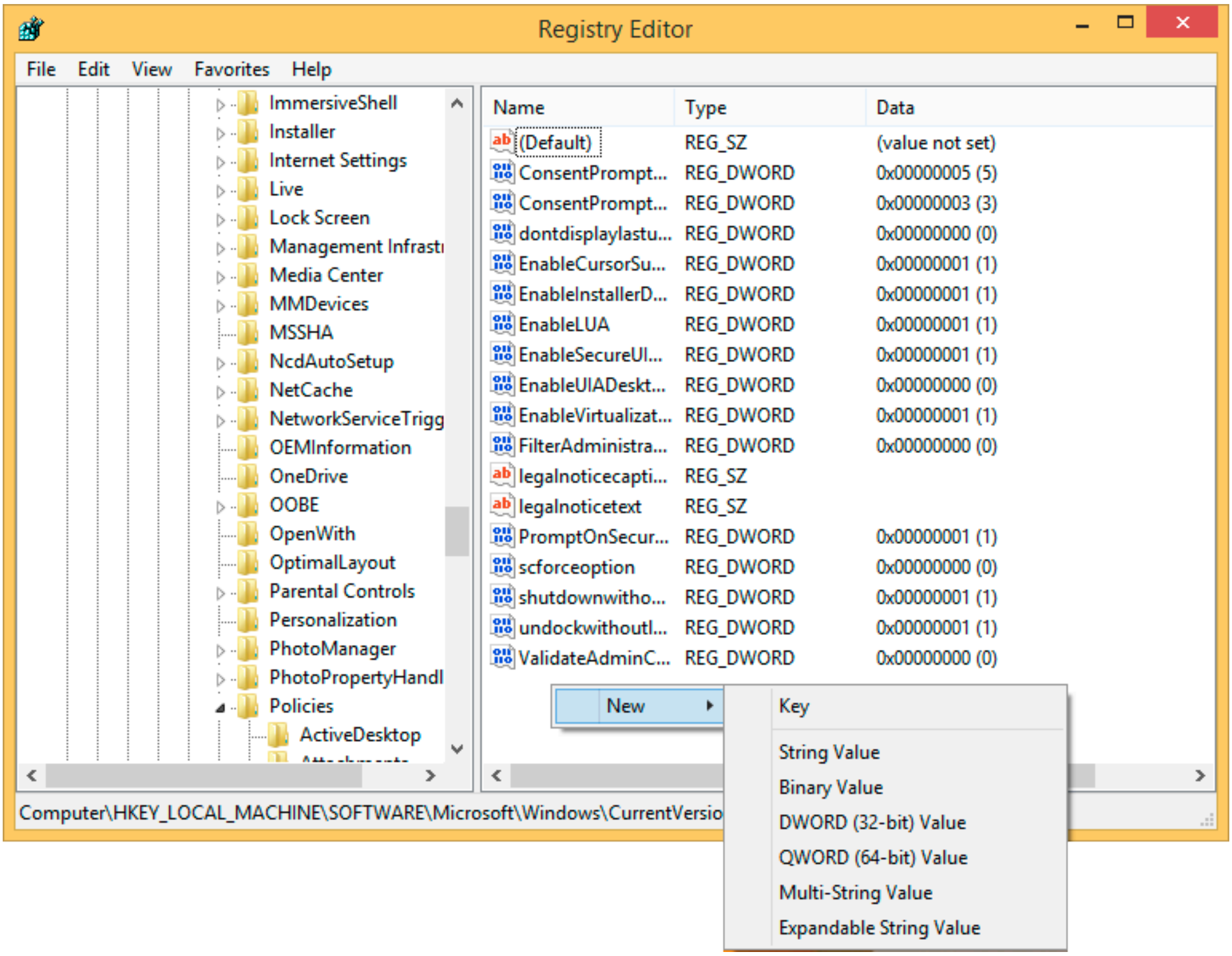
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

In the newly appeared window, enter **Regedit**. The Windows Registry Editor will open. Navigate to the following registry branch:

[HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM]

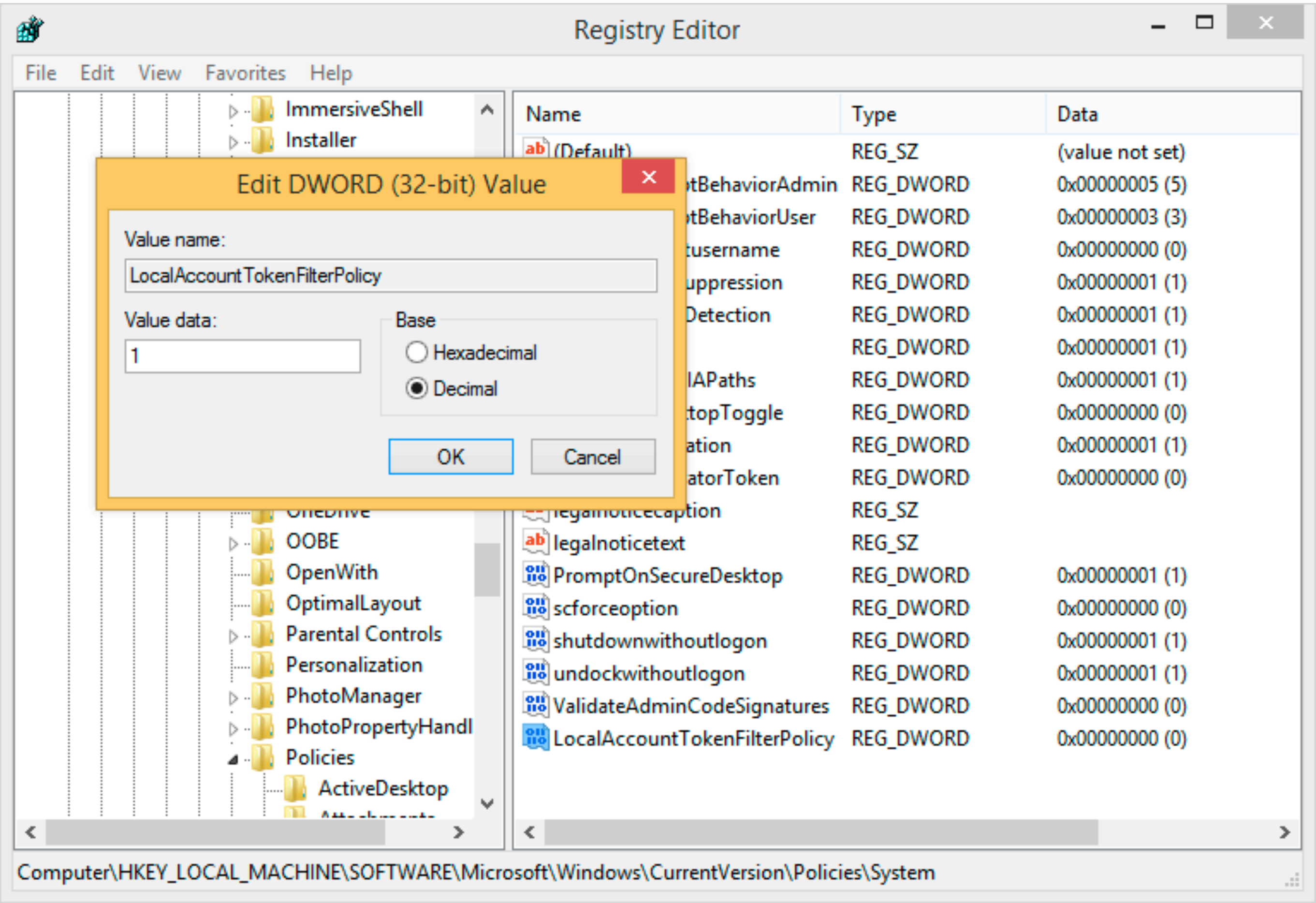
In the right pane of the Registry Editor window, right click on your mouse and select **DWORD (32-bit) Value**.



Name	Type	Data
(Default)	REG_SZ	(value not set)
ConsentPrompt...	REG_DWORD	0x00000005 (5)
ConsentPrompt...	REG_DWORD	0x00000003 (3)
dontdisplaylastu...	REG_DWORD	0x00000000 (0)
EnableCursorSu...	REG_DWORD	0x00000001 (1)
EnableInstallerD...	REG_DWORD	0x00000001 (1)
EnableLUA	REG_DWORD	0x00000001 (1)
EnableSecureUI...	REG_DWORD	0x00000001 (1)
EnableUIADeskt...	REG_DWORD	0x00000000 (0)
EnableVirtualizat...	REG_DWORD	0x00000001 (1)
FilterAdministra...	REG_DWORD	0x00000000 (0)
legalnoticecapti...	REG_SZ	
legalnoticetext	REG_SZ	
PromptOnSecur...	REG_DWORD	0x00000001 (1)
scforceoption	REG_DWORD	0x00000000 (0)
shutdownwitho...	REG_DWORD	0x00000001 (1)
undockwithoutl...	REG_DWORD	0x00000001 (1)
ValidateAdminC...	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersio

Set the name of the parameter LocalAccountTokenFilterPolicy. Double-click on the newly created parameter. The **Edit DWORD (32-bit) Value** window will appear. Set the value to 1 and click on **OK**.



Edit DWORD (32-bit) Value

Value name: LocalAccountTokenFilterPolicy

Value data: 1

Base

○ Hexadecimal

● Decimal

Name	Type	Data
(Default)	REG_SZ	(value not set)
tBehaviorAdmin	REG_DWORD	0x00000005 (5)
tBehaviorUser	REG_DWORD	0x00000003 (3)
tusername	REG_DWORD	0x00000000 (0)
uppression	REG_DWORD	0x00000001 (1)
Detection	REG_DWORD	0x00000001 (1)
	REG_DWORD	0x00000001 (1)
IAPaths	REG_DWORD	0x00000001 (1)
topToggle	REG_DWORD	0x00000000 (0)
ation	REG_DWORD	0x00000001 (1)
atorToken	REG_DWORD	0x00000000 (0)
legalnoticecaption	REG_SZ	
legalnoticetext	REG_SZ	
PromptOnSecureDesktop	REG_DWORD	0x00000001 (1)
scforceoption	REG_DWORD	0x00000000 (0)
shutdownwithoutlogon	REG_DWORD	0x00000001 (1)
undockwithoutlogon	REG_DWORD	0x00000001 (1)
ValidateAdminCodeSignatures	REG_DWORD	0x00000000 (0)
LocalAccountTokenFilterPolicy	REG_DWORD	0x00000000 (0)

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

Quit the registry editor. Change the remaining settings (as described in sections 2-6) and restart the system.

Configuring the Firewall

If a firewall is being used to protect the remote computer, additional configuration, as described below, is required.

If you use Windows Firewall, in its settings tab, go to **Advanced options**, select **Inbound Rules**, and enable the following exceptions: **Netlogon service (NP-In)** and **File sharing and printer sharing (SMB-In)**.

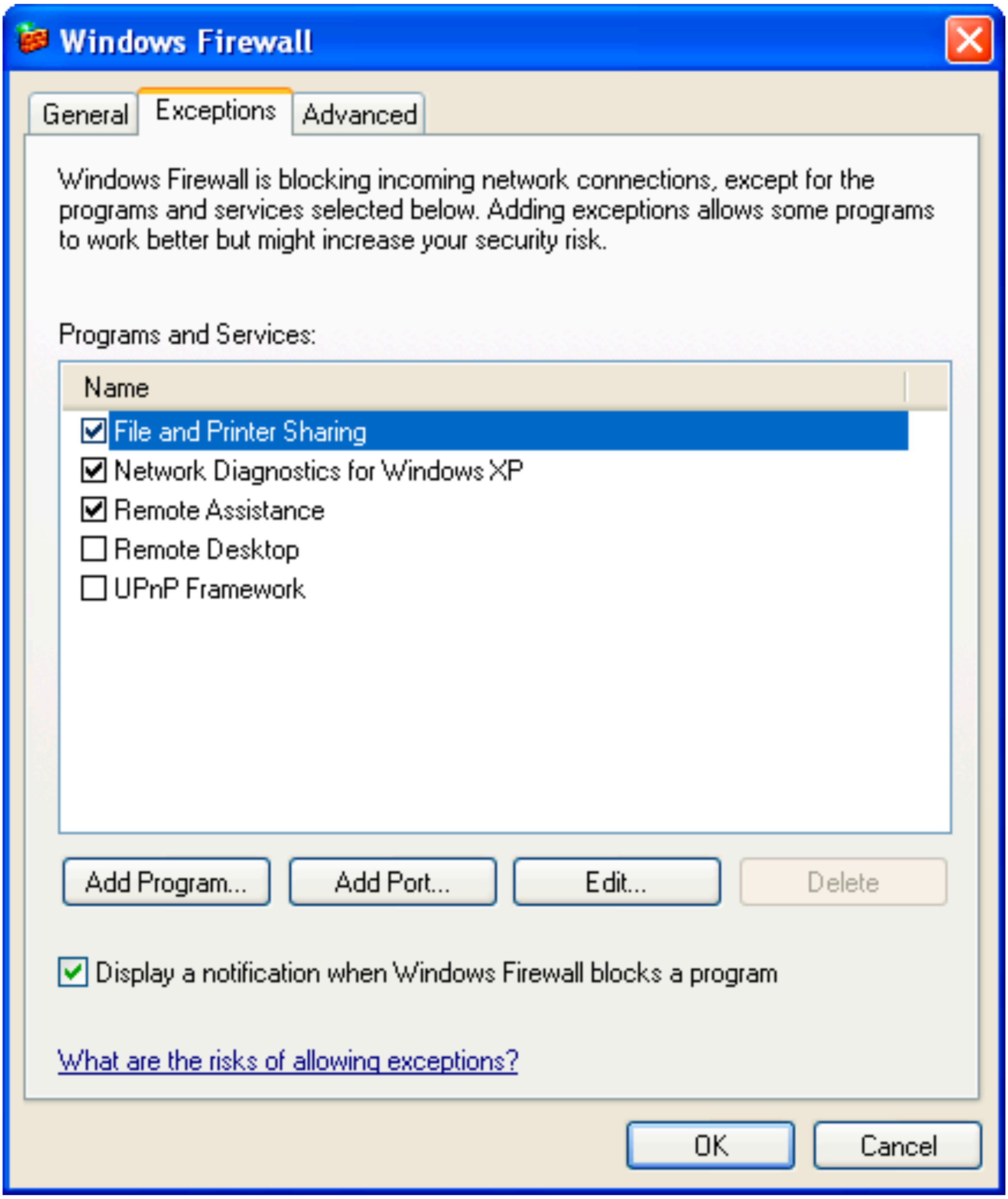
Exceptions must be enabled for the **Private** firewall profile. If the station is in a domain, exceptions must be enabled for the **Domain** profile.

If you are using other firewalls, you must open port 445.

An example of **File and Printer Sharing** settings if the Windows Firewall is used:

- **Windows XP, Windows 2003**

Go to **Start** → **Control Panel** → **Windows Firewall**. The **Windows Firewall** window will open. Go to the **Exceptions** tab. Select the **File and Printer Sharing** option. Click on **OK**.



Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

Name

☑ File and Printer Sharing

☑ Network Diagnostics for Windows XP

☑ Remote Assistance

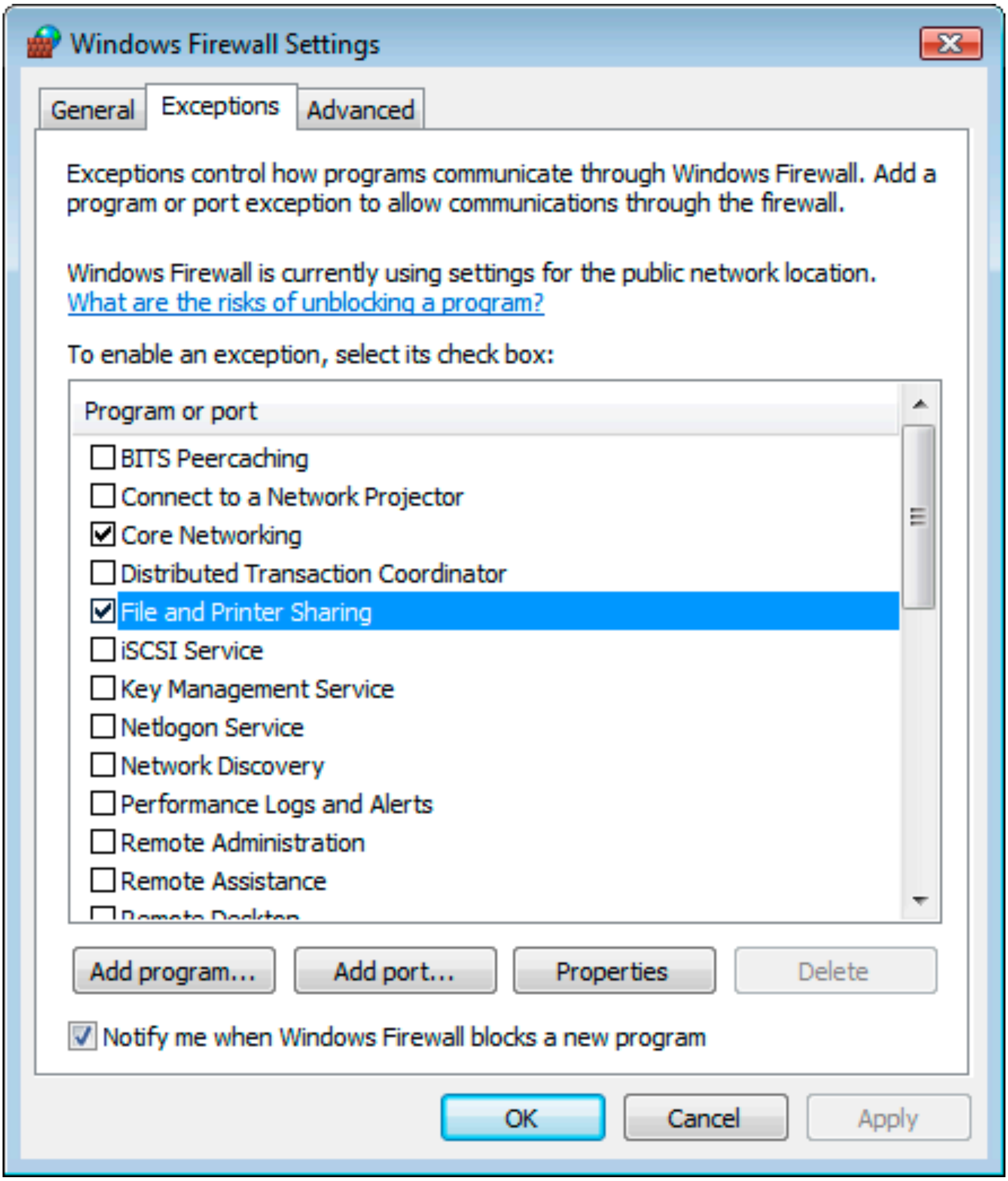
□ Remote Desktop

□ UPnP Framework

☑ Display a notification when Windows Firewall blocks a program

- **Windows Vista, Windows Server 2008**

Go to **Start** → **Control Panel** → **Security** →**Windows Firewall**. Click on **Turn Windows Firewall on or off**. In the **Windows Firewall** window, go to **Exceptions**. Check the **File and Printer Sharing** box.



Windows Firewall Settings

General | Exceptions | Advanced

Exceptions control how programs communicate through Windows Firewall. Add a program or port exception to allow communications through the firewall.

Windows Firewall is currently using settings for the public network location.
What are the risks of unblocking a program?

To enable an exception, select its check box:

Program or port

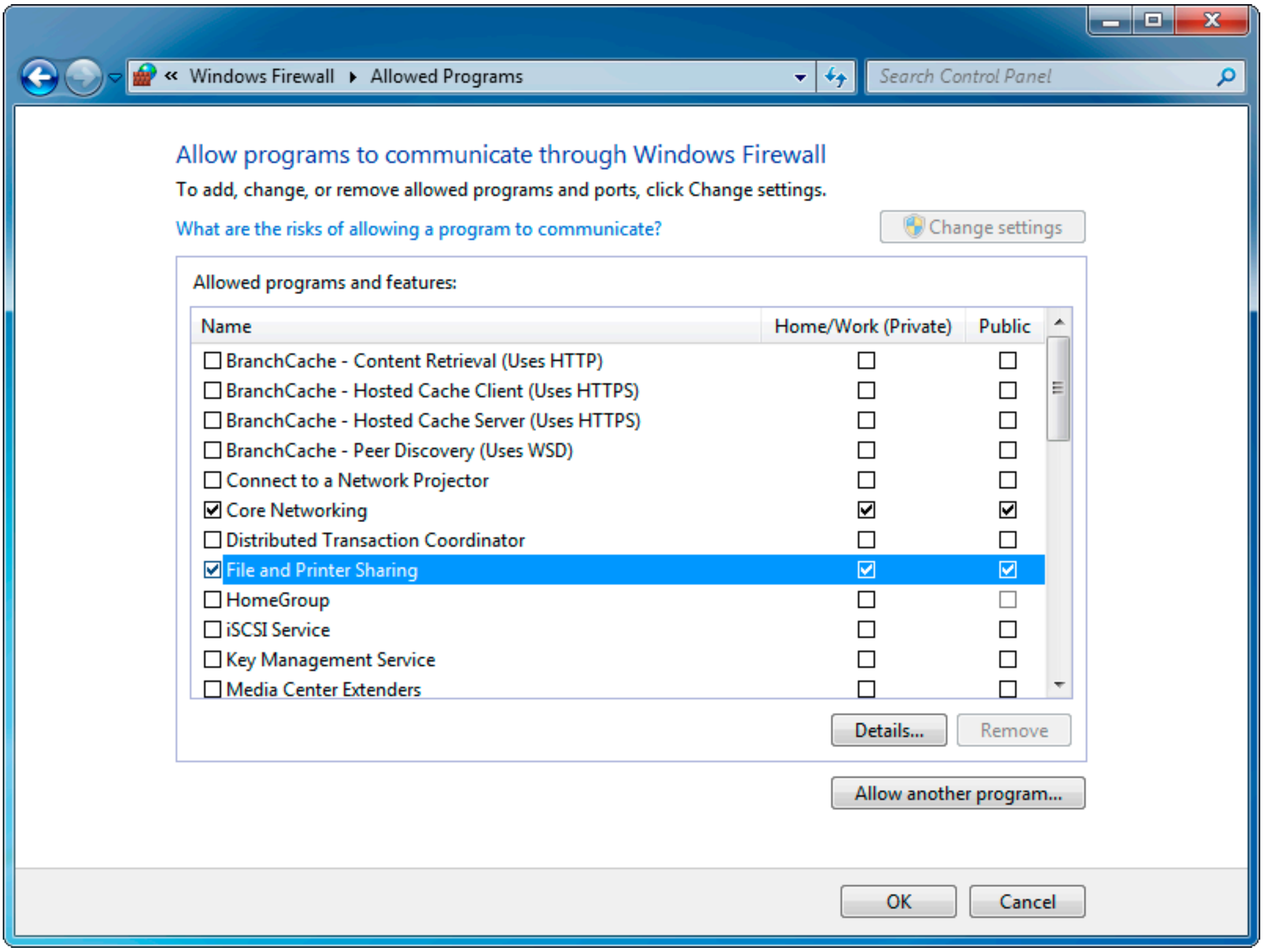
- □ BITS Peercaching
- □ Connect to a Network Projector
- ☑ Core Networking
- □ Distributed Transaction Coordinator
- ☑ File and Printer Sharing
- □ iSCSI Service
- □ Key Management Service
- □ Netlogon Service
- □ Network Discovery
- □ Performance Logs and Alerts
- □ Remote Administration
- □ Remote Assistance
- □ Remote Desktop

☑ Notify me when Windows Firewall blocks a new program

Click on **OK**.

- **Windows 7, Windows Server 2008 R2**

Click on **Start** and go to **Control Panel** → **System and Security** → **Windows Firewall** → **Allow programs to communicate through Windows Firewall**. Click on **Change settings**. Check the **File and Printer Sharing** box.



Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

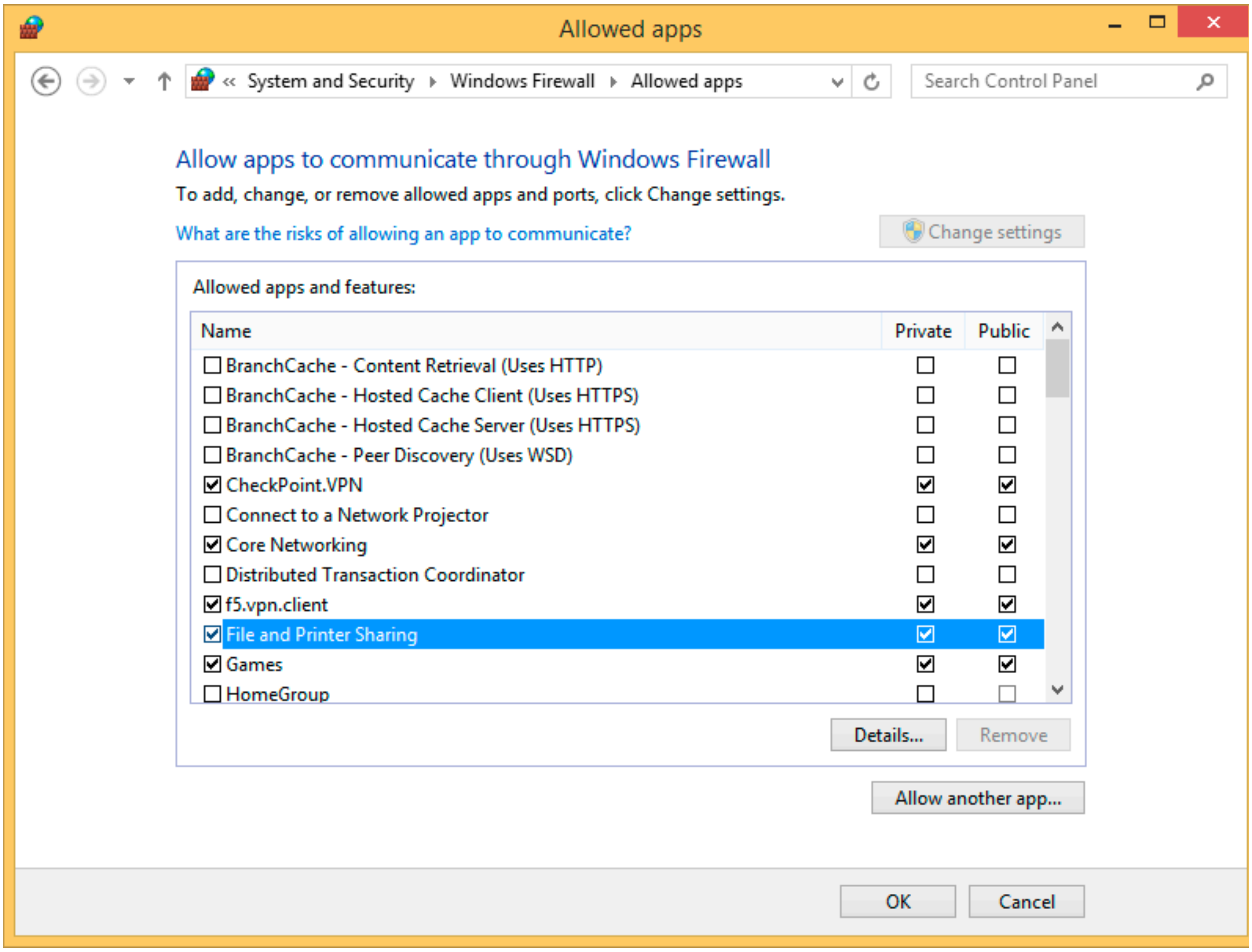
Allowed programs and features:

Name	Home/Work (Private)	Public
□ BranchCache - Content Retrieval (Uses HTTP)	□	□
□ BranchCache - Hosted Cache Client (Uses HTTPS)	□	□
□ BranchCache - Hosted Cache Server (Uses HTTPS)	□	□
□ BranchCache - Peer Discovery (Uses WSD)	□	□
□ Connect to a Network Projector	□	□
☑ Core Networking	☑	☑
□ Distributed Transaction Coordinator	□	□
☑ File and Printer Sharing	☑	☑
□ HomeGroup	□	□
□ iSCSI Service	□	□
□ Key Management Service	□	□
□ Media Center Extenders	□	□

Click on **OK**.

- **Windows 8, 10, Windows 8.1 Windows Server 2012**

Click on the **Windows** + **X** buttons. In the newly appeared context menu, select **Control Panel** → **System and Security** → **Windows Firewall** → **Allow programs to communicate through Windows Firewall**. Click on **Change settings**. Check the **File and Printer Sharing** box.



Allow apps to communicate through Windows Firewall

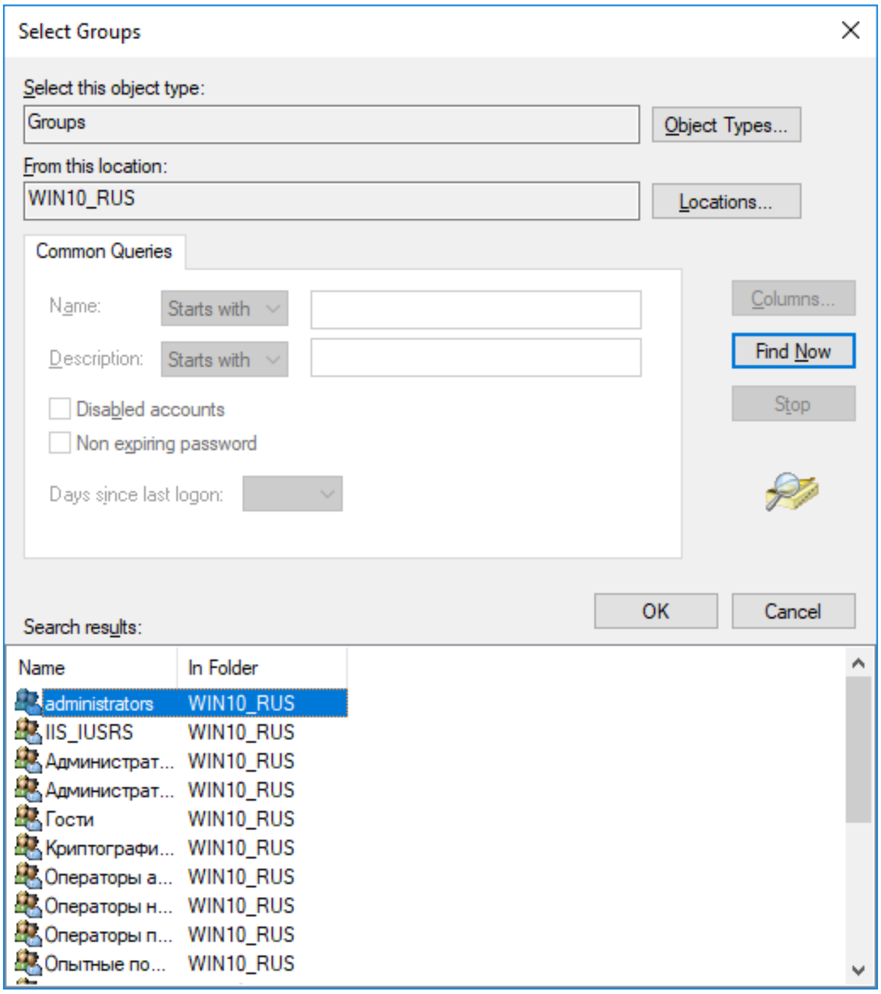
To add, change, or remove allowed apps and ports, click Change settings.

What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
☐ BranchCache - Content Retrieval (Uses HTTP)	☐	☐
☐ BranchCache - Hosted Cache Client (Uses HTTPS)	☐	☐
☐ BranchCache - Hosted Cache Server (Uses HTTPS)	☐	☐
☐ BranchCache - Peer Discovery (Uses WSD)	☐	☐
☑ CheckPoint.VPN	☑	☑
☐ Connect to a Network Projector	☐	☐
☑ Core Networking	☑	☑
☐ Distributed Transaction Coordinator	☐	☐
☑ f5.vpn.client	☑	☑
☑ File and Printer Sharing	☑	☑
☑ Games	☑	☑
☐ HomeGroup	☐	☐

If you have installed another firewall, this group of settings will be blocked.



Select this object type: Groups

From this location: WIN10_RUS

Search results:

Name	In Folder
administrators	WIN10_RUS
IIS_IUSRS	WIN10_RUS
Администрат...	WIN10_RUS
Администрат...	WIN10_RUS
Гости	WIN10_RUS
Криптографи...	WIN10_RUS
Операторы а...	WIN10_RUS
Операторы н...	WIN10_RUS
Операторы п...	WIN10_RUS
Опытные по...	WIN10_RUS

Click on **OK**.

Configuring Local Security Policy.

The sharing and security model should be used for local accounts.

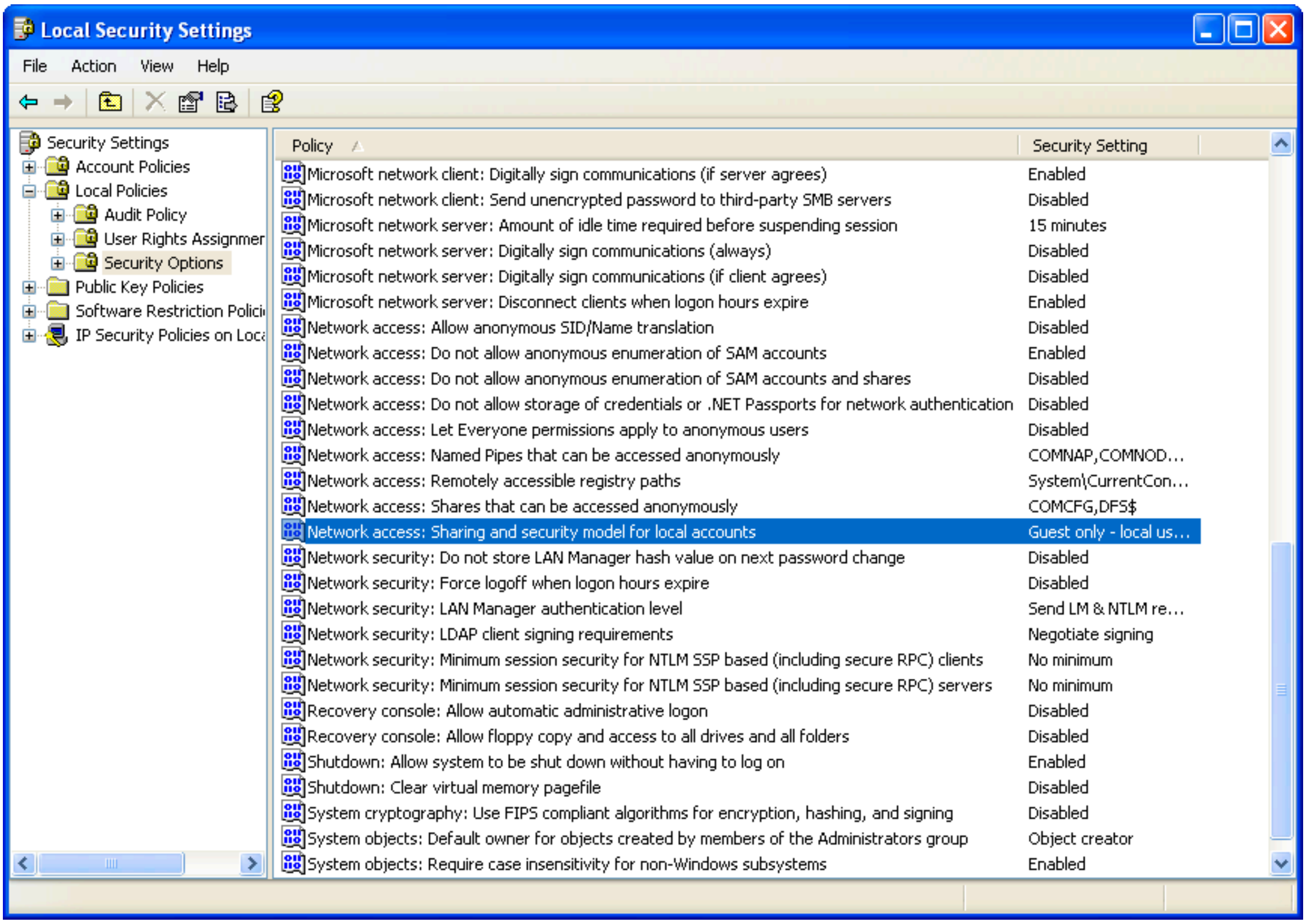
By default, the connection to the remote computer cannot be established if the account used contains a blank password. To connect, specify a non-empty password.

- **Windows XP, Windows 2003**

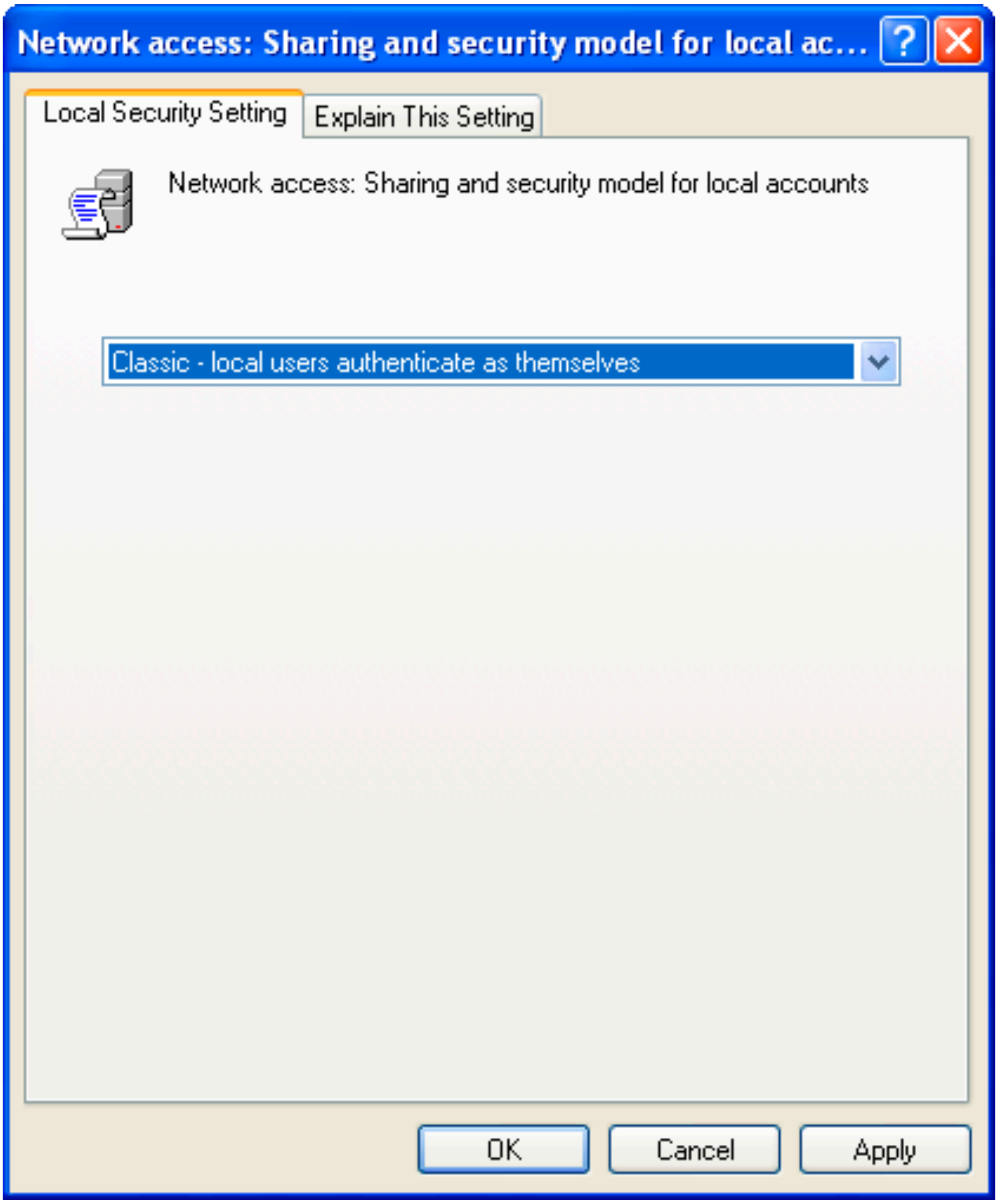
Go to **Control Panel** → **Administration** (if this section is missing, click on **Switch to standard view**) → **Local Security Policy** → **Local policies** → **Security settings**.

Double-click on the policy **Network access: sharing and security model for local accounts**. The **Properties** window will open. Select **Classic — local users authenticate as themselves.**

To start the local security policy configuration utility, you can also type the command **secpol.msc** in the Windows search field and click on **ENTER.**



Policy	Security Setting
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Disabled
Network access: Let Everyone permissions apply to anonymous users	Disabled
Network access: Named Pipes that can be accessed anonymously	COMNAP,COMNOD...
Network access: Remotely accessible registry paths	System\CurrentCon...
Network access: Shares that can be accessed anonymously	COMCFG,DFS$
Network access: Sharing and security model for local accounts	Guest only - local us...
Network security: Do not store LAN Manager hash value on next password change	Disabled
Network security: Force logoff when logon hours expire	Disabled
Network security: LAN Manager authentication level	Send LM & NTLM re...
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	No minimum
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	No minimum
Recovery console: Allow automatic administrative logon	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled
Shutdown: Allow system to be shut down without having to log on	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled
System objects: Default owner for objects created by members of the Administrators group	Object creator
System objects: Require case insensitivity for non-Windows subsystems	Enabled



Network access: Sharing and security model for local accounts

Classic - local users authenticate as themselves

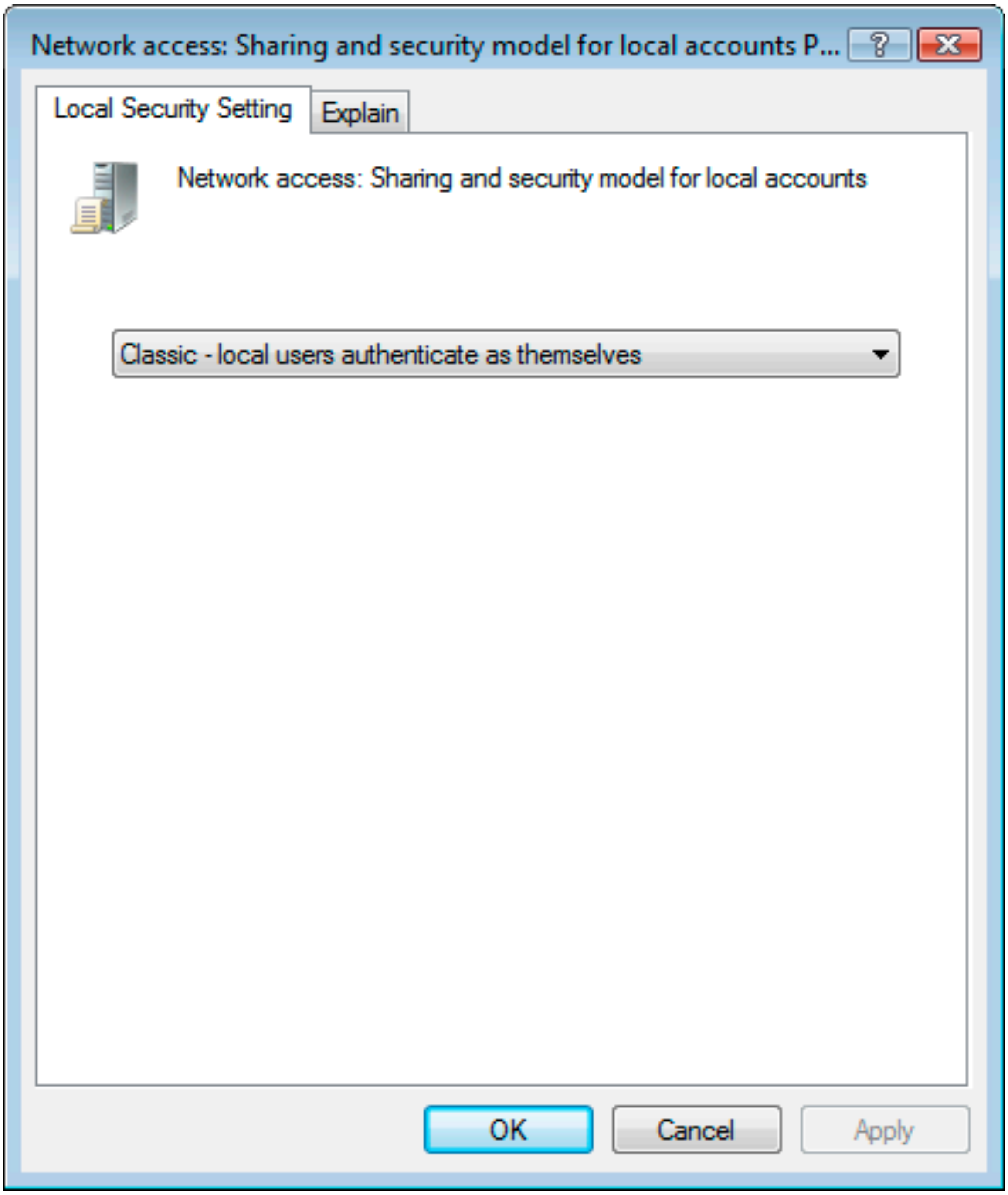
Successively click on **Apply** and **OK**. Close the **Local Security Settings** window.

Right-click on the network connection. In the context menu, select **Properties**. The network connection properties window will open.

Click on **OK**.

- **Windows Vista, Windows Server 2008**

Click on **Start** and go to **Control Panel** → **System and Maintenance** → **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 — local users authenticate as themselves**, and click on **OK**.



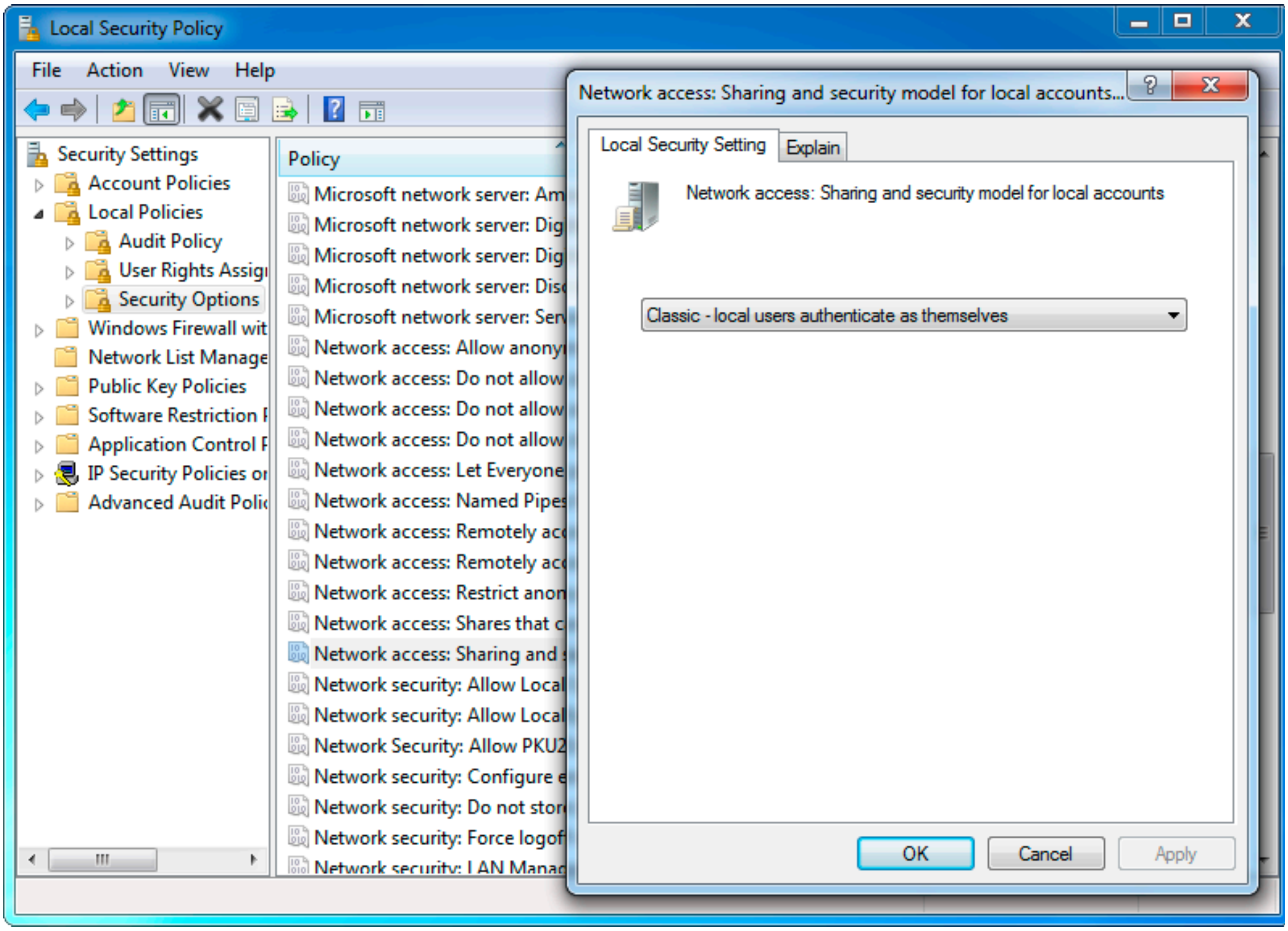
Network access: Sharing and security model for local accounts P...

