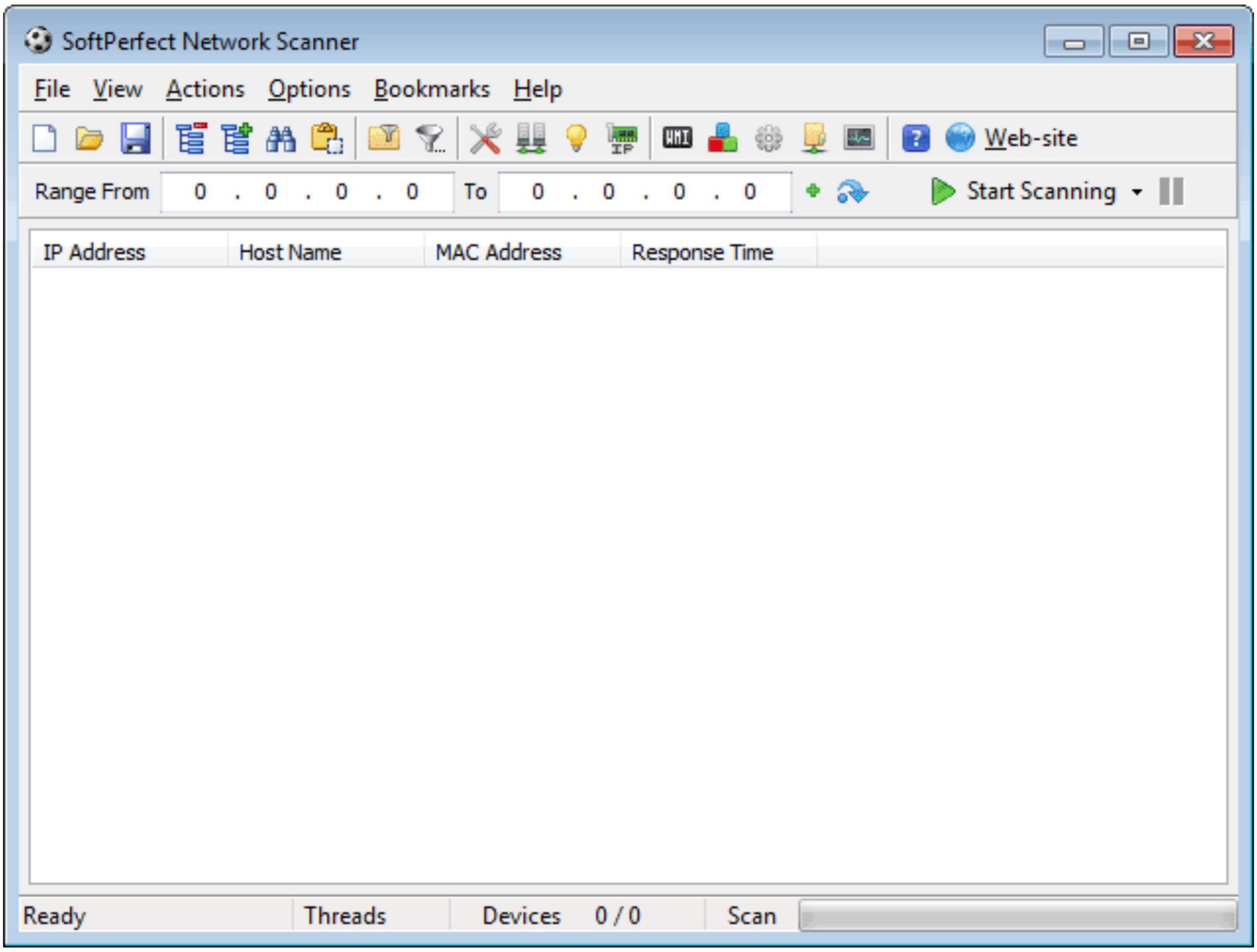
SoftPerfect Network Scanner Online Manual

Product Page / Download

Getting started

This is the main window you see when you run the SoftPerfect Network Scanner.