Network access: Sharing and security model for local accounts

Classic - local users authenticate as themselves

- **Windows 7, Windows Server 2008 R2**

Click on **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 — local users authenticate as themselves**, and click on **OK.**

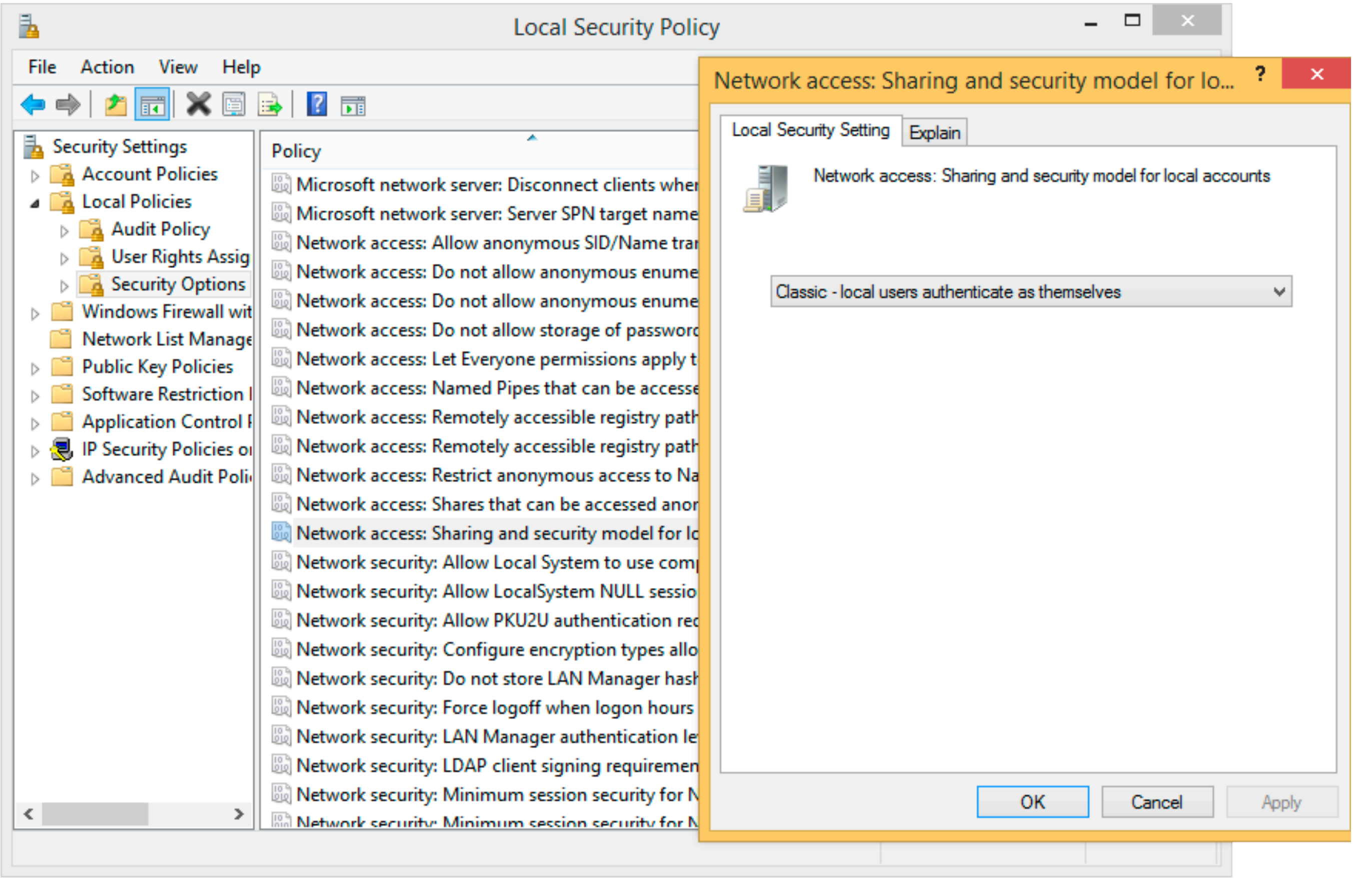

Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assigı
Security Options
Windows Firewall wit
Network List Manage
Public Key Policies
Software Restriction I
Application Control F
IP Security Policies or
Advanced Audit Polic
Policy
Microsoft network server: Am
Microsoft network server: Dig
Microsoft network server: Dig
Microsoft network server: Dis
Microsoft network server: Ser
Network access: Allow anony
Network access: Do not allow
Network access: Do not allow
Network access: Do not allow
Network access: Let Everyone
Network access: Named Pipes
Network access: Remotely acc
Network access: Remotely acc
Network access: Restrict anon
Network access: Shares that c
Network access: Sharing and s
Network security: Allow Local
Network security: Allow Local
Network Security: Allow PKU2
Network security: Configure e
Network security: Do not stor
Network security: Force logof
Network security: LAN Manag
Network access: Sharing and security model for local accounts...
?
Local Security Setting
Explain
OK
Cancel
Apply

Network access: Sharing and security model for local accounts

Classic - local users authenticate as themselves

- **Windows 8, 10, Windows 8.1, Windows Server 2012**

Click on the **Windows** + **X** buttons. In the context menu, select **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 — local users authenticate as themselves**, and click on **OK**.



Microsoft network server: Disconnect clients wher
Microsoft network server: Server SPN target name
Network access: Allow anonymous SID/Name tran
Network access: Do not allow anonymous enume
Network access: Do not allow anonymous enume
Network access: Do not allow storage of passworc
Network access: Let Everyone permissions apply t
Network access: Named Pipes that can be accesse
Network access: Remotely accessible registry path
Network access: Remotely accessible registry path
Network access: Restrict anonymous access to Na
Network access: Shares that can be accessed anor
Network access: Sharing and security model for lo
Network security: Allow Local System to use comp
Network security: Allow LocalSystem NULL sessio
Network security: Allow PKU2U authentication rec
Network security: Configure encryption types allo
Network security: Do not store LAN Manager hash
Network security: Force logoff when logon hours
Network security: LAN Manager authentication le
Network security: LDAP client signing requiremen
Network security: Minimum session security for N
Network security: Minimum session security for N

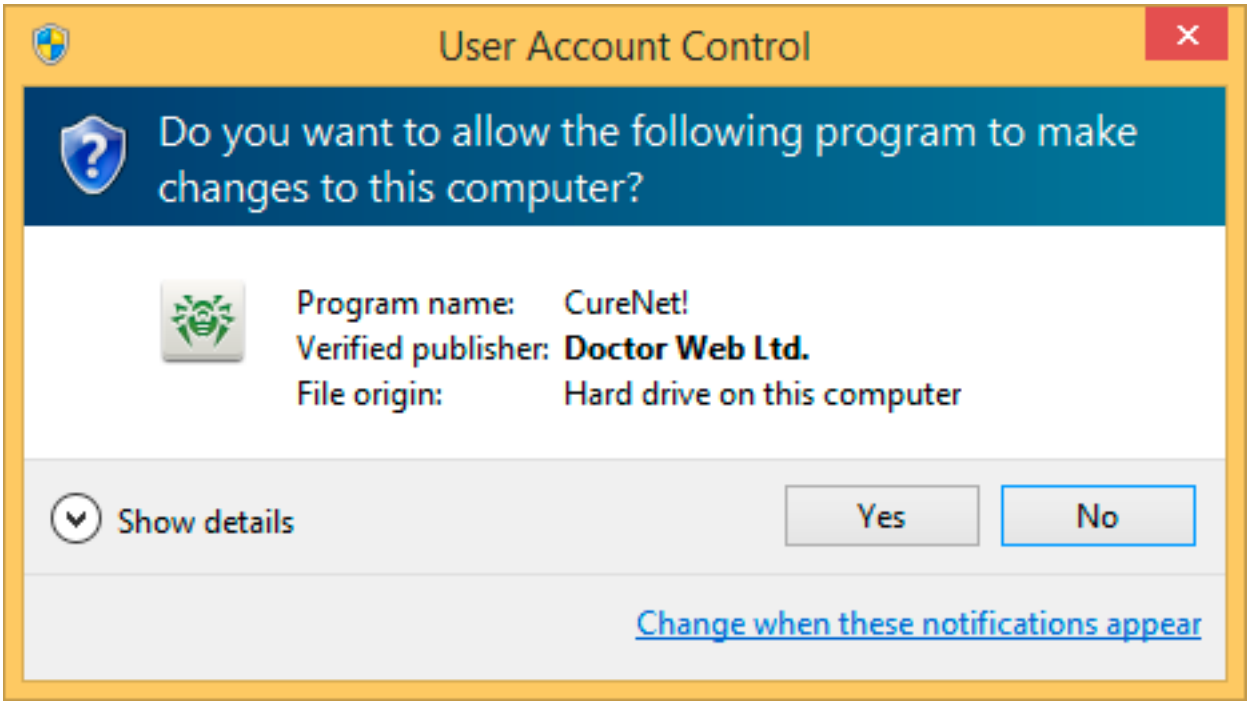
Network access: Sharing and security model for lo...

Network access: Sharing and security model for local accounts

Classic - local users authenticate as themselves

Launching Dr.Web CureNet!

1. Launch the CureNet!.exe file you downloaded, and, if necessary, confirm its launch.



User Account Control

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

Program name: CureNet!

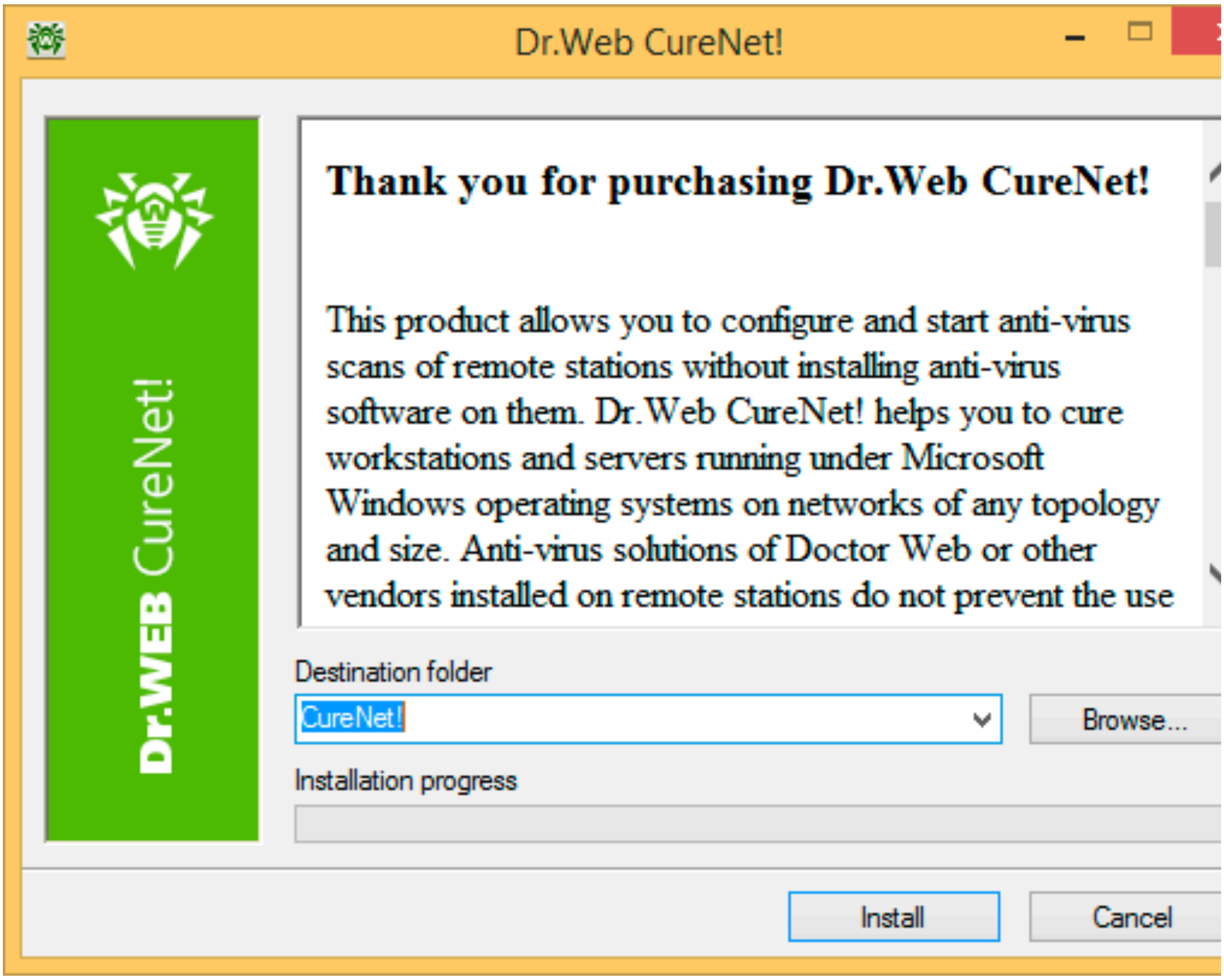
Verified publisher: **Doctor Web Ltd.**

File origin: Hard drive on this computer

Important! The procedure for starting Dr.Web CureNet! after the first launch will be described below.

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

2. Click on **Install** to continue.



Thank you for purchasing Dr.Web CureNet!

This product allows you to configure and start anti-virus scans of remote stations without installing anti-virus software on them. Dr.Web CureNet! helps you to cure workstations and servers running under Microsoft Windows operating systems on networks of any topology and size. Anti-virus solutions of Doctor Web or other vendors installed on remote stations do not prevent the use

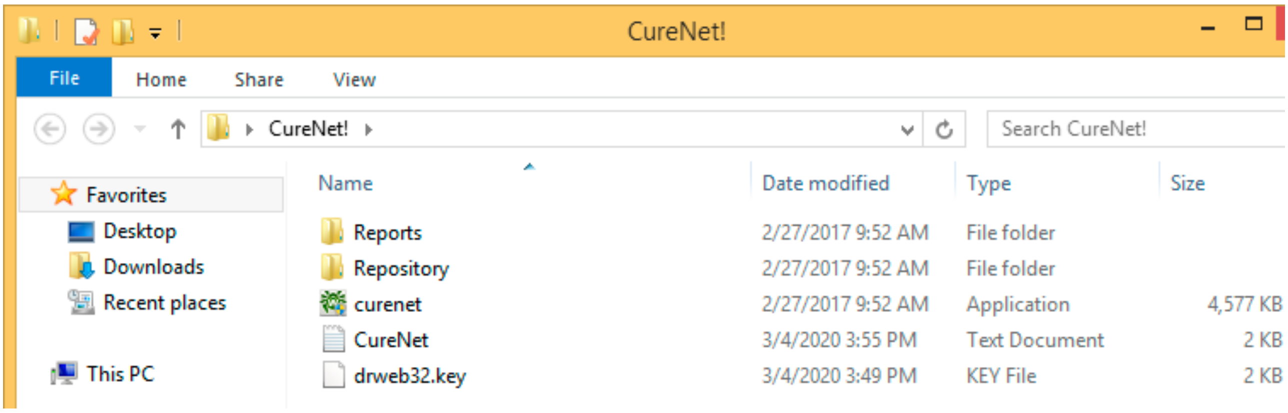
Destination folder: CureNet!

Installation progress

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 **Browse**.

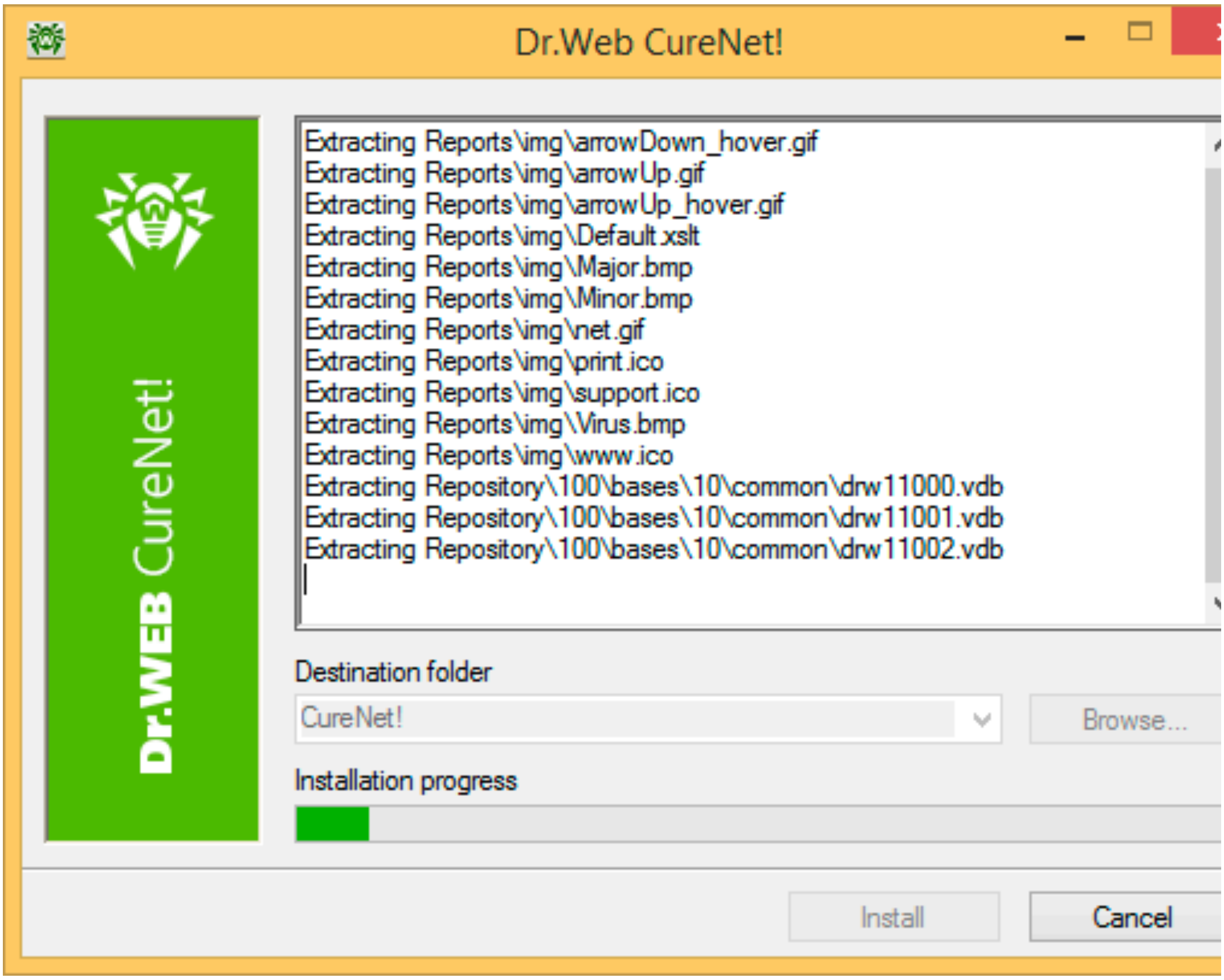
CureNet!.exe is a self-extracting archive and does not require installation. All you need to do is select the location to which the archive's contents will be extracted. The default folder's name is CureNet!, but you can change it to whatever name you like. If you extract the archived files onto a USB flash drive or any other removable data-storage device, you will be able to carry Dr.Web CureNet! with you wherever you go so it is always at hand should any emergency situations arise.

The product's repository files and the key file will be extracted to the destination folder.



Name	Date modified	Type	Size
Reports	2/27/2017 9:52 AM	File folder	
Repository	2/27/2017 9:52 AM	File folder	
curenet	2/27/2017 9:52 AM	Application	4,577 KB
CureNet	3/4/2020 3:55 PM	Text Document	2 KB
drweb32.key	3/4/2020 3:49 PM	KEY File	2 KB

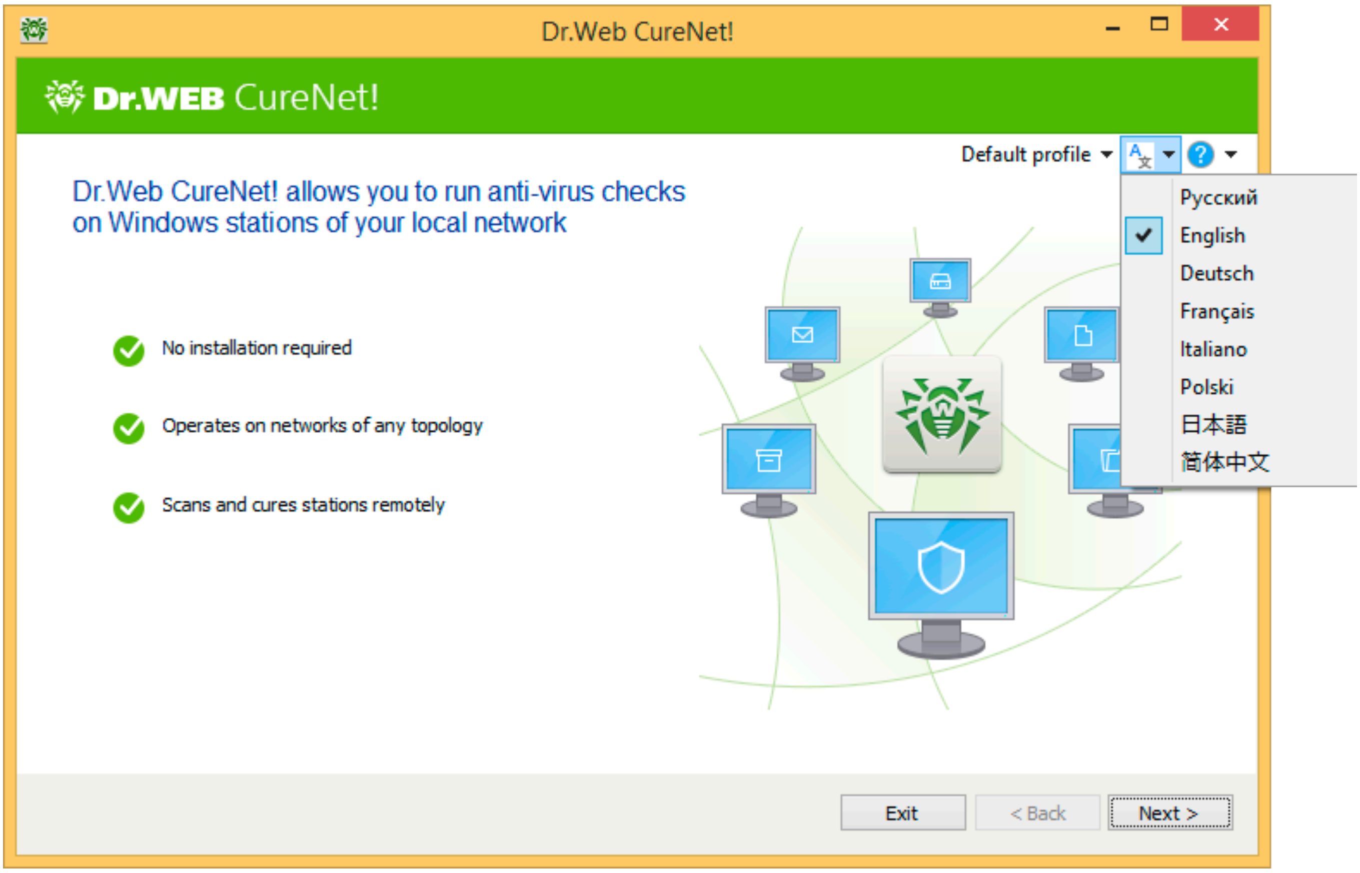
To continue the installation, click on **Install**.



```
Extracting Reports\img\arrowDown_hover.gif
Extracting Reports\img\arrowUp.gif
Extracting Reports\img\arrowUp_hover.gif
Extracting Reports\img\Default.xslt
Extracting Reports\img\Major.bmp
Extracting Reports\img\Minor.bmp
Extracting Reports\img\net.gif
Extracting Reports\img\print.ico
Extracting Reports\img\support.ico
Extracting Reports\img\Virus.bmp
Extracting Reports\img\www.ico
Extracting Repository\100\bases\10\common\drw11000.vdb
Extracting Repository\100\bases\10\common\drw11001.vdb
Extracting Repository\100\bases\10\common\drw11002.vdb
```

Destination folder: CureNet!