SoftPerfect Network Scanner
File View Actions Options Bookmarks Help
Web-site
Range From 0 . 0 . 0 . 0 To 0 . 0 . 0 . 0
Start Scanning
IP Address
Host Name
MAC Address
Response Time
Ready
Threads
Devices 0 / 0
Scan

Under the menu there is a toolbar with buttons used to access the main features.
The program controls are as follows:

Clear the display

Load the scan results from a XML file.

Save the scan results to a file.

Collapse the results tree.

Expand the results tree.

Search the results tree.

Paste IP address from the clipboard.

Apply the shares filter. Only computers with available shared folders are shown.

Open the advanced filter panel.

Program options.

Discover DHCP servers.

Open the Wake-on-LAN manager.

Automatically detect the network configuration.

Open the Windows Management Instrumentation manager.

Open the remote registry query manager.

Open the remote service query manager.

Open the remote file query manager.

Open the SNMP query manager.

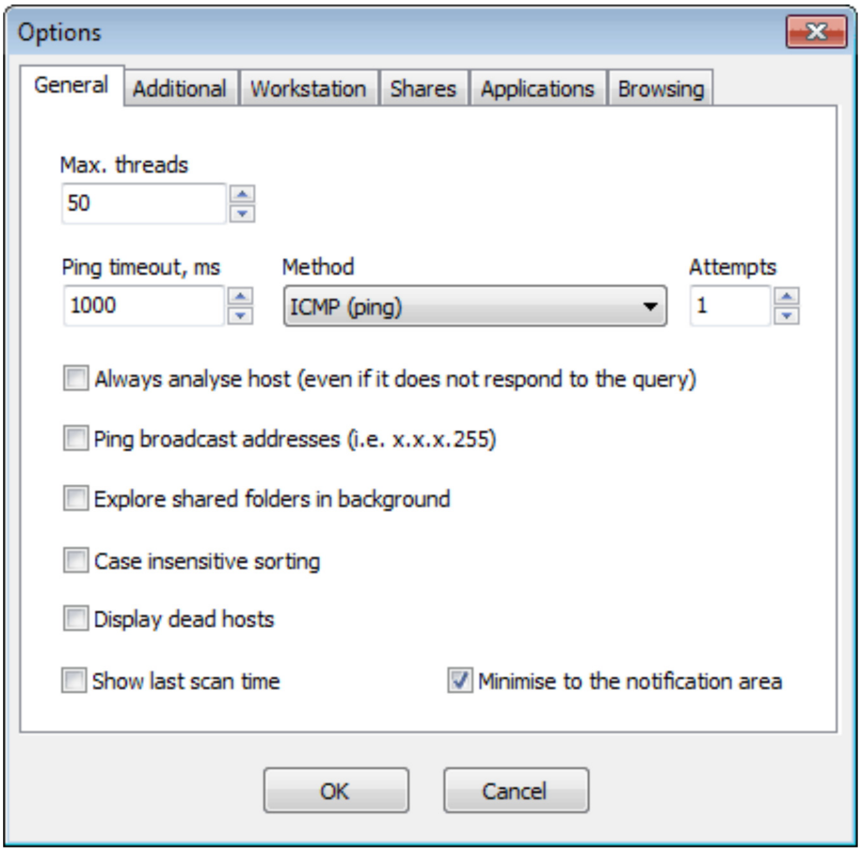
Online Help (this web page).

Add one or more IP address range to scan.

Toggle noncontiguous scan mode.