4. Click on the button in the upper-right corner 🔤 of the next window to select the localisation language.

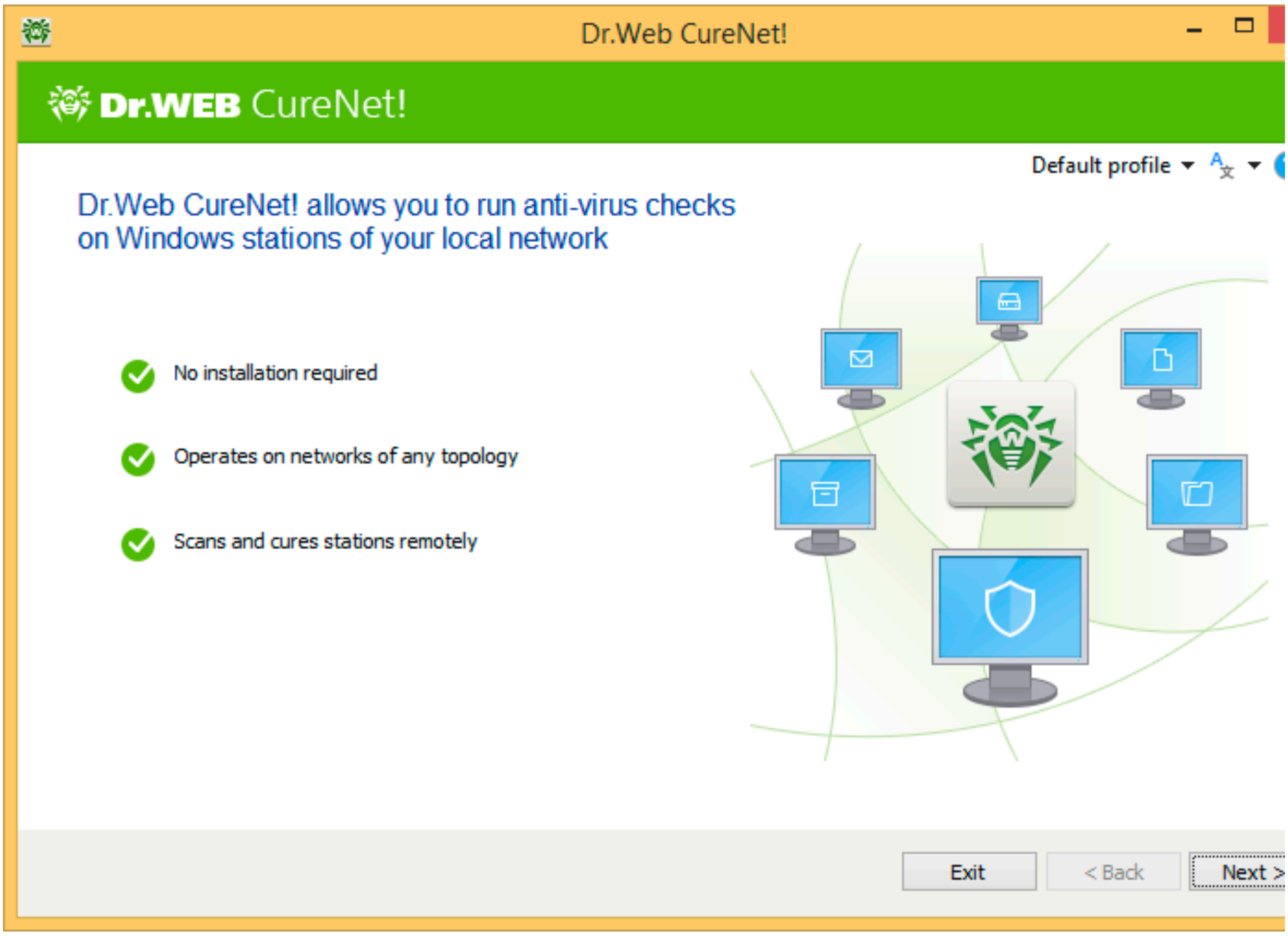


Dr.Web CureNet! allows you to run anti-virus checks on Windows stations of your local network

- No installation required
- Operates on networks of any topology
- Scans and cures stations remotely

Important! If you are using the English language version of your operating system, make sure that it has all the components needed to display English characters.

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

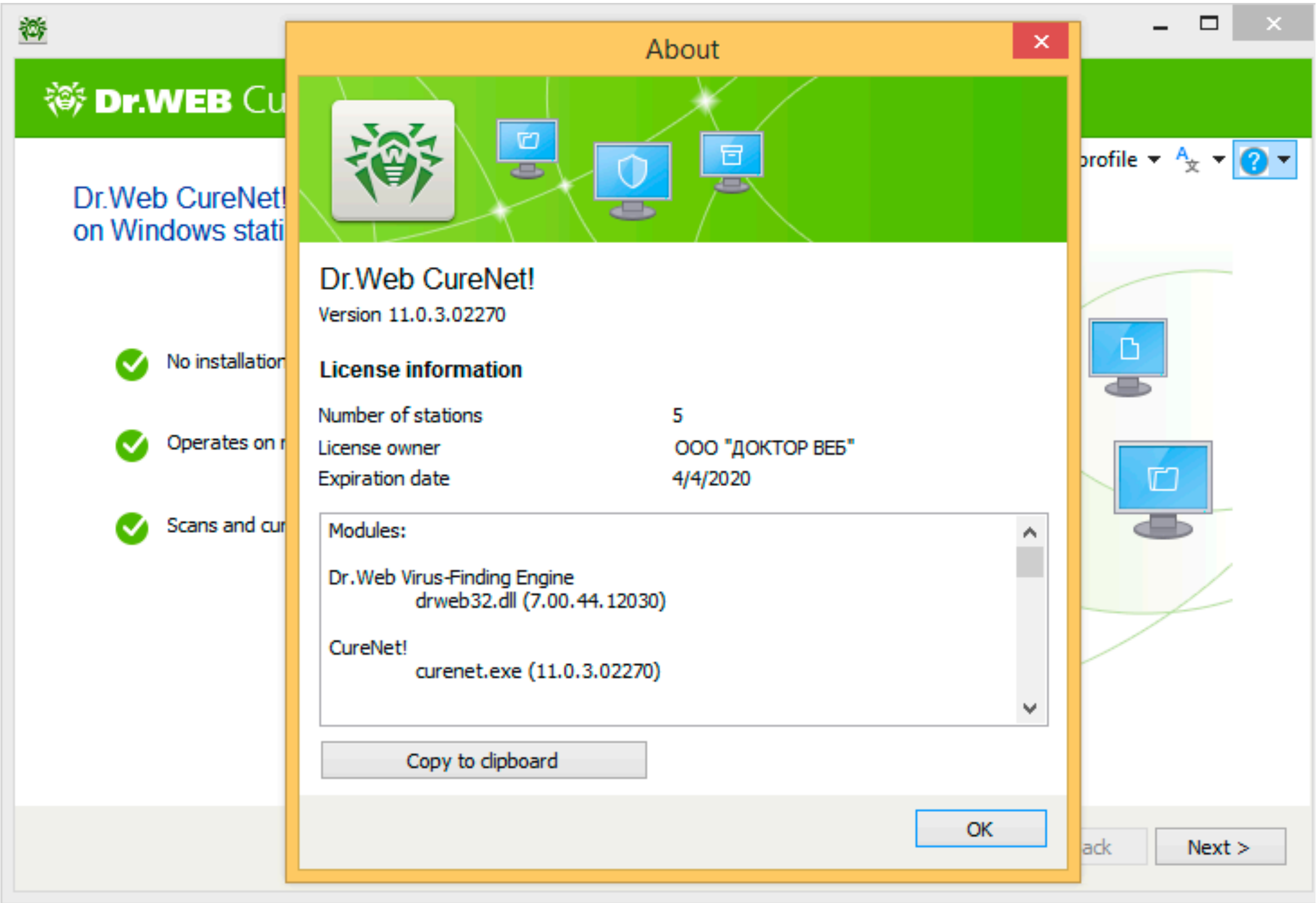


Dr.Web CureNet! allows you to run anti-virus checks on Windows stations of your local network

- ✓ No installation required
- ✓ Operates on networks of any topology
- ✓ Scans and cures stations remotely

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

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



About

Dr.Web CureNet!
Version 11.0.3.02270

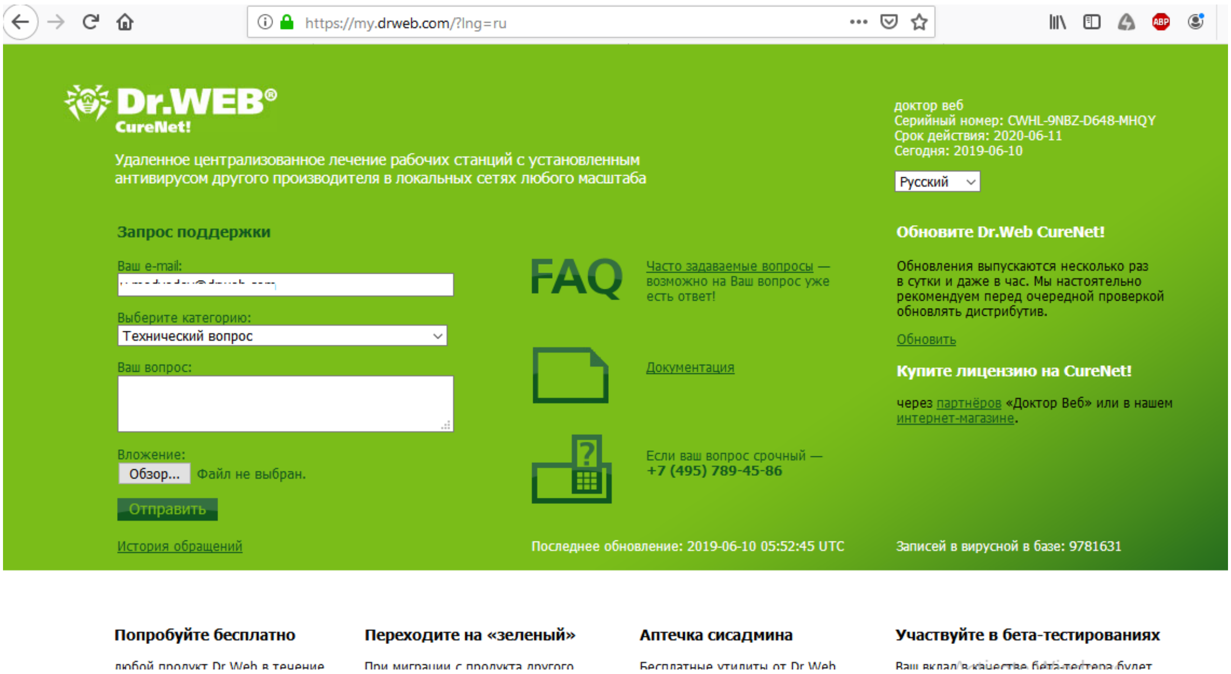
License information

Number of stations	5
License owner	ООО "ДОКТОР ВЕБ"
Expiration date	4/4/2020

```
Modules:

Dr.Web Virus-Finding Engine
        drweb32.dll (7.00.44.12030)

CureNet!
        curenet.exe (11.0.3.02270)
```



https://my.drweb.com/?lng=ru

Удаленное централизованное лечение рабочих станций с установленным антивирусом другого производителя в локальных сетях любого масштаба

доктор веб
Серийный номер: CWHL-9NBZ-D648-MHQY
Срок действия: 2020-06-11
Сегодня: 2019-06-10

Русский

Запрос поддержки

Ваш e-mail:

Выберите категорию: Технический вопрос

Ваш вопрос:

Вложение: Обзор... Файл не выбран.

Часто задаваемые вопросы — возможно на Ваш вопрос уже есть ответ!

Документация

Если ваш вопрос срочный — +7 (495) 789-45-86

Обновите Dr.Web CureNet!

Обновления выпускаются несколько раз в сутки и даже в час. Мы настоятельно рекомендуем перед очередной проверкой обновлять дистрибутив.

Обновить

Купите лицензию на CureNet!

через партнёров «Доктор Веб» или в нашем интернет-магазине.

Последнее обновление: 2019-06-10 05:52:45 UTC

Записей в вирусной в базе: 9781631

Попробуйте бесплатно

любой продукт Dr.Web в течение

Переходите на «зеленый»

При миграции с продукта другого

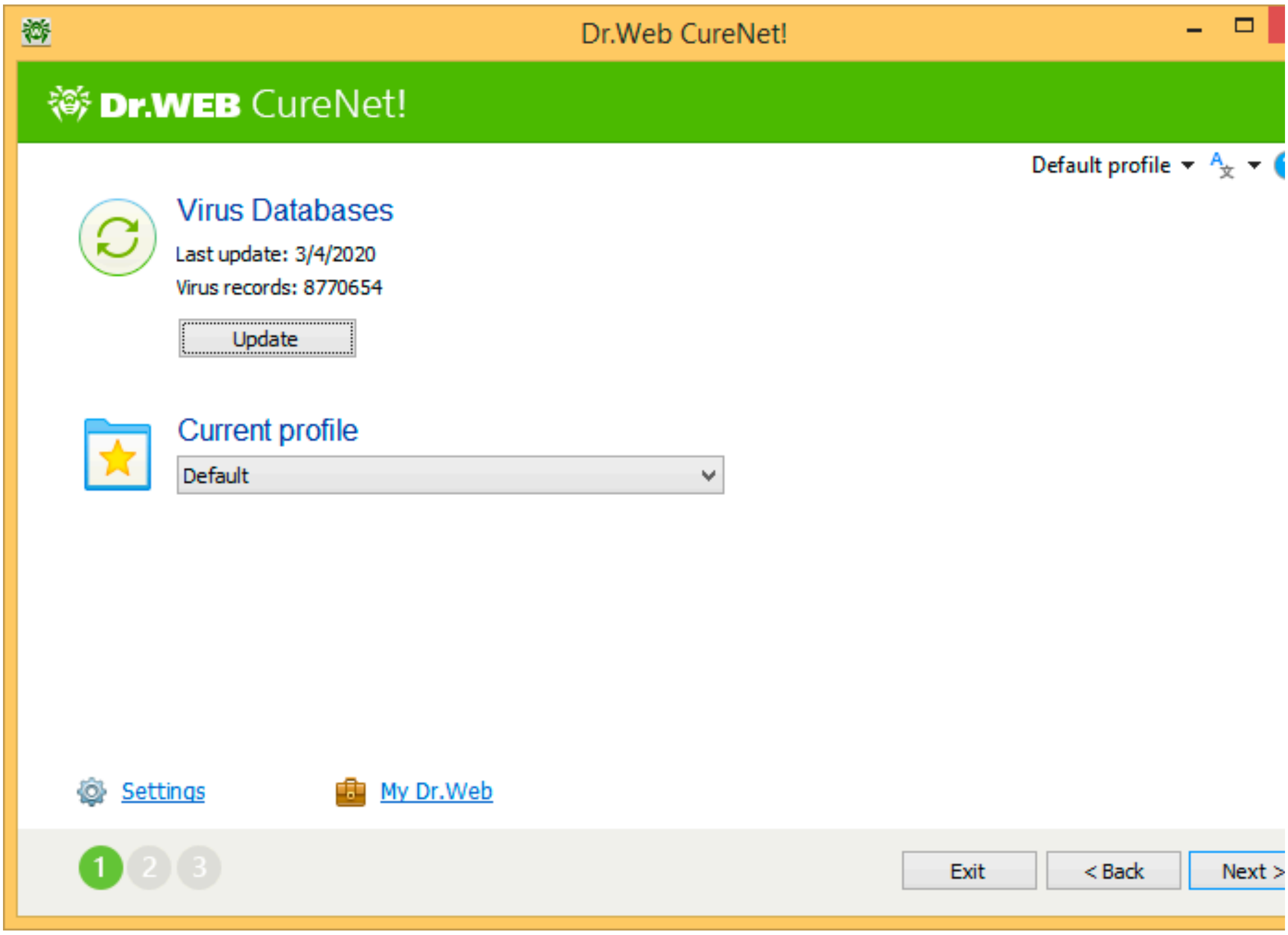
Аптечка сисадмина

Бесплатные утилиты от Dr.Web

Участвуйте в бета-тестированиях

Ваш вклад в качестве бета-тестера будет

Click on **Next** to continue.



Virus Databases

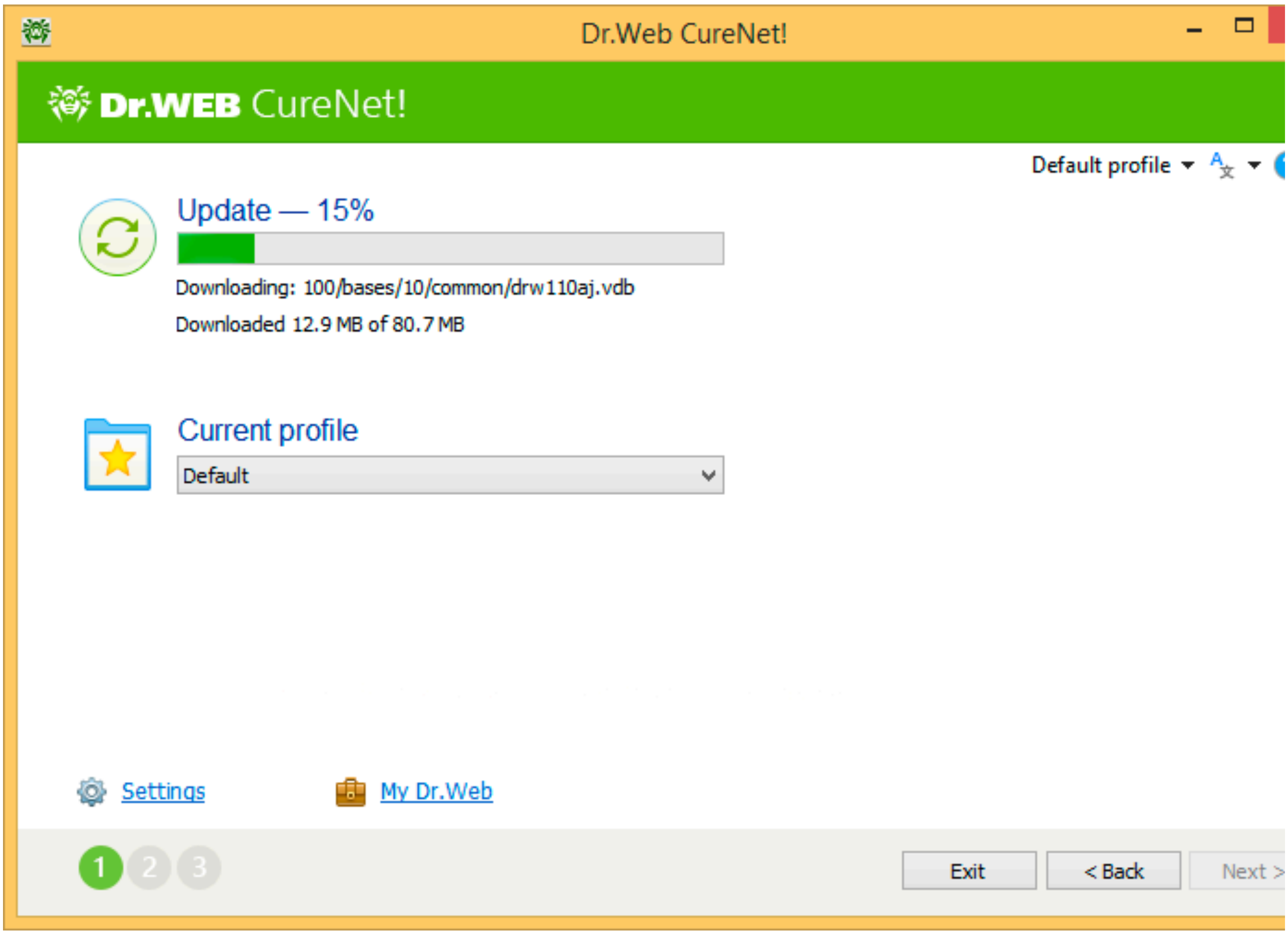
Last update: 3/4/2020

Virus records: 8770654

Current profile

Default

Click on the **Update** button to update the virus databases.



Update — 15%

Downloading: 100/bases/10/common/drw110aj.vdb

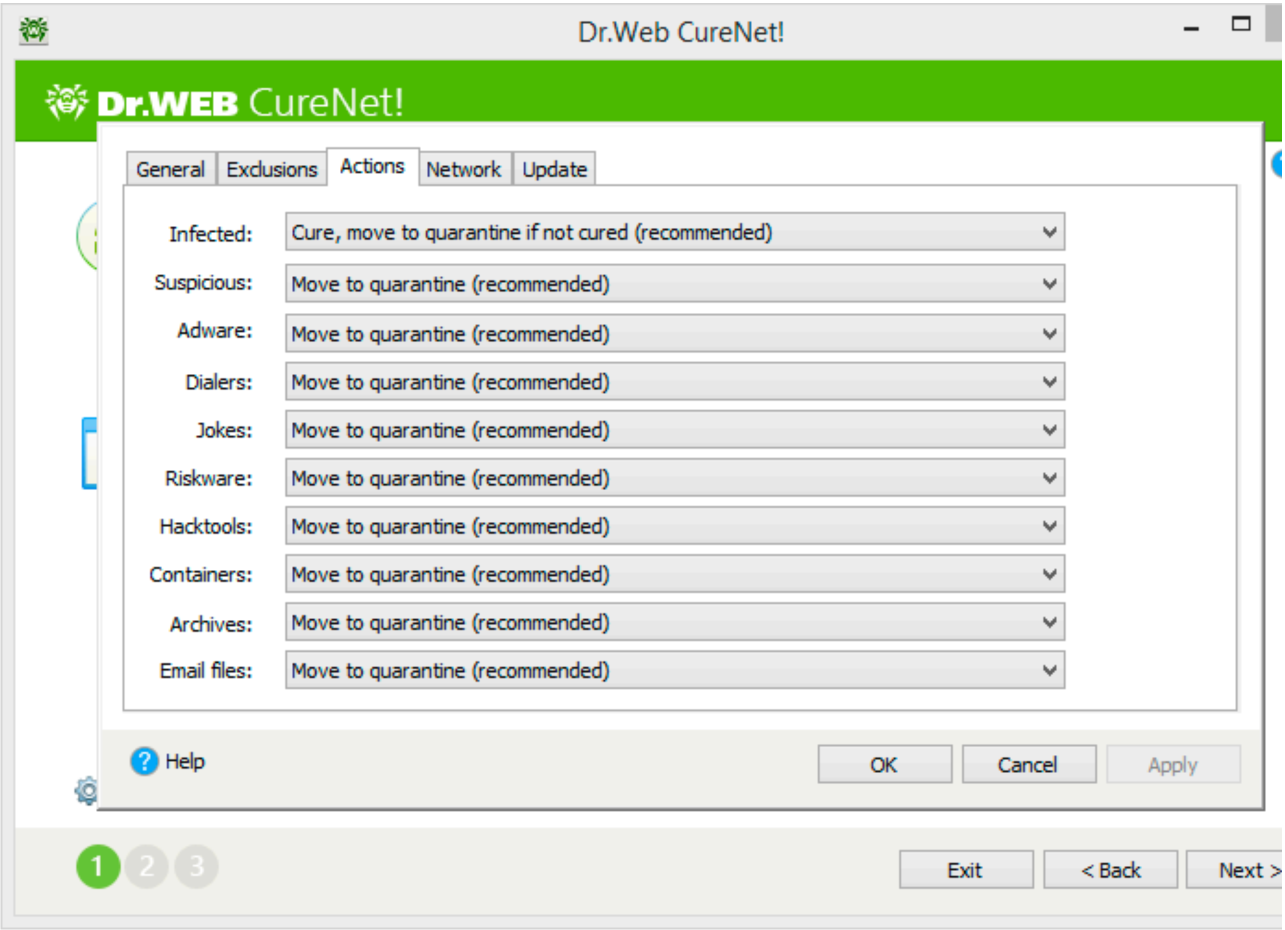
Downloaded 12.9 MB of 80.7 MB

Current profile

Default

Important! Success in detecting and neutralising viruses depends greatly on the virus definitions in the database. Therefore, it is strongly recommended that you update the databases whenever you launch Dr.Web CureNet!

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

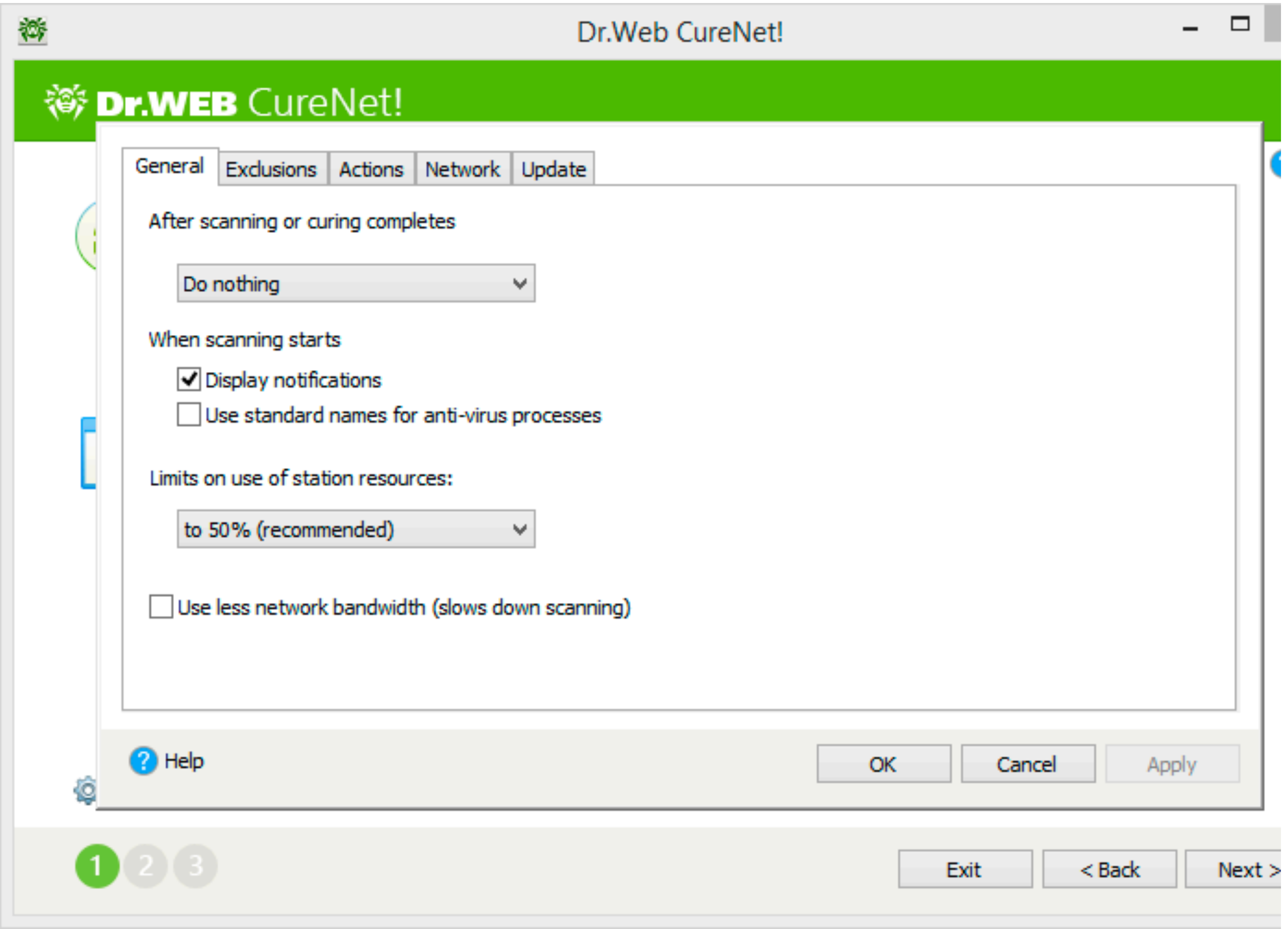


Infected:	Cure, move to quarantine if not cured (recommended)
Suspicious:	Move to quarantine (recommended)
Adware:	Move to quarantine (recommended)
Dialers:	Move to quarantine (recommended)
Jokes:	Move to quarantine (recommended)
Riskware:	Move to quarantine (recommended)
Hacktools:	Move to quarantine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

In the **Actions** tab, you can select the actions to be performed with different types of malicious objects. **Move** is set as the default action that is to be performed when most types of malicious objects are detected.

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

Important! A system restart is necessary to cure many viruses. However, the **Restart station** option (the **General** tab) is disabled by default since forced rebooting may interfere with the user experience. Therefore, if a virus is detected in your system, you should notify all users and scan all networked machines.



After scanning or curing completes

Do nothing

When scanning starts

☑ Display notifications

□ Use standard names for anti-virus processes

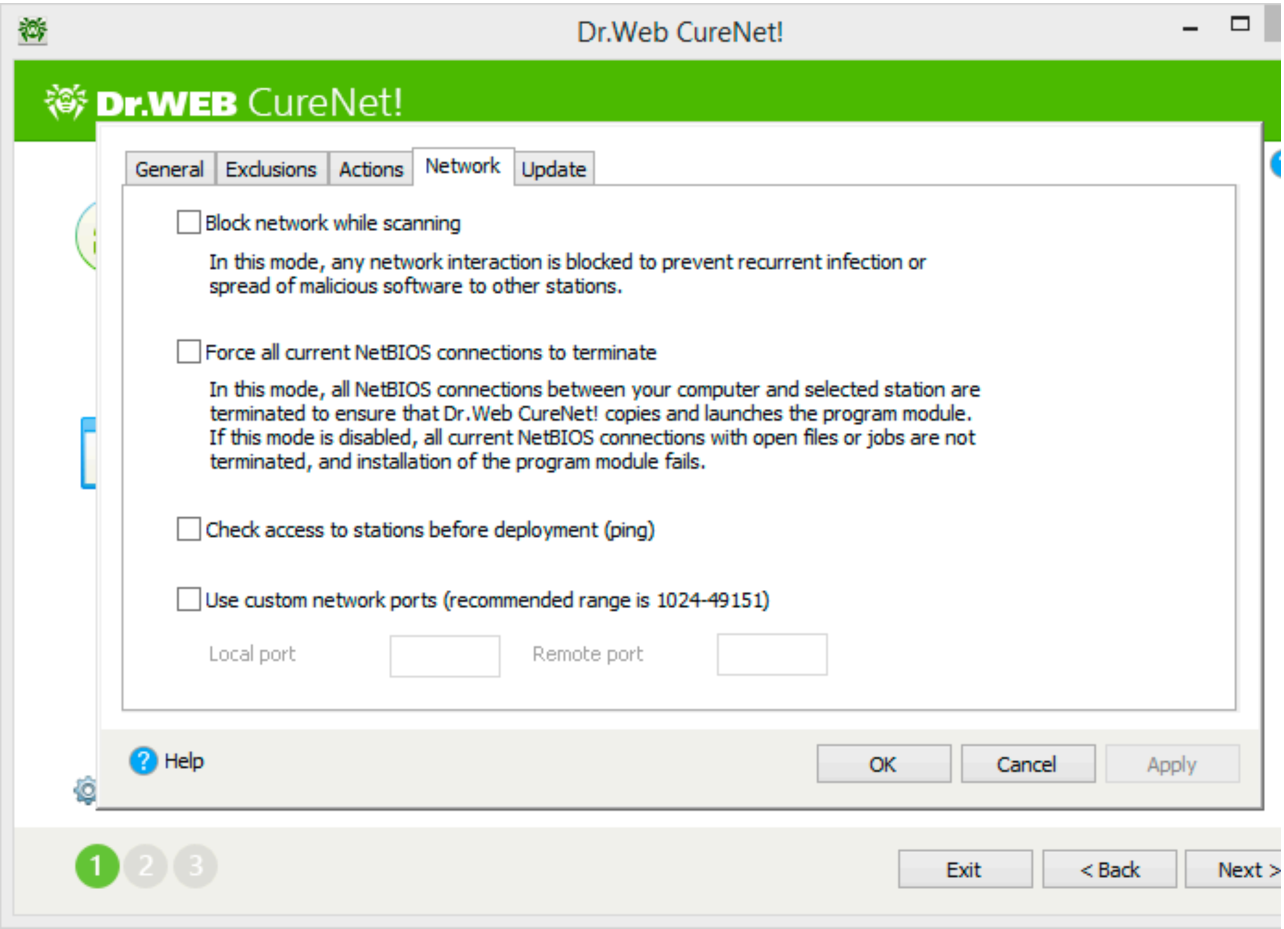
Limits on use of station resources:

to 50% (recommended)

□ Use less network bandwidth (slows down scanning)

By default, random names are generated for Dr.Web files when you copy them to a scanned station. If the station has an anti-virus with a firewall installed on it, the administrator may need to set exceptions for it during each scanning session. In such a situation, it is recommended that you enable **Use standard names for anti-virus processes** in order for Dr.Web files to be copied to the station under their own names. And, in this case, the administrator will only need to specify a firewall exception on the station that's being scanned once.

The scan parameters are selected in the **Network** tab.



□ 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.

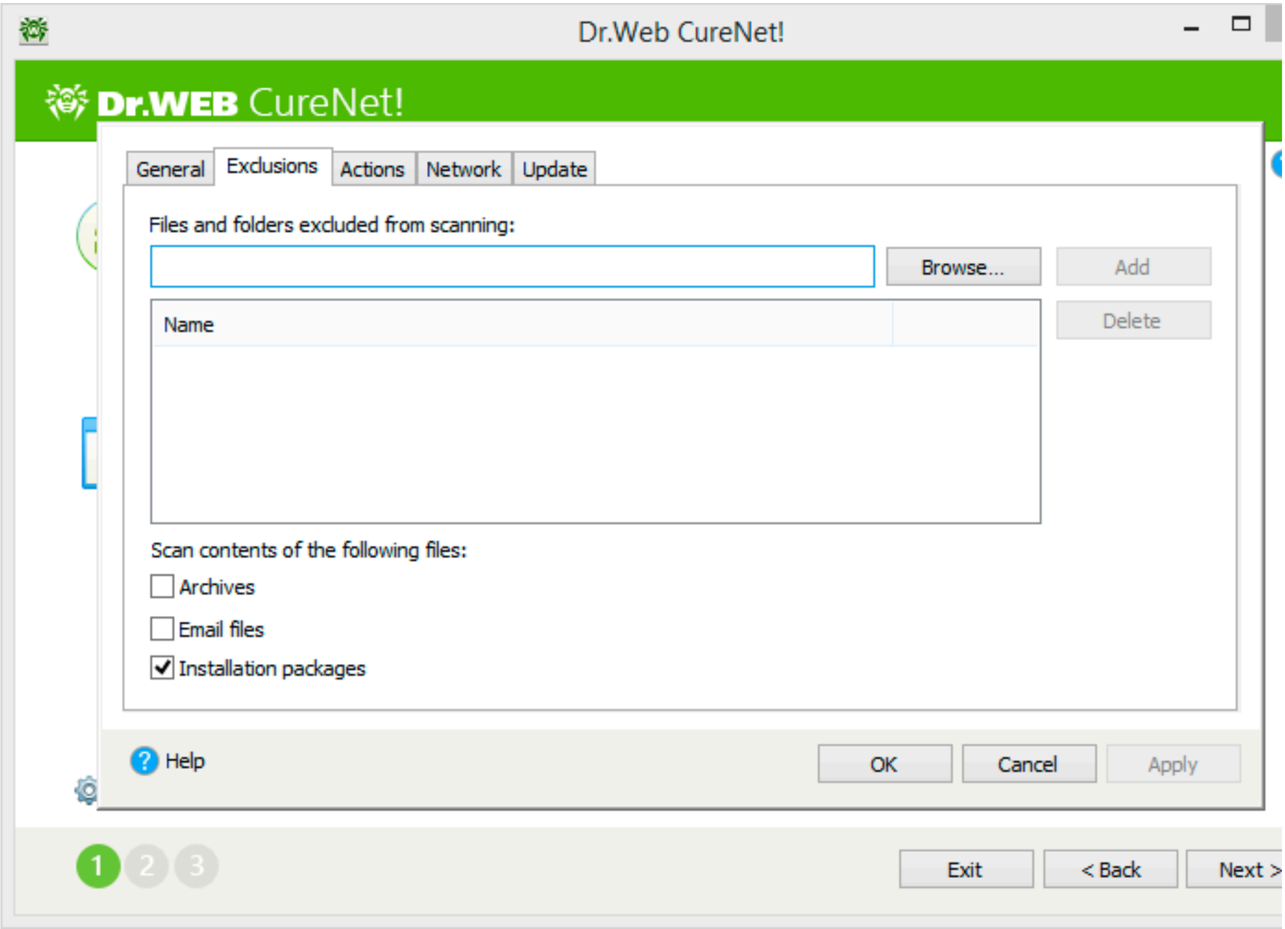
□ Check access to stations before deployment (ping)

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

Local port

Remote port

In the **Exclusions** tab, specify any files and folders that should be excluded from scanning and also indicate that packed and composite objects need to be scanned.

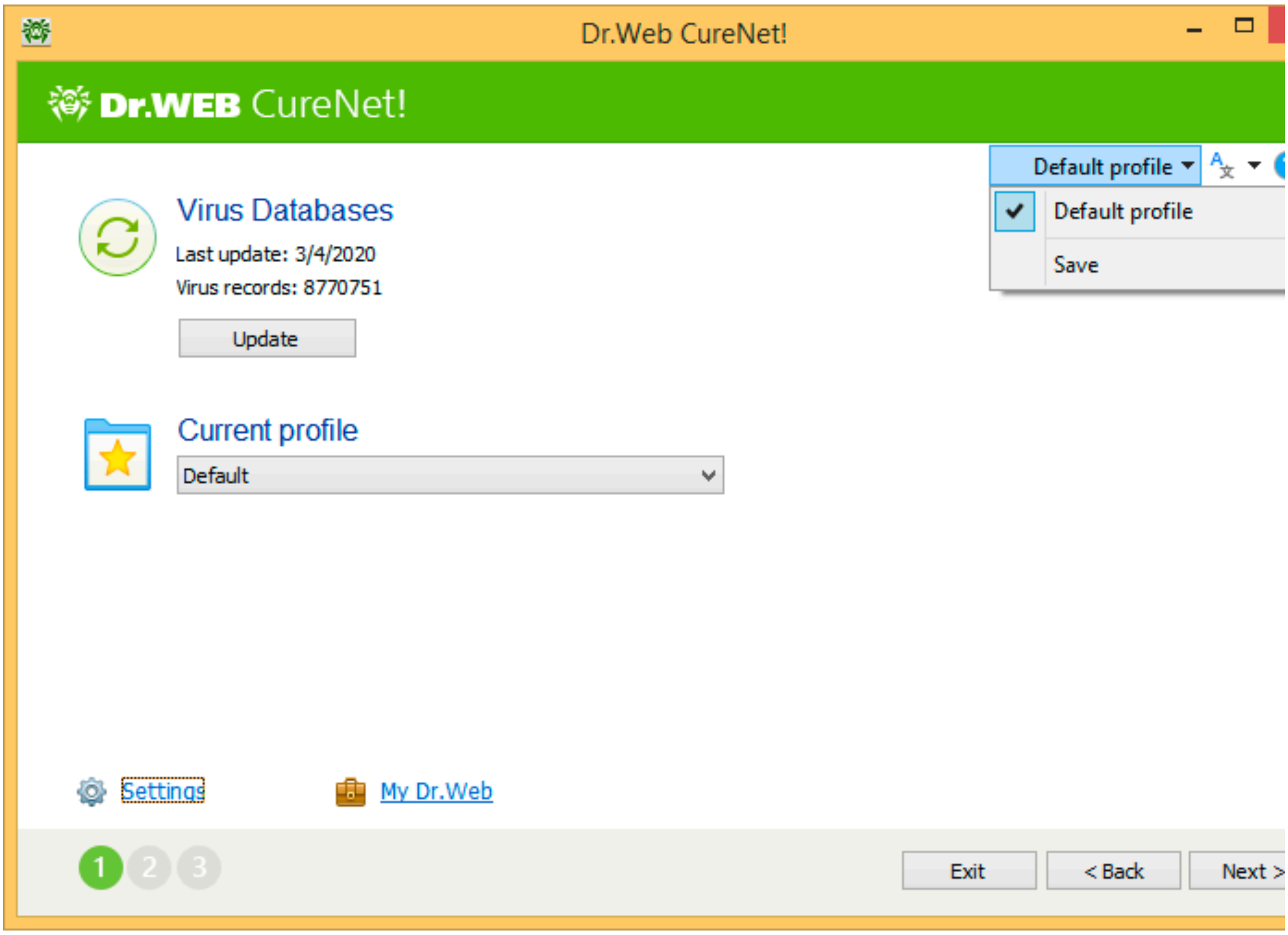


Files and folders excluded from scanning:

Scan contents of the following files:

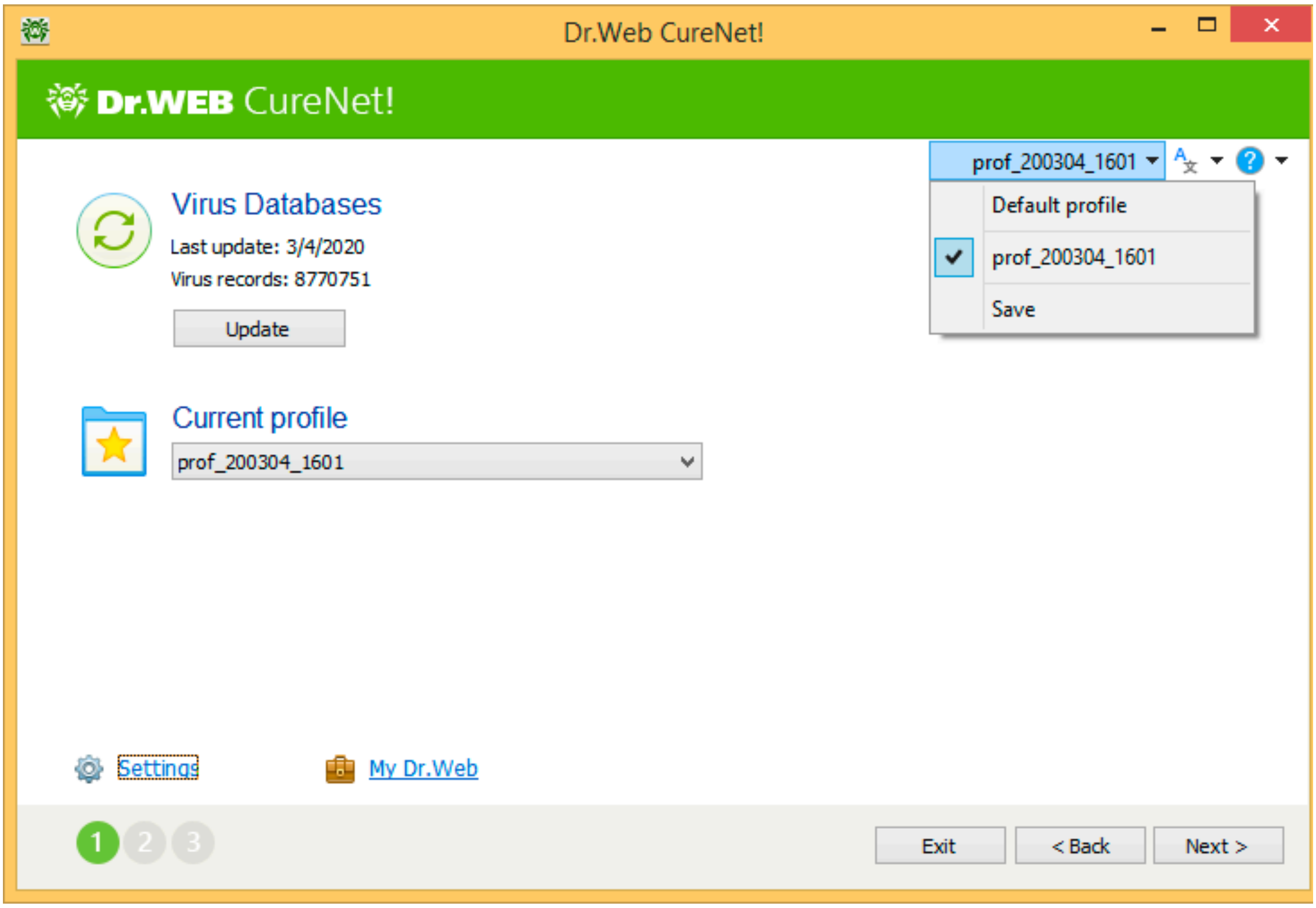
- ☐ Archives
- ☐ Email files
- ☑ Installation packages

To save the settings, select the **Default profile** and choose **Save** in the newly appeared menu.



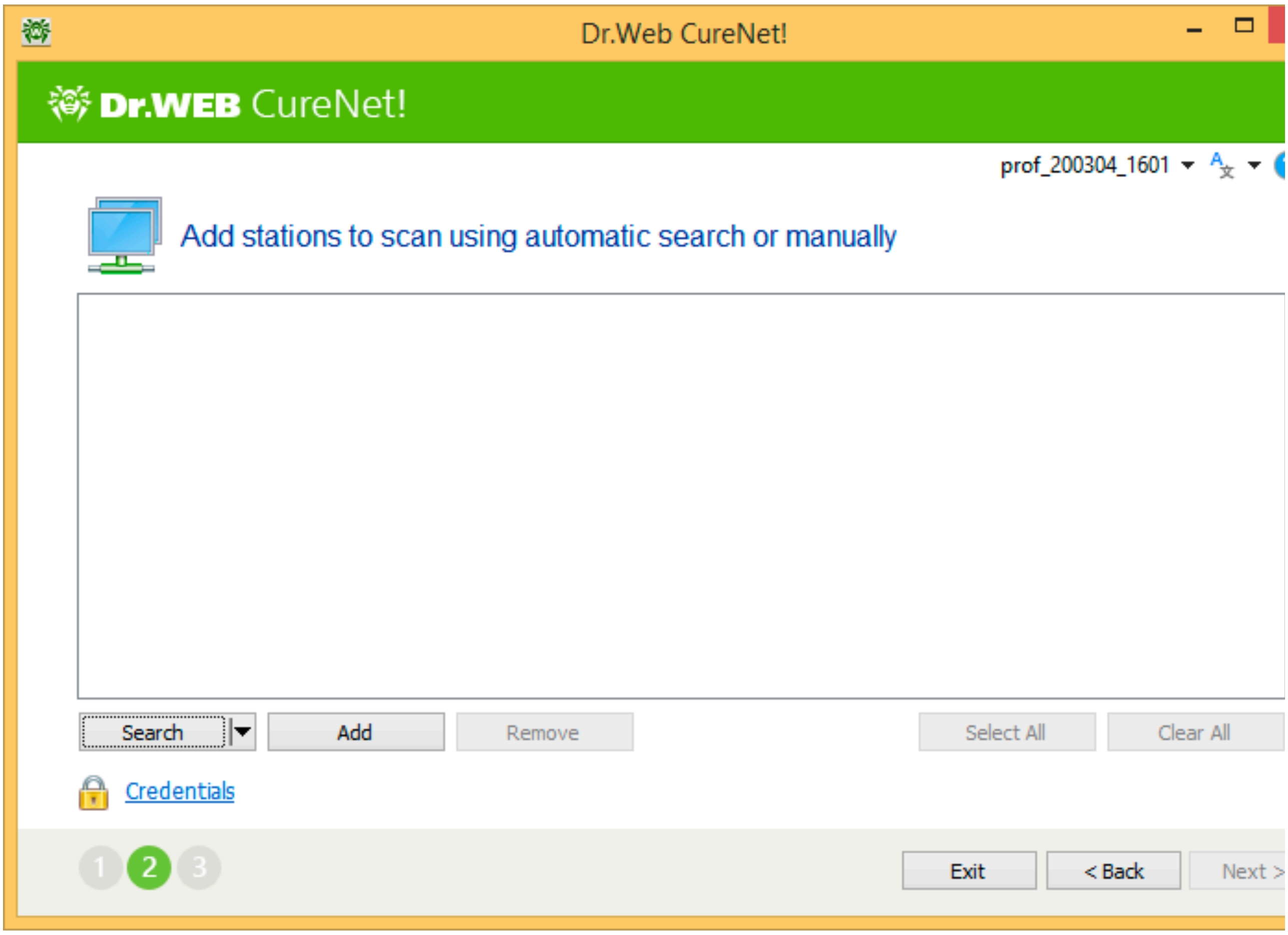
Important! It is recommended that you use the default settings since all Doctor Web products come with settings that ensure optimal performance.