Program options

Press **Ctrl+O** or the button to access the network scanner options



Max. threads: 50

Ping timeout, ms: 1000

Method: ICMP (ping)

Attempts: 1

☐ Always analyse host (even if it does not respond to the query)

☐ Ping broadcast addresses (i.e. x.x.x.255)

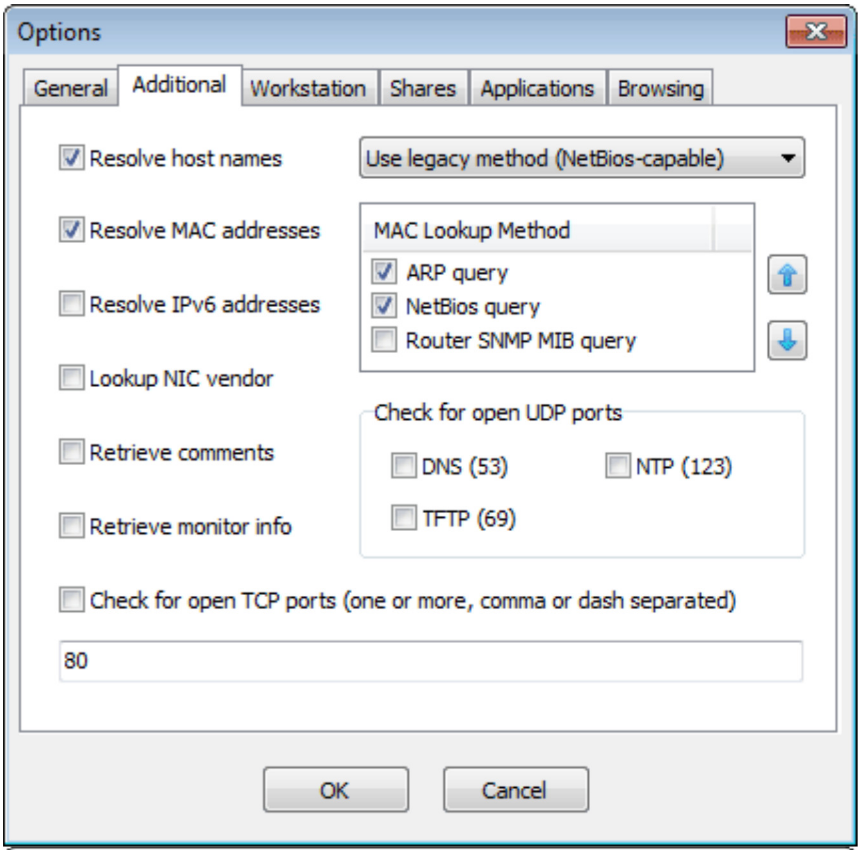
☐ Explore shared folders in background

☐ Case insensitive sorting

☐ Display dead hosts

☐ Show last scan time

☑ Minimise to the notification area



☑ Resolve host names — Use legacy method (NetBios-capable)