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



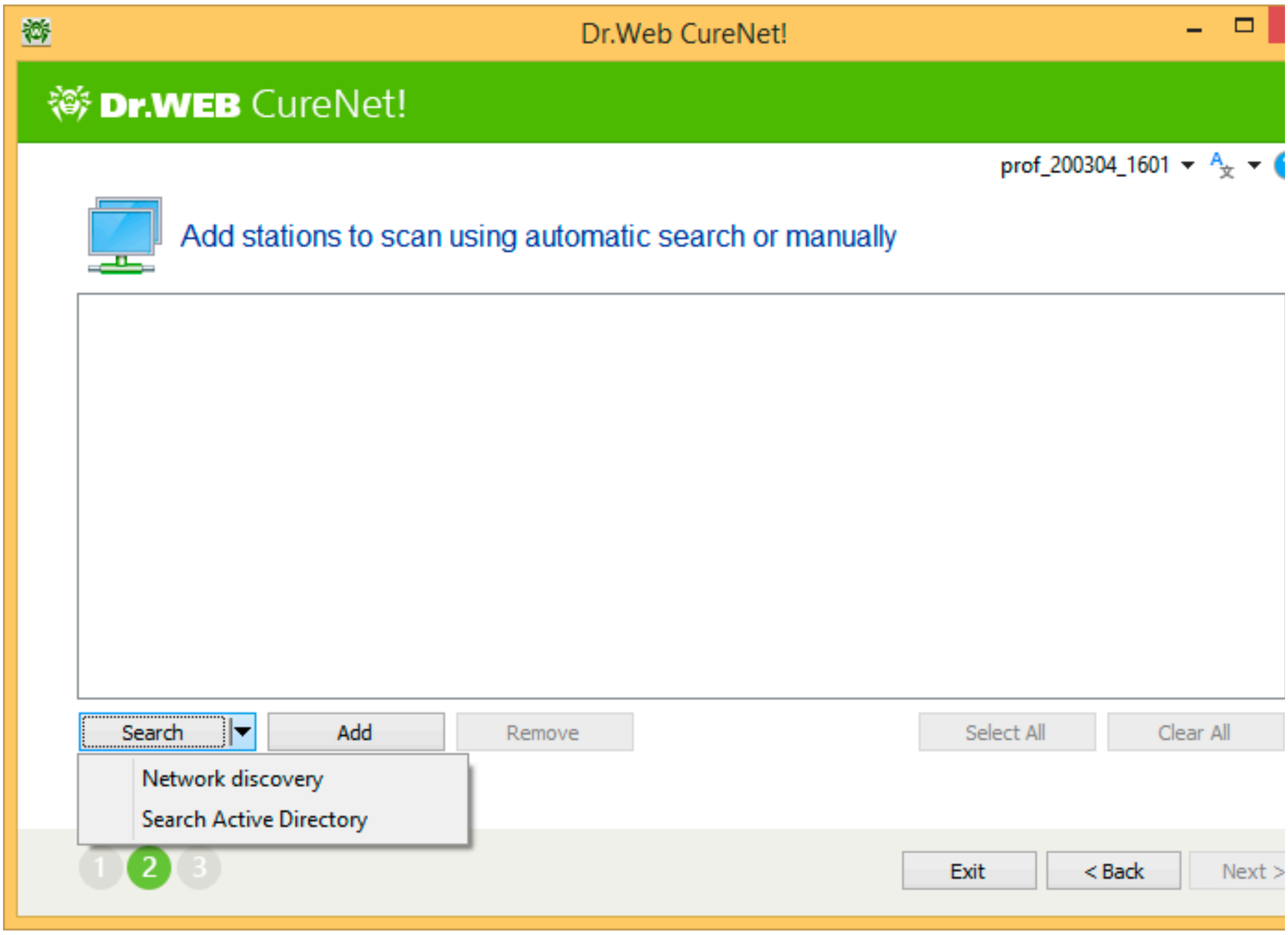
Select **Next** to continue.

5. In the newly opened window, you need to create a list of the networked computers that are to be scanned for viruses.



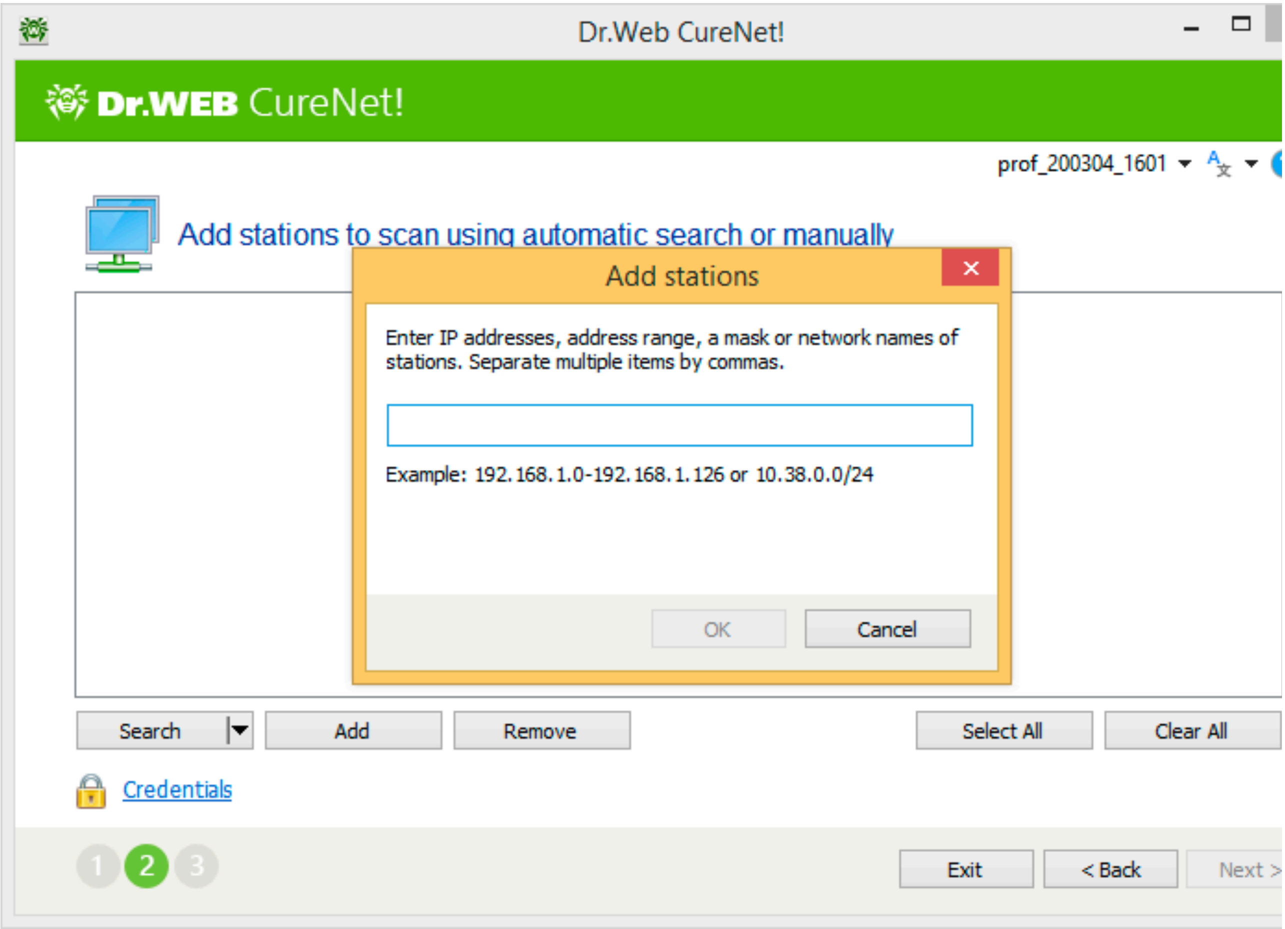
Add stations to scan using automatic search or manually

Click on **Search** to search for computers in the network.



If you select **Network discovery**, searching all the stations can take a long time. At any moment, you can click on **Stop search**. All the stations found up to this point will be added to the list. If, while searching, a station was not found, add it manually.

If you wish to create the list manually, click on the **Add** button and enter the address of an individual machine or a range of addresses to be searched for within the system.



Add stations to scan using automatic search or manually

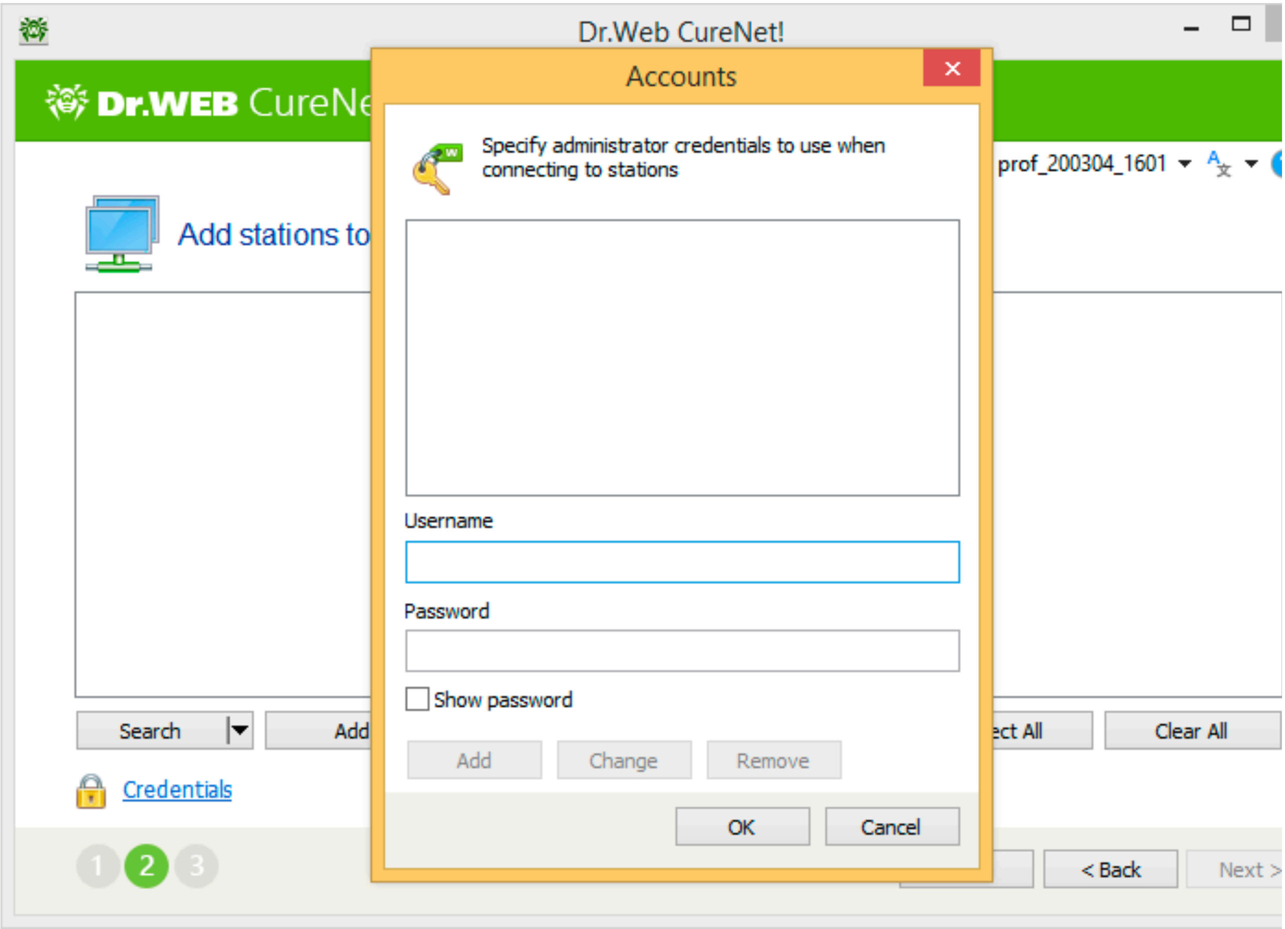
Enter IP addresses, address range, a mask or network names of stations. Separate multiple items by commas.

Example: 192.168.1.0-192.168.1.126 or 10.38.0.0/24

In the list, select the stations you need by checking the box next to its name or IP address in the list, or by clicking on **Select All**. Stations added to the list manually are automatically selected for further work with them.

If the network you are checking does not have a domain structure, click on **Credentials**, and in the newly opened window, enter the passwords used to access the respective target machines.

Once you have finished making your selections, create a list of the accounts under which Dr.Web will connect to these stations. By default, a connection is established using the privileges of the account under which the Wizard is running. If a connection cannot be established under this account, use the information specified in the list.

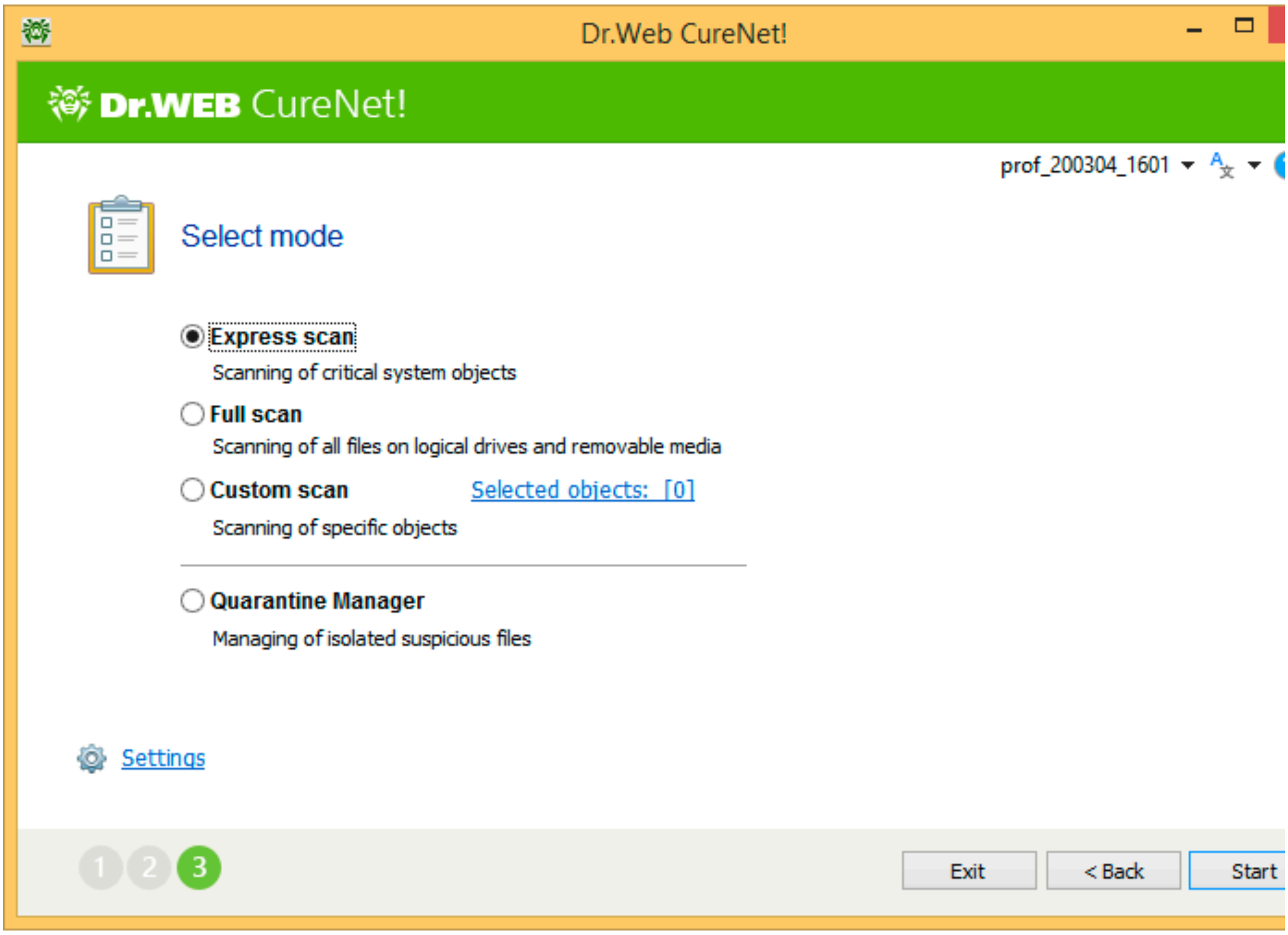


Specify administrator credentials to use when connecting to stations

Click on **Next** to continue.

6. In the newly opened window, choose the scan type: **Express**, **Full** or **Custom**.

Important! Choosing the Express scan will instruct the anti-virus to scan only system directories and running processes, which does not guarantee that your computer will be fully cured if an infection is detected. For example, some viruses running in a system can infect clean files that have already been scanned.



Select mode

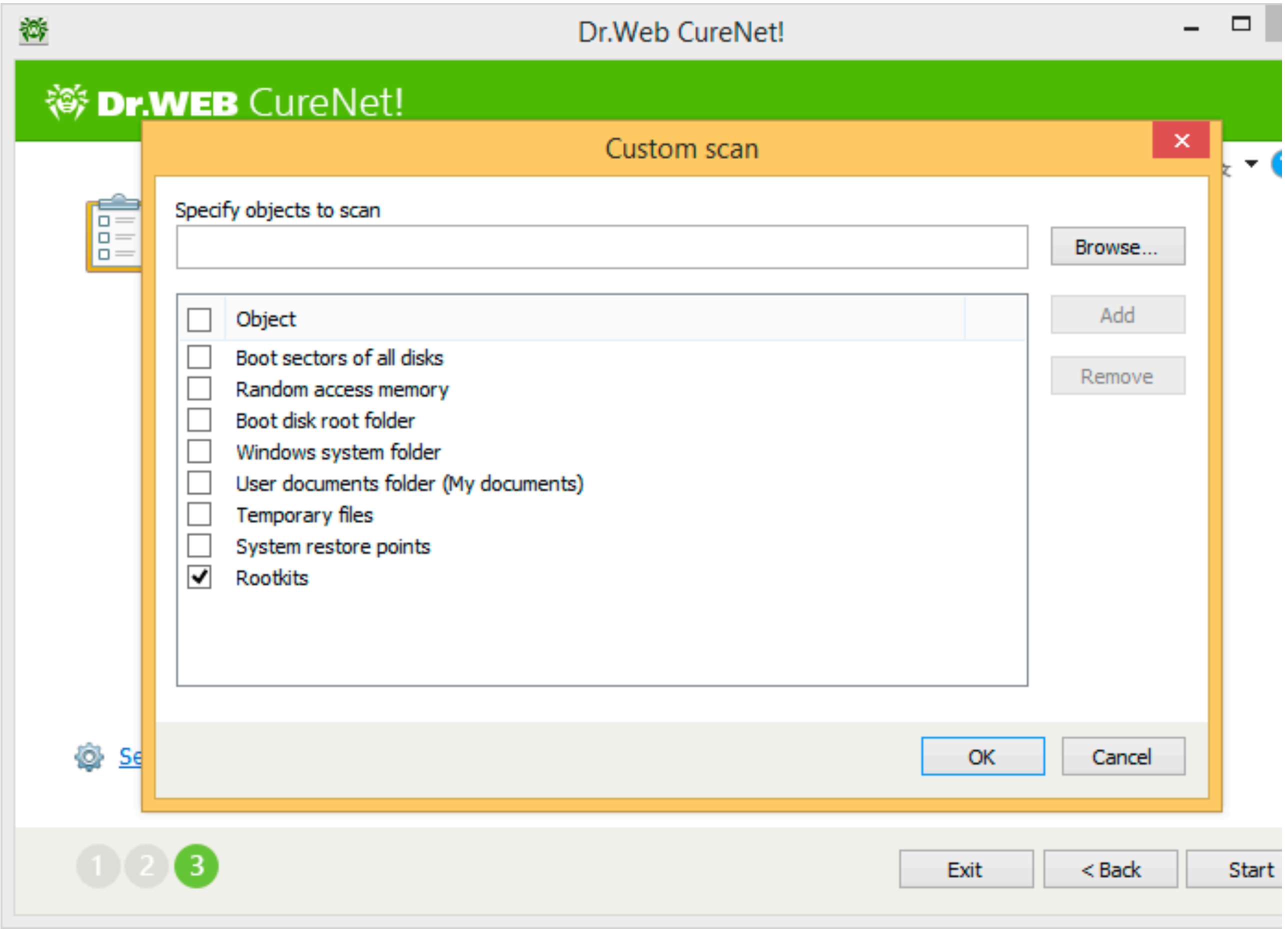
● Express scan
Scanning of critical system objects

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

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

○ Quarantine Manager
Managing of isolated suspicious files

If you choose **Custom scan**, specify the list of objects to be scanned.

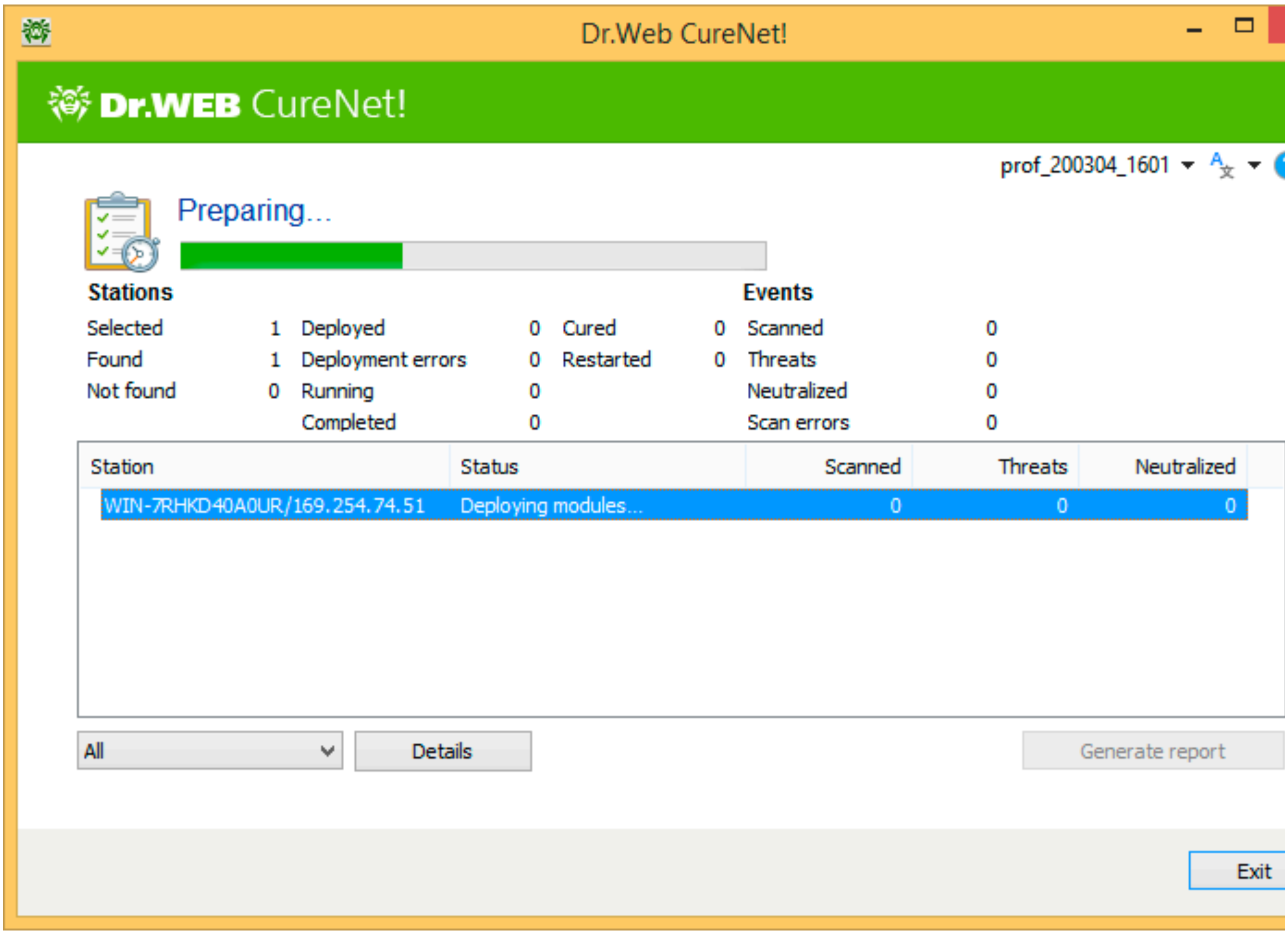


Custom scan

Specify objects to scan

□ Object
□ Boot sectors of all disks
□ Random access memory
□ Boot disk root folder
□ Windows system folder
□ User documents folder (My documents)
□ Temporary files
□ System restore points
☑ Rootkits

Click on the **Start** button to continue.



Stations

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

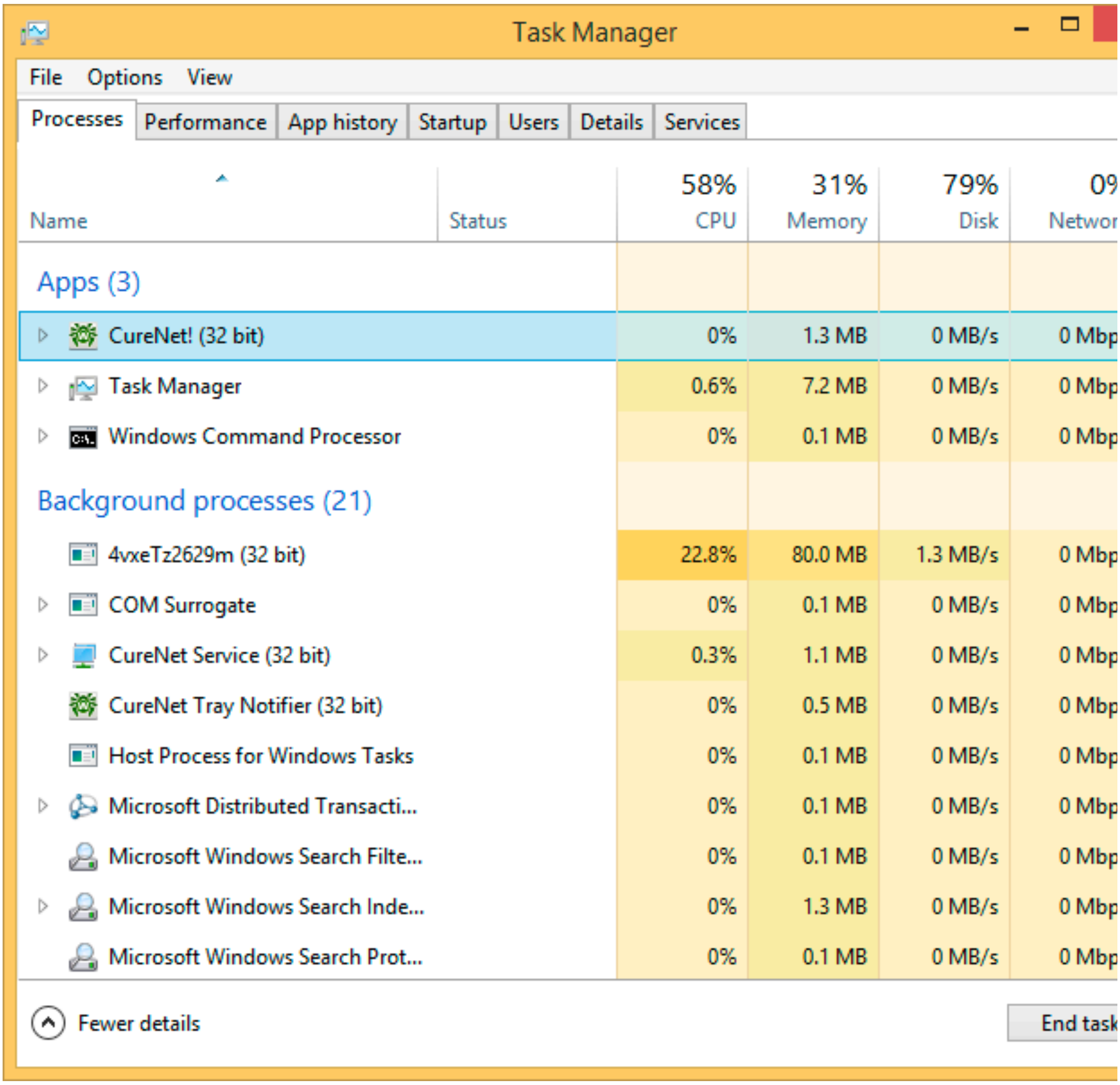
Events

Station	Status	Scanned	Threats	Neutralized
WIN-7RHKD40A0UR/169.254.74.51	Deploying modules...	0	0	0

This window displays the scanning progress taking place on the remote computers and the scan results. The statistics that are provided do not depend on the quality of the connection between the computers. Even if the connection is interrupted, Dr.Web CureNet! will update the statistics once the connection is re-established.

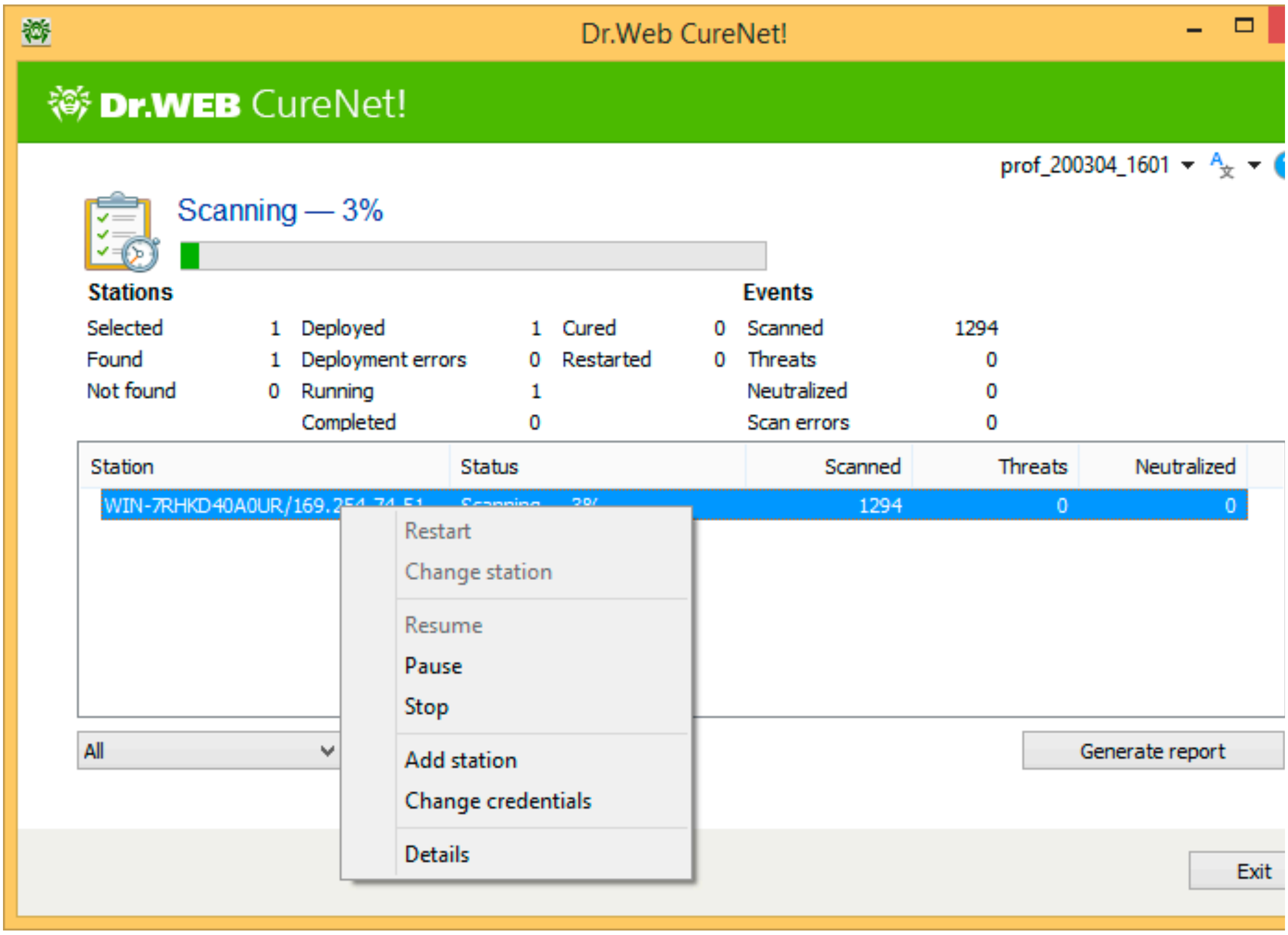
Important! It is not recommended to stop scanning prematurely.

The running processes involved in the scanning utilise self-defence mechanisms that protect them against malware.


Task Manager
File Options View
Processes Performance App history Startup Users Details Services
Fewer details
End task

Name	Status	58% CPU	31% Memory	79% Disk	0 Networ
Apps (3)					
CureNet! (32 bit)		0%	1.3 MB	0 MB/s	0 Mbp
Task Manager		0.6%	7.2 MB	0 MB/s	0 Mbp
Windows Command Processor		0%	0.1 MB	0 MB/s	0 Mbp
Background processes (21)					
4vxeTz2629m (32 bit)		22.8%	80.0 MB	1.3 MB/s	0 Mbp
COM Surrogate		0%	0.1 MB	0 MB/s	0 Mbp
CureNet Service (32 bit)		0.3%	1.1 MB	0 MB/s	0 Mbp
CureNet Tray Notifier (32 bit)		0%	0.5 MB	0 MB/s	0 Mbp
Host Process for Windows Tasks		0%	0.1 MB	0 MB/s	0 Mbp
Microsoft Distributed Transacti...		0%	0.1 MB	0 MB/s	0 Mbp
Microsoft Windows Search Filte...		0%	0.1 MB	0 MB/s	0 Mbp
Microsoft Windows Search Inde...		0%	1.3 MB	0 MB/s	0 Mbp
Microsoft Windows Search Prot...		0%	0.1 MB	0 MB/s	0 Mbp

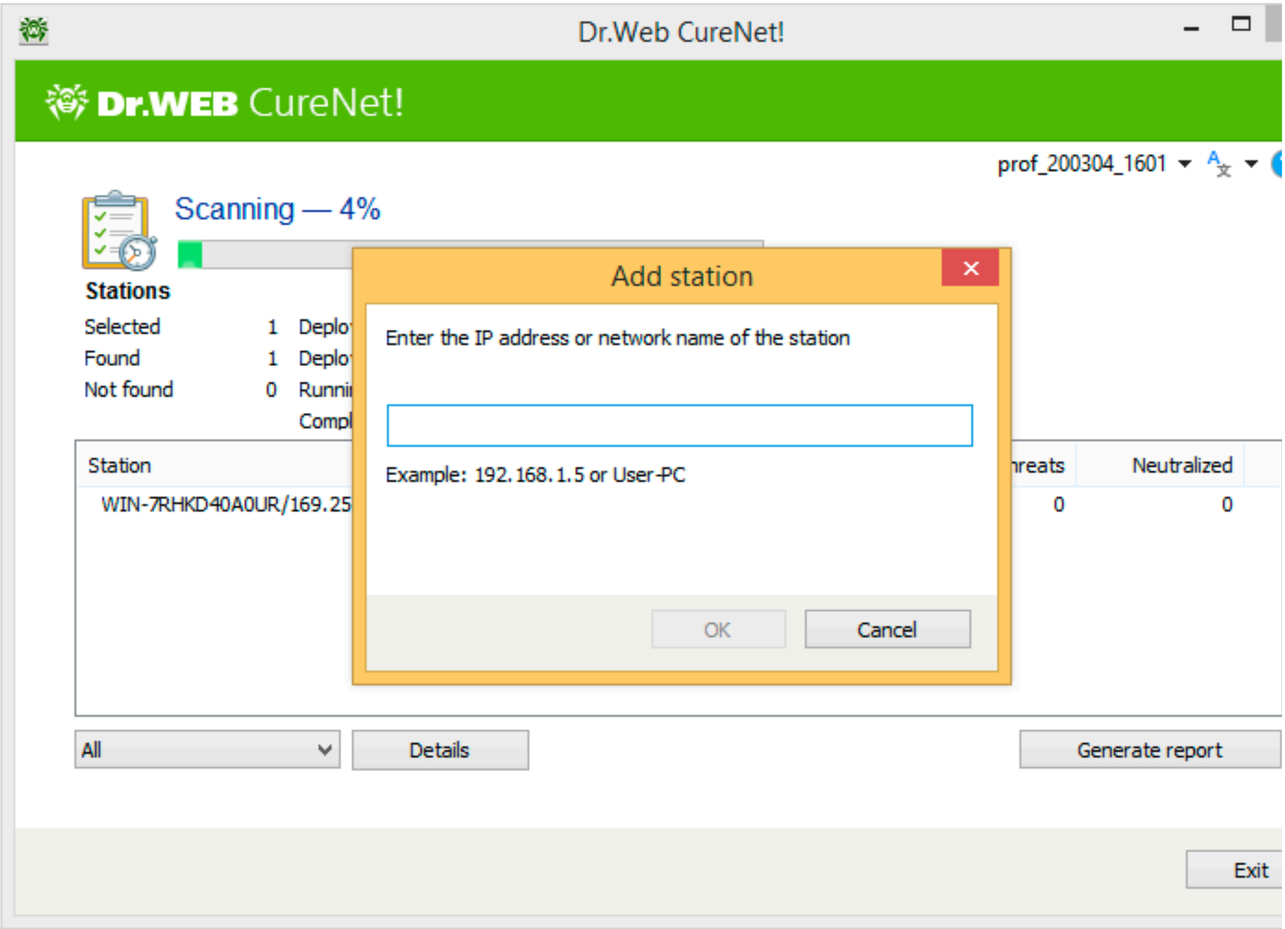
Using the context menu, you can stop or continue the scanning process, add a station in real time or change credentials.



Scanning — 3%

Stations						Events	
Selected	1	Deployed	1	Cured	0	Scanned	1294
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
WIN-7RHKD40A0UR/169.254.74.51	Scanning — 3%	1294	0	0



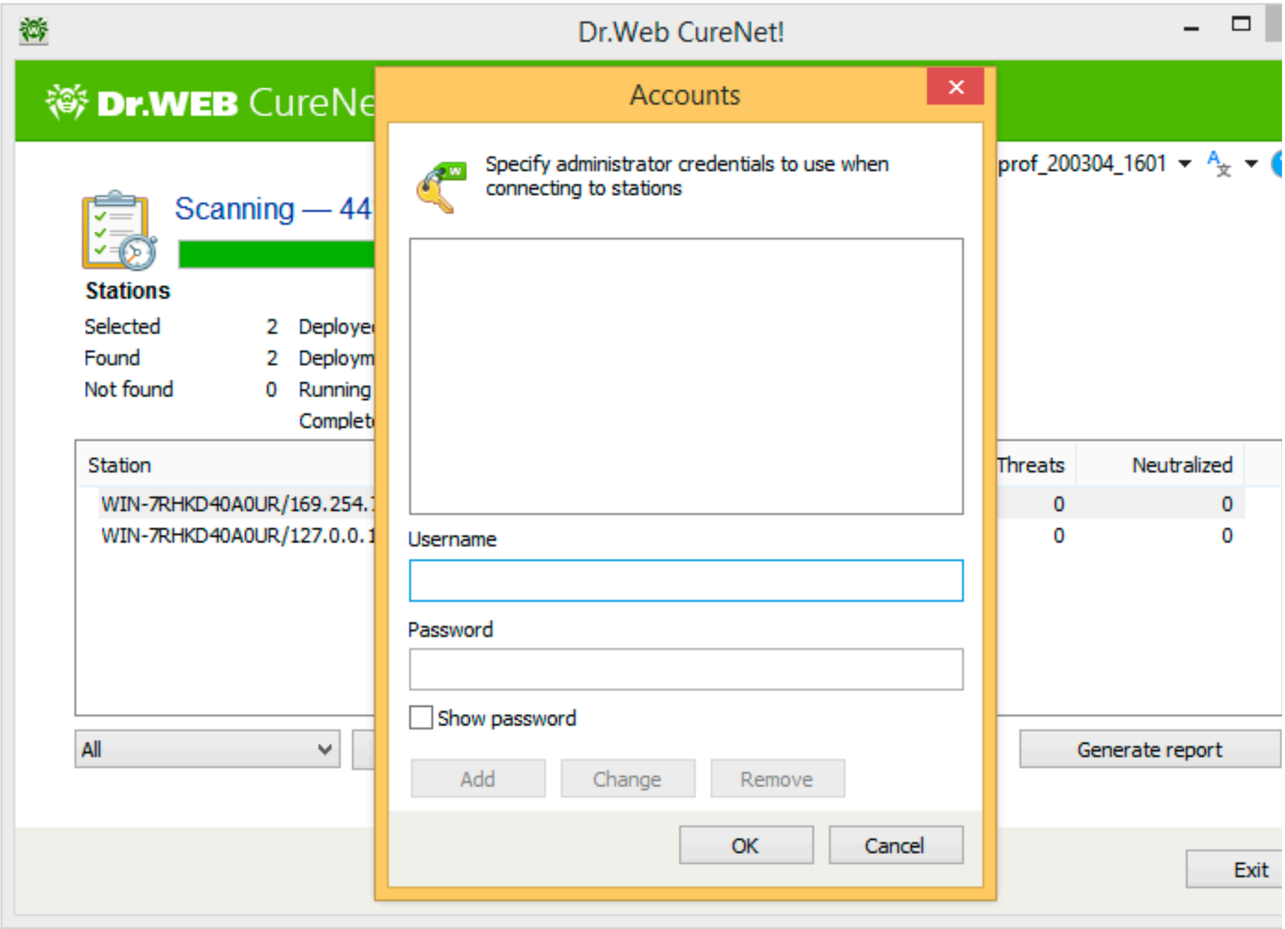
Scanning — 4%

Stations			
Selected	1	Deplo	
Found	1	Deplo	
Not found	0	Runni	
		Compl	

Station		hreats	Neutralized
WIN-7RHKD40A0UR/169.25		0	0

Enter the IP address or network name of the station

Example: 192.168.1.5 or User-PC



Specify administrator credentials to use when connecting to stations

Selected	2	Deploye	
Found	2	Deploym	
Not found	0	Running	
		Complet	

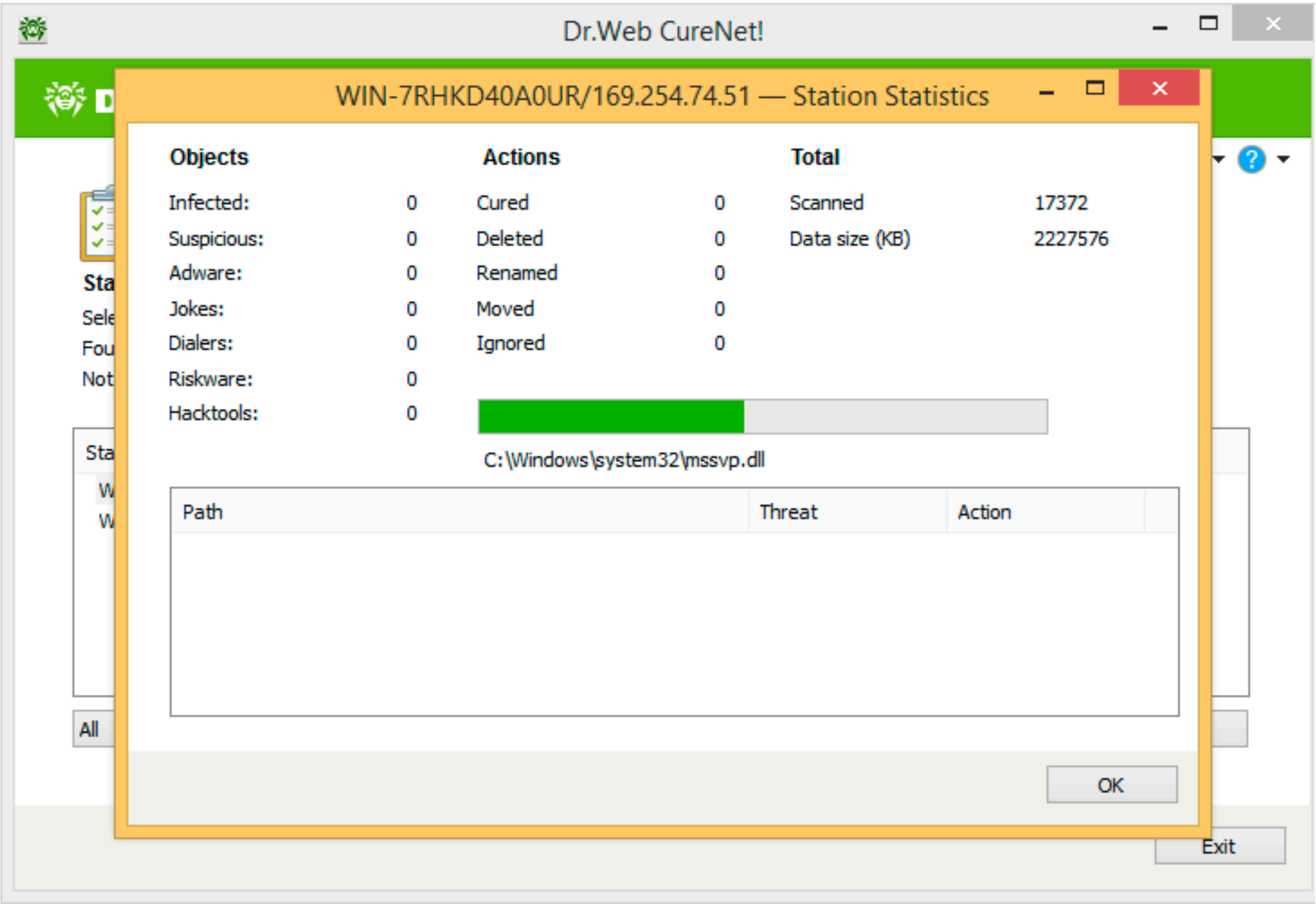
Station	Threats	Neutralized
WIN-7RHKD40A0UR/169.254.1	0	0
WIN-7RHKD40A0UR/127.0.0.1	0	0

Important!

- Actions cannot be executed immediately for some infected or suspicious objects (e.g., registry keys and files used by other Windows applications). When detected, such files are marked as to be processed (depending on the action specified) after a station restart. For the correct processing of these objects, you can allow the operating systems of the scanned stations to be restarted if needed or turn them off automatically after scanning is complete. The user will be prompted with a warning and have time to complete their current work and save their information.
- When viruses are detected in the Master Boot Record (MBR), Dr.Web Scanner forces a reboot of the station immediately after a virus is discovered and the boot record (hard reboot) is restored. The system will be restarted regardless of whether or not the **Restart station** option is enabled.

The station scanning process does not depend on whether or not the Wizard is launched. To exit the Wizard, click on **Cancel**. When you do that, the scanning process does not stop, but statistics are no longer available.

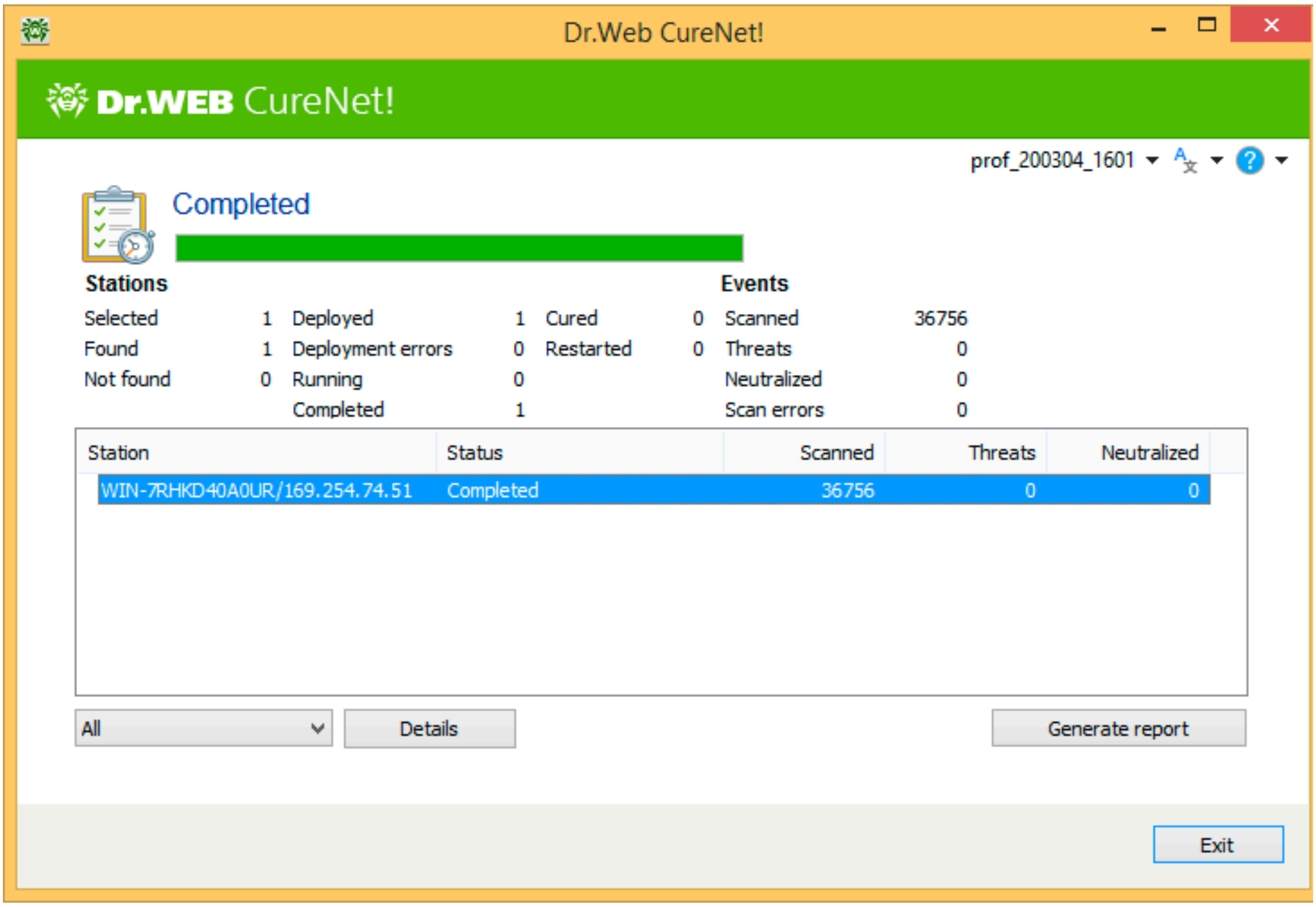
By clicking on **Details**, you will see detailed statistics.