☑ Resolve MAC addresses

MAC Lookup Method
☑ ARP query
☑ NetBios query
□ Router SNMP MIB query

□ Resolve IPv6 addresses

□ Lookup NIC vendor

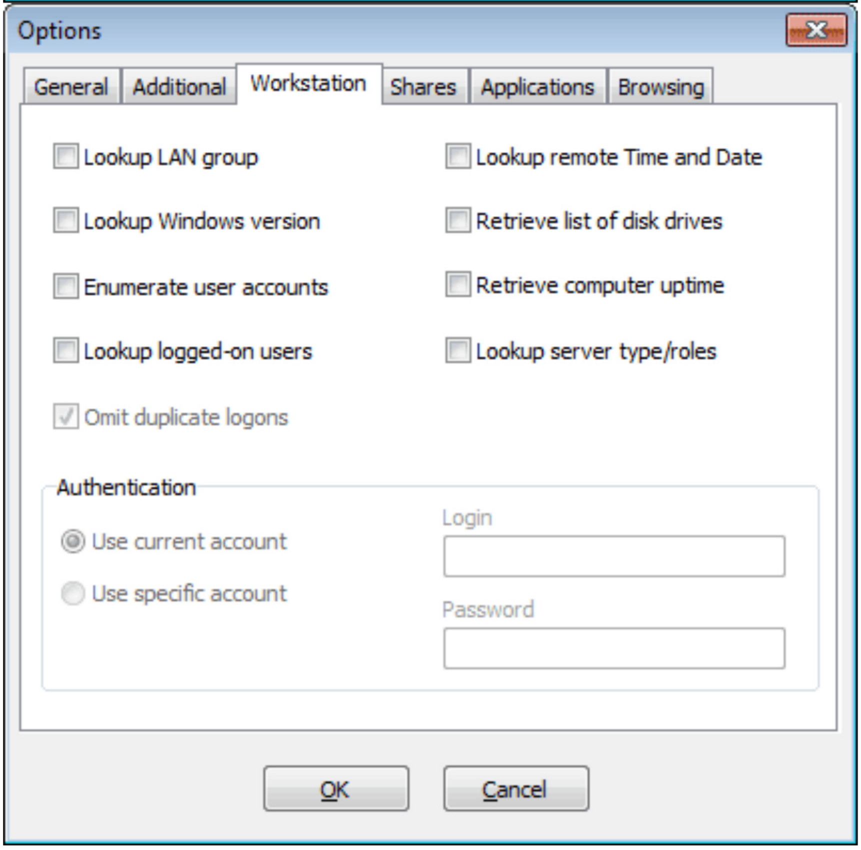
□ Retrieve comments

□ Retrieve monitor info

Check for open UDP ports
□ DNS (53)
□ NTP (123)
□ TFTP (69)

□ Check for open TCP ports (one or more, comma or dash separated)

80



□ Lookup LAN group
□ Lookup remote Time and Date
□ Lookup Windows version
□ Retrieve list of disk drives
□ Enumerate user accounts
□ Retrieve computer uptime
□ Lookup logged-on users
□ Lookup server type/roles
☑ Omit duplicate logons

Authentication
● Use current account
○ Use specific account
Login
Password

On the **General** tab:

- **Max. threads** - the maximum number of scanning threads.
- **Method** - the ping method. Can be chosen from ICMP (ping), ARP (arping), or both.
- **Ping Timeout** - the period to wait for a reply from the remote computer.
- **Retries** - the maximum number of ping requests.
- **Always analyse host** - forces the scanner to analyse a non-responding host.
- **Ping broadcast addresses** - when enabled the scanner tries to ping IP addresses ending with .255.
- **Explore shared folders in background** - If this option is set, whenever you choose to explore a folder

the network scanner launches a separate process of Windows Explorer to avoid temporary unresponsiveness.

- **Case insensitive sorting** - ignores case type when results are sorted.
- **Display dead hosts** - add non-responding hosts into the results.
- **Show last scan time** - shows the time when the host was last scanned.
- **Minimise to the notification area** - the application will be minimised to the system tray.

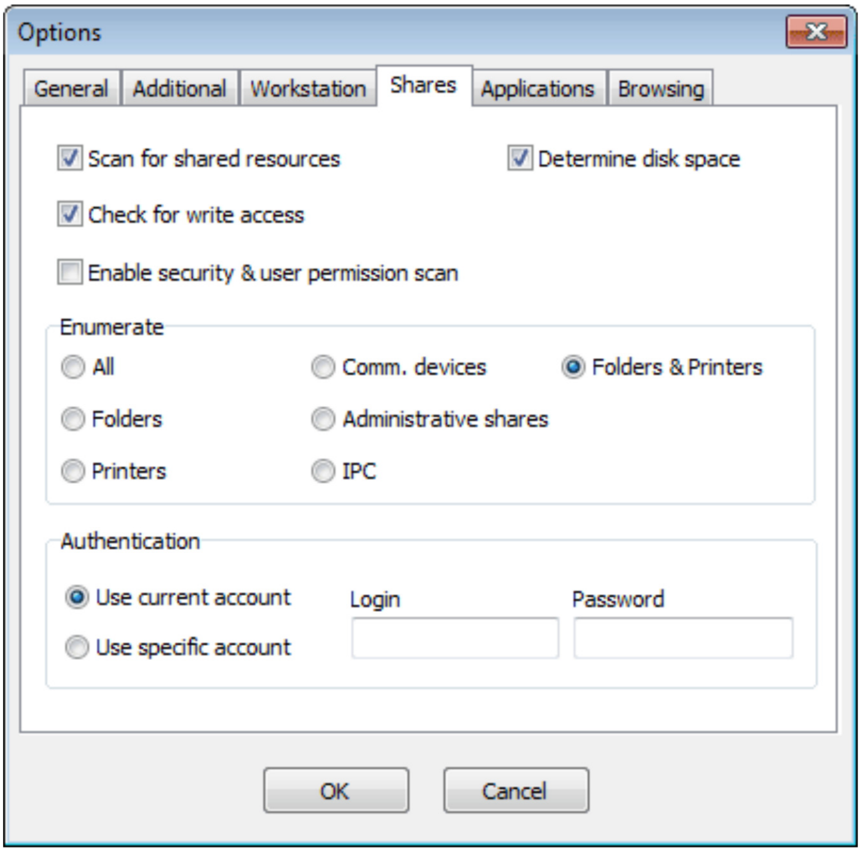
On the **Additional** tab:

- **Resolve Host Names** - when enabled, the IP addresses are converted to the host names.
- **Resolve MAC addresses** - when enabled, you will see hardware (MAC) addresses. There are three discovery methods available: ARP query, NetBios query and Router SNMP MIB query. The **ARP query** option sends an ARP packet to the target device to resolve its MAC address directly. Similarly, the **NetBios query** option sends a NetBios packet to the target device. If the target device responds to the query, the network scanner will obtain the MAC address of that device. The **Router SNMP MIB query** option works differently. Before starting scanning the application will send a few SNMP requests to the default gateway configured in your network card's properties in order to retrieve the information on what MAC address corresponds to what IP address. If the gateway is SNMP capable and responds the query, the application will cache this information and use it for MAC address resolution. Generally, the ARP query option is sufficient to resolve all MAC addresses in a local subnet. However, if you also require to discover those behind the router, enable the **NetBios query** and **Router SNMP MIB query** options and place them first and second in the list.
- **Resolve IPv6 addresses** - enables the network scanner to obtain the IPv6 address of a remote host. This feature requires Windows Vista or above and discovers addresses of hosts with a dual IPv4/IPv6 stack.
- **Lookup NIC vendor** - as per the IEEE standard, the first three octets of a MAC address represent the NIC's vendor. In order to use this feature you will need to download this file from the IEEE and save it to the network scanner folder.
- **Retrieve comments** - displays a comment assigned to a Windows workstation.
- **Retrieve monitor info** - displays monitor vendor, model and serial number if available. This feature requires the remote registry service as the information is read from the registry.
- **Check for open TCP ports** - attempts connection to the specified TCP ports and reports those open (you can specify several ports separated by a comma or dash, e.g. 21, 80, 110-115).
- **Check for open UDP ports** - discovers some UDP-based services such as DNS, TFTP and NTP.

On the **Workstation** tab:[1]

- **Lookup LAN group** - displays the workgroup/domain name which a Windows workstation belongs to.
- **Lookup logged-on users** - displays a list of users currently logged-on to a Windows workstation.
- **Lookup Windows version** - displays the Windows version on a workstation.
- **Lookup remote Time and Date** - Retrieves and shows the time of the day on a remote system.
- **Retrieve list of disk drives** - Lists all disk drives available on a remote computer.
- **Retrieve computer uptime** - Shows how long a remote computer was up and running.
- **Enumerate user accounts** - lists all user accounts registered on a remote computer.
- **Lookup server type/roles** - displays all roles (e.g. PDC, SQL server, Master Browser) assigned to a server.

[1] See the rightmost columns on the main screen once you have enabled one or more options.