Objects		Actions		Total	
Infected:	0	Cured	0	Scanned	17372
Suspicious:	0	Deleted	0	Data size (KB)	2227576
Adware:	0	Renamed	0		
Jokes:	0	Moved	0		
Dialers:	0	Ignored	0		
Riskware:	0				
Hacktools:	0				

C:\Windows\system32\mssvp.dll

Path	Threat	Action

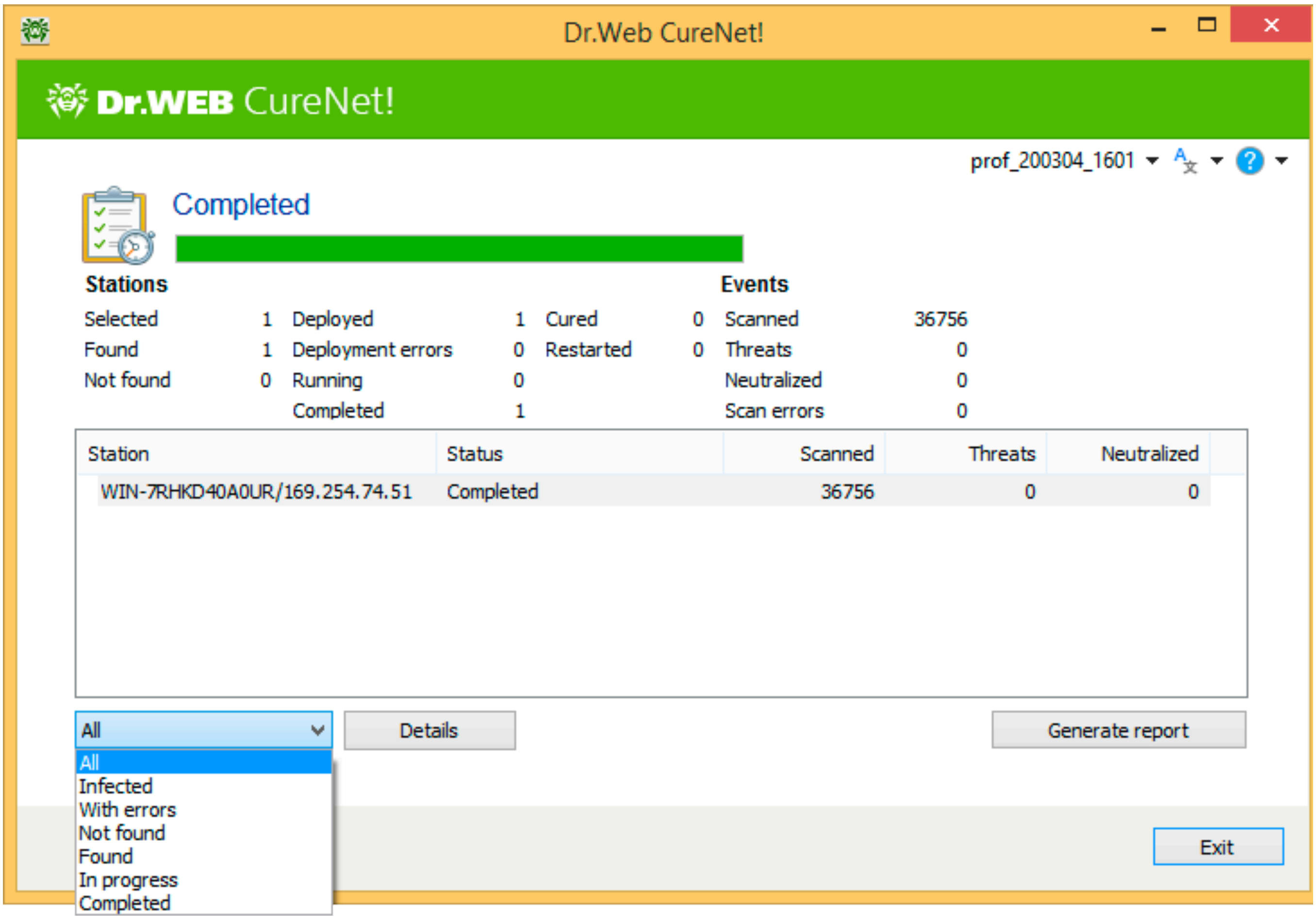


Completed

Stations						Events	
Selected	1	Deployed	1	Cured	0	Scanned	36756
Found	1	Deployment errors	0	Restarted	0	Threats	0
Not found	0	Running	0			Neutralized	0
		Completed	1			Scan errors	0

Station	Status	Scanned	Threats	Neutralized
WIN-7RHKD40A0UR/169.254.74.51	Completed	36756	0	0

After clicking on the drop-down menu, you can select the display mode.



Stations

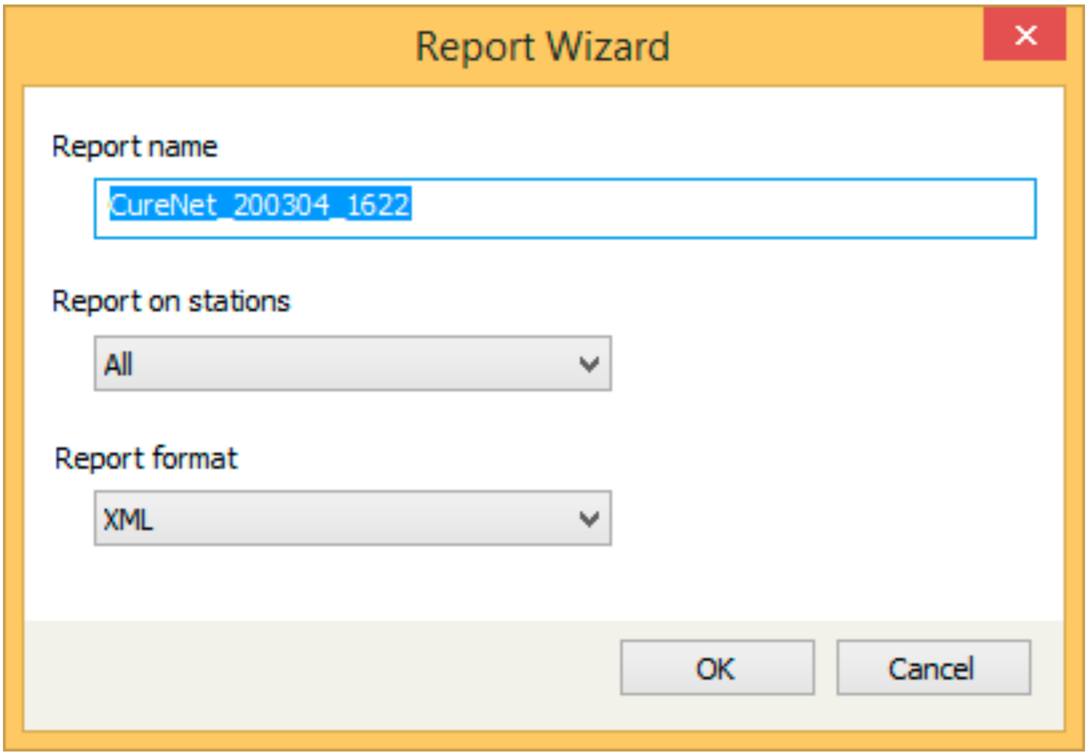
Selected	1	Deployed	1	Cured	0
Found	1	Deployment errors	0	Restarted	0
Not found	0	Running	0		
		Completed	1		

Events

Scanned	36756
Threats	0
Neutralized	0
Scan errors	0

Station	Status	Scanned	Threats	Neutralized
WIN-7RHKD40A0UR/169.254.74.51	Completed	36756	0	0

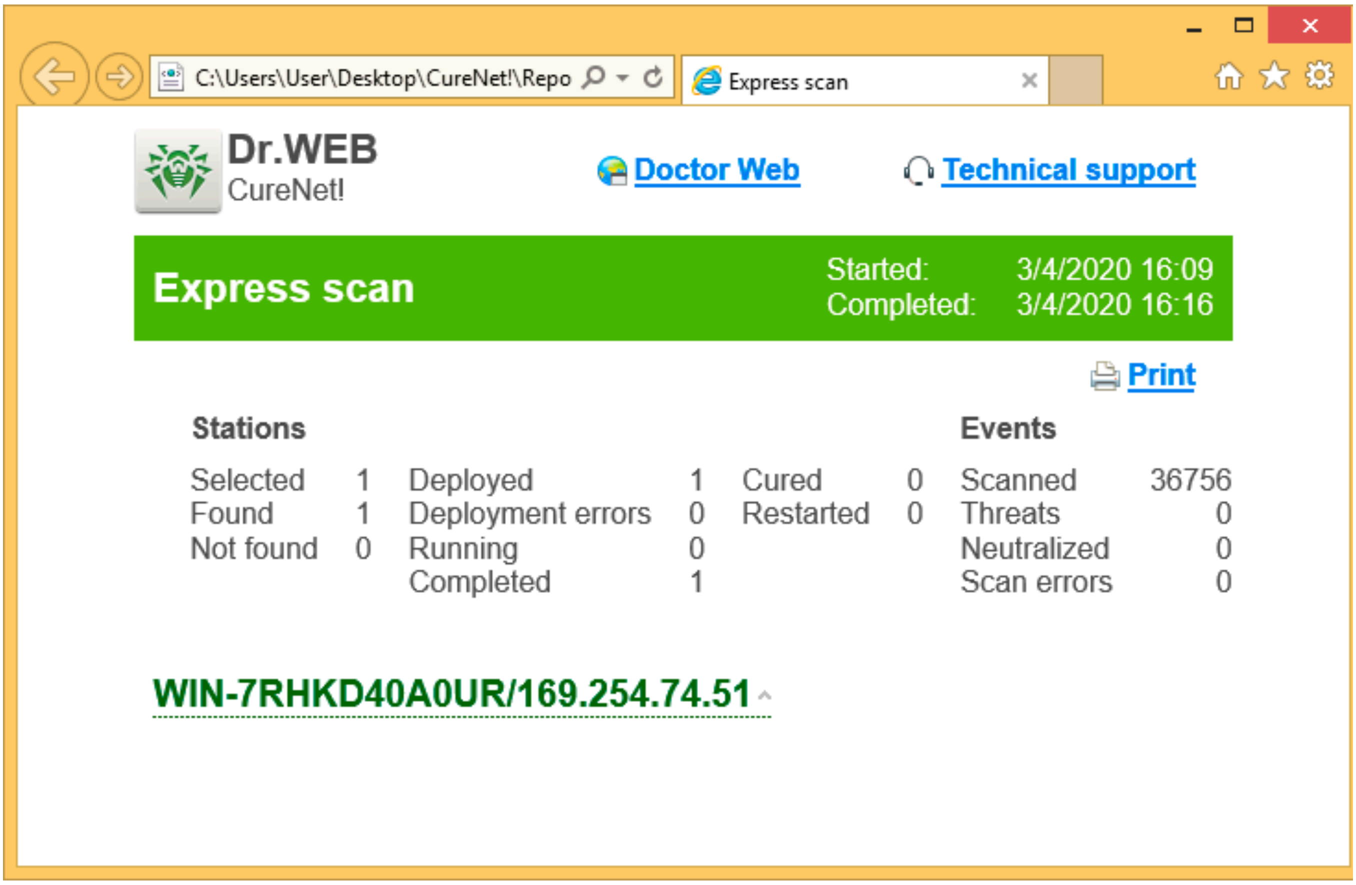
Click on the **Generate report** button to create a network scanning report.



Report name: CureNet_200304_1622

Report on stations: All

Report format: XML



Express scan

Started: 3/4/2020 16:09
Completed: 3/4/2020 16:16

Stations						Events	
Selected	1	Deployed	1	Cured	0	Scanned	36756
Found	1	Deployment errors	0	Restarted	0	Threats	0
Not found	0	Running	0			Neutralized	0
		Completed	1			Scan errors	0

WIN-7RHKD40A0UR/169.254.74.51

Click on **Exit** to close the program.

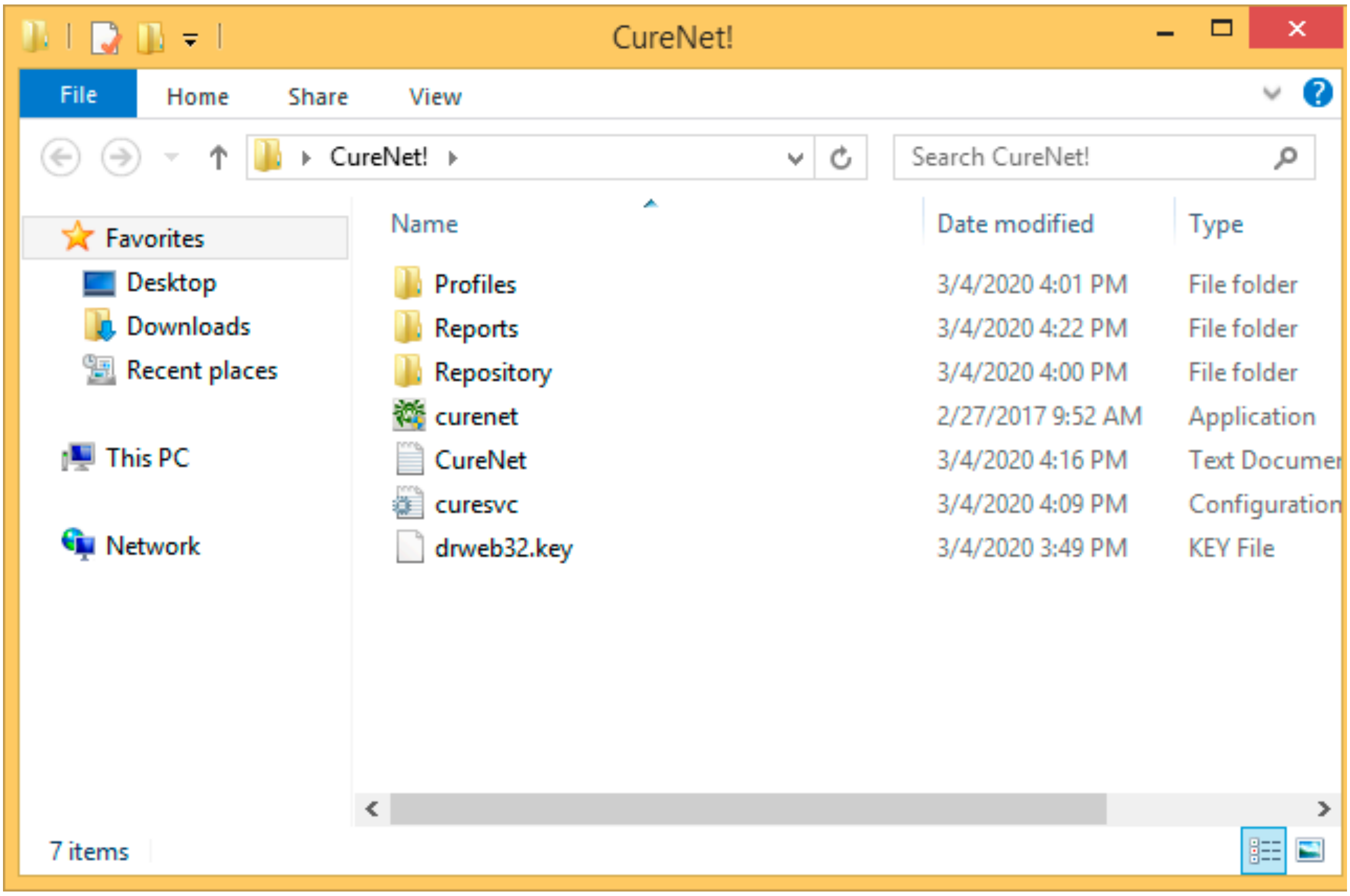
For detailed information about the product, its configuration, scanning, and the use of profiles, refer to the Dr.Web CureNet! administrator manual

Using Dr.Web CureNet!

It is recommended that you perform regular anti-virus scans of your system. In particular, files on the disks scanned by the file monitor may contain viruses that were not known to the anti-virus when it scanned the files.

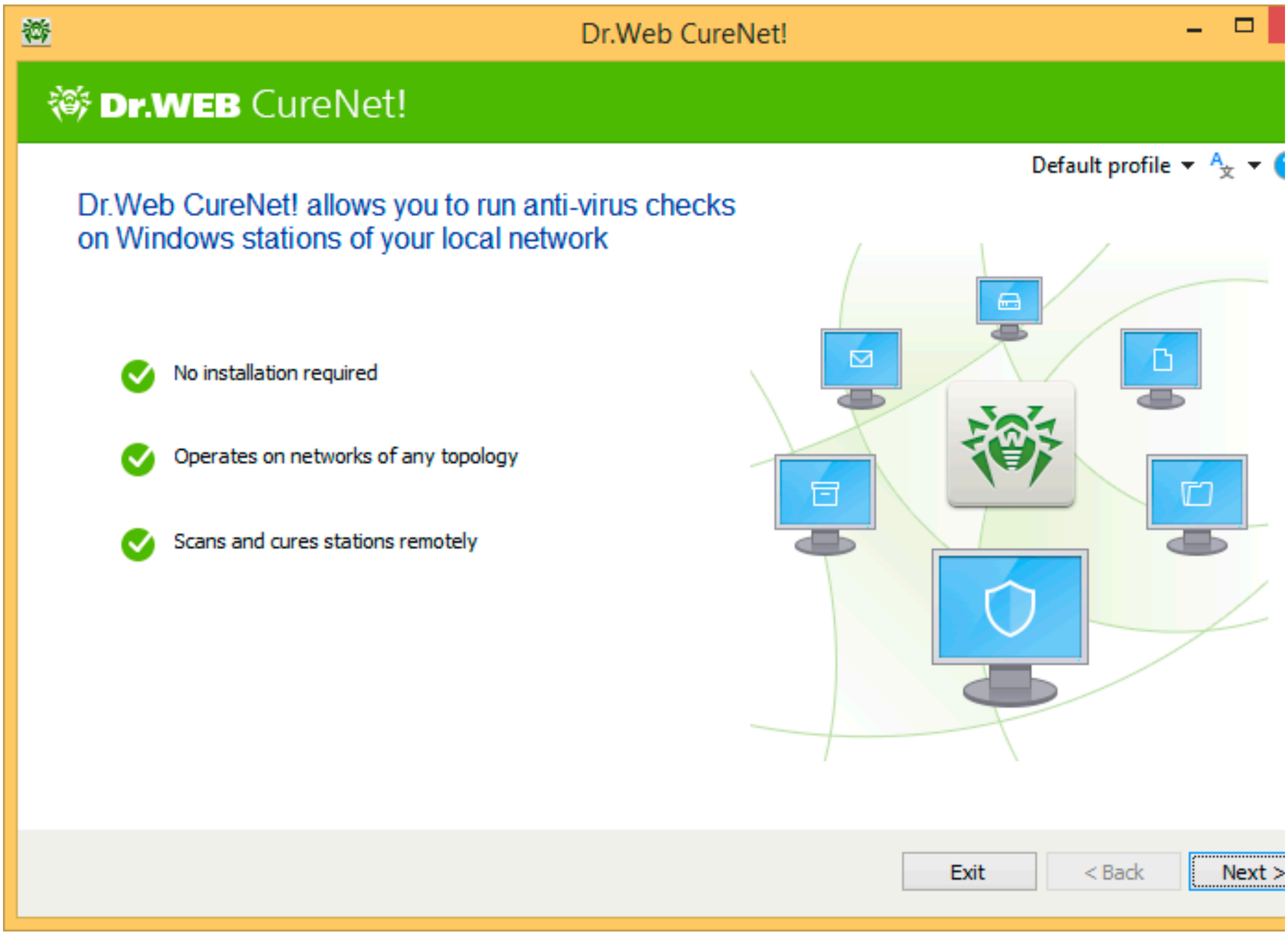
To perform a scan:

1. Open the folder where the **Dr.Web CureNet!** files were saved when it was first launched (by default, this is the **CureNet** folder in the directory where you ran the utility's installation file, or **Desktop** if you saved the installation file on it) and run the **CureNet file**.



Name	Date modified	Type
Profiles	3/4/2020 4:01 PM	File folder
Reports	3/4/2020 4:22 PM	File folder
Repository	3/4/2020 4:00 PM	File folder
curenet	2/27/2017 9:52 AM	Application
CureNet	3/4/2020 4:16 PM	Text Documer
curesvc	3/4/2020 4:09 PM	Configuration
drweb32.key	3/4/2020 3:49 PM	KEY File

If you are using UAC, you will need to click on **Yes** to confirm that you want the program to start. Once you have launched Dr.Web CureNet! you may proceed with scanning as described above.

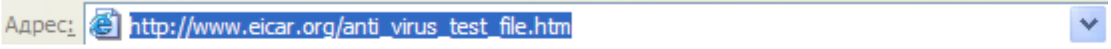


Dr.Web CureNet! allows you to run anti-virus checks on Windows stations of your local network

- No installation required
- Operates on networks of any topology
- Scans and cures stations remotely

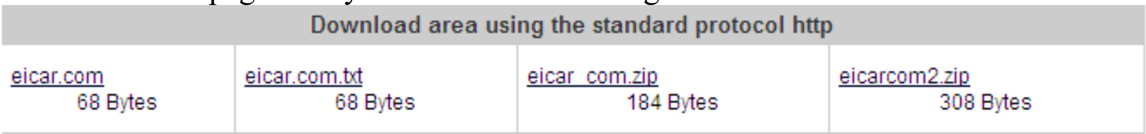
Product operation testing

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.

   Important! If you use Dr.Web CureNet! to supplement your other (non-Dr.Web) anti-virus, disable the anti-virus prior to saving the file.

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

Malware analysis by Doctor Web security researchers

No automated routine can ever replace the experience and knowledge of a security researcher. If Dr.Web vxCube returns a “safe” verdict on your analysed file, but you still have your doubts about this result, Doctor Web's security researchers, who have a wealth of experience analysing malware, are ready to assist you.

With this service, a malicious file of any complexity can be analysed. The resulting report includes:

- Information about the malware’s basic principles of operation and that of its modules;
- An object assessment: downright malicious, potentially dangerous (suspicious), etc.;
- An analysis of the malware's networking features and the location of its command and control servers;
- The impact on the infected system and recommendations on how the threat can be neutralised.

You can submit an anti-virus research request here: https://support.drweb.com

Virus-related computer incident (VCI) expert consultations

If malware has wreaked havoc in your corporate infrastructure and you require the expertise of security researchers to investigate the incident, Doctor Web's information security task force is at your service.

VCI consultations include:

- A preliminary estimate of the incident, the scope of the investigation, and the measures required to neutralise the incident’s consequences.
- An examination of the computer and other related items (hard disks, and text, audio, photo, and video materials) that are presumably related to the VCI.
- Exclusive! A psychological evaluation of individuals (company personnel) to identify possible accomplices involved in/assisting with/covering up or supporting illegal activities against the customer (a comprehensive risk assessment) as well as facts related to inaction or dereliction of duty.
- Recommendations on the deployment of an anti-virus protection system that would prevent VCIs or reduce them to a minimum in the future.

Useful links

About VCI consultations: https://antifraud.drweb.com/expertise

Submit your consultation request here: https://support.drweb.com/expertise

About Doctor Web

Doctor Web is the Russian developer of Dr.Web anti-virus software. Dr.Web products have been developed since 1992. All rights to Dr.Web technologies are reserved by Doctor Web. The company is one of the few anti-virus vendors in the world to have its own technologies for detecting and curing malware. Doctor Web has its own anti-virus laboratory, global virus-monitoring service, and technical support service located in Russia.

Doctor Web is a key player on the Russian market for software that meets the fundamental need of any business — information security. Russia's State Duma, Central Election Committee, Ministry of Defence, Supreme Court, Federation Council, Central Bank, and many other government institutions and large companies have chosen to rely on Dr.Web products.

Here are just some of our customers: https://customers.drweb.com.

Dr.Web products are included in the Unified Register of Russian Computer Programs and Databases of the Ministry of Digital Development, Communications and Mass Media of the Russian Federation.

When customers use Russian-made Dr.Web anti-virus software they are protected from the risks associated with a changing international situation. For example, they do not need to worry about being denied the ability to use, renew, or receive the software or to receive updates, and they are protected from threats that have been created to engage in targeted attacks against Russian organisations and citizens.

Products awarded the quality mark

- Doctor Web possesses certificates that allow Dr.Web software to be used in companies with high security requirements.
- Dr.Web is certified to contain no undeclared features — control level 2, compliance with "Anti-virus protection requirements", approved by FSTEC Russia No. 28 on March 20, 2012, and compliance with FSB Russia's requirements for anti-virus solutions.
- Dr.Web software protects information (including classified information constituting State secrets, personal data, etc.) in the most diverse IT environments.
- Using Dr.Web software ensures proper compliance with the standard requirements of the laws of the Russian Federation on applying measures to protect:
  - sensitive information (state secrets, personal information, etc.);
  - certain categories of citizens from information that can inflict damage.

FSTEC Russia certificates	Russian Defence Ministry certificates	Certificates of the Federal Security Service (FSB)	All certificates and trademarks

Doctor Web has received state certificates and awards; our satisfied customers spanning the globe are clear evidence that the quality of our products, created by a talented team of Russian programmers, is undisputed.

© Doctor Web 2003-2020

3rd street Yamskogo polya 2-12A, Moscow, Russia, 125040

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

Fax: +7 (495) 789-45-97

www.drweb.com