☑ Scan for shared resources
☑ Determine disk space
☑ Check for write access
□ Enable security & user permission scan

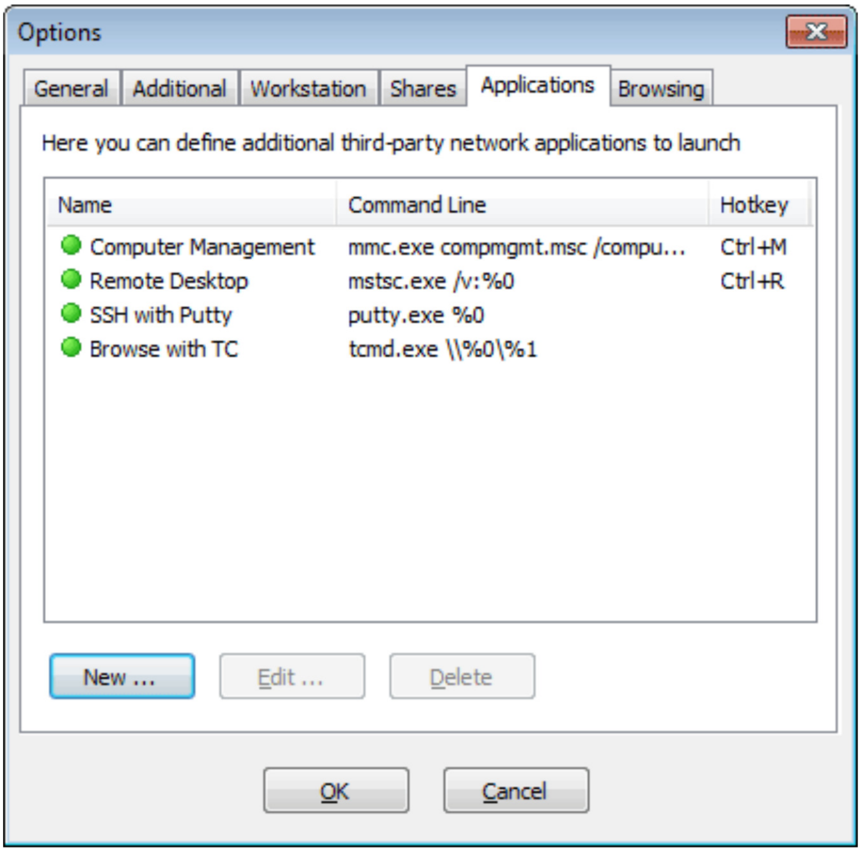
Enumerate

○ All
○ Comm. devices
● Folders & Printers
○ Folders
○ Administrative shares
○ Printers
○ IPC

Authentication

● Use current account
○ Use specific account
Login
Password

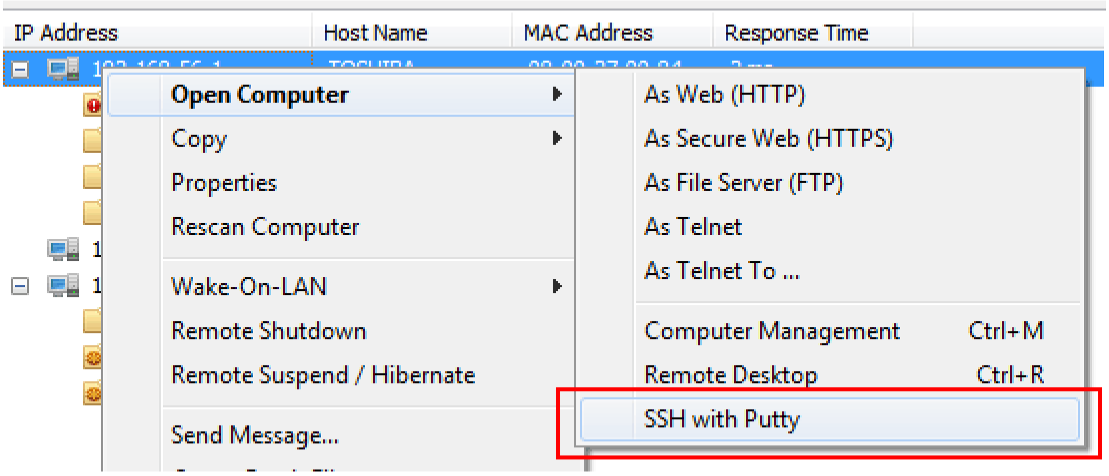
- **Scan for shared resources** - enables scanning of shared resources. Below are all the possible types of shared resources.
- **Check for write access** - determines if the shared folder is writable or not (read only).
- **Enable security & user permission scan** - with this option enabled, the network scanner will discover what reading and writing privileges are assigned to shared folders. You may have to be an administrator to retrieve this information.
- **Determine disk space** - determines shared folders' total and free space.
- **All** - all resources.
- **Folders** - shared folders or drives.
- **Printers** - shared printers.
- **Comm. device** - communication devices.
- **Administrative shares** - special share reserved for remote administration of the server, e.g. ADMIN$, C$, D$, E$, etc.
- **IPC** - interprocess communication (IPC).

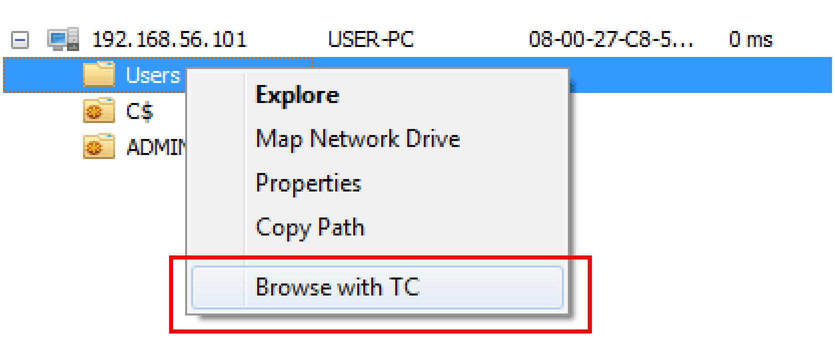


Here you can define additional third-party network applications to launch

Name	Command Line	Hotkey
● Computer Management	mmc.exe compmgmt.msc /compu...	Ctrl+M
● Remote Desktop	mstsc.exe /v:%0	Ctrl+R
● SSH with Putty	putty.exe %0	
● Browse with TC	tcmd.exe \\%0\%1	

The **Applications** tab extends support for third-party applications. For example, if you use remote administration or specific network client software, you can setup the network scanner to connect to a remote host using the additional software directly from the network scanner.

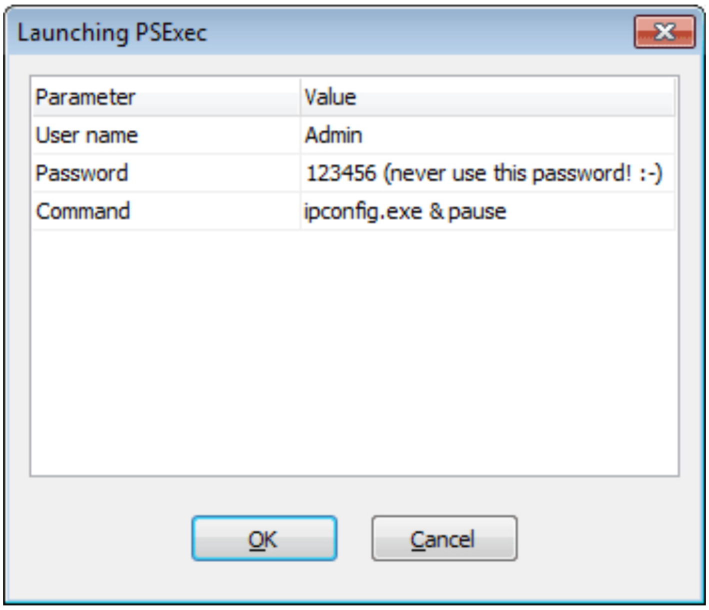




Should you require to pass extra arguments upon launching an application, you can use user-prompted parameters specified in braces. As an example, the following line lets you quickly execute commands on the remote system with **PsExec** from SysInternals.

```
psexec.exe \\%0 -u {User name} -p {Password} {Command}
```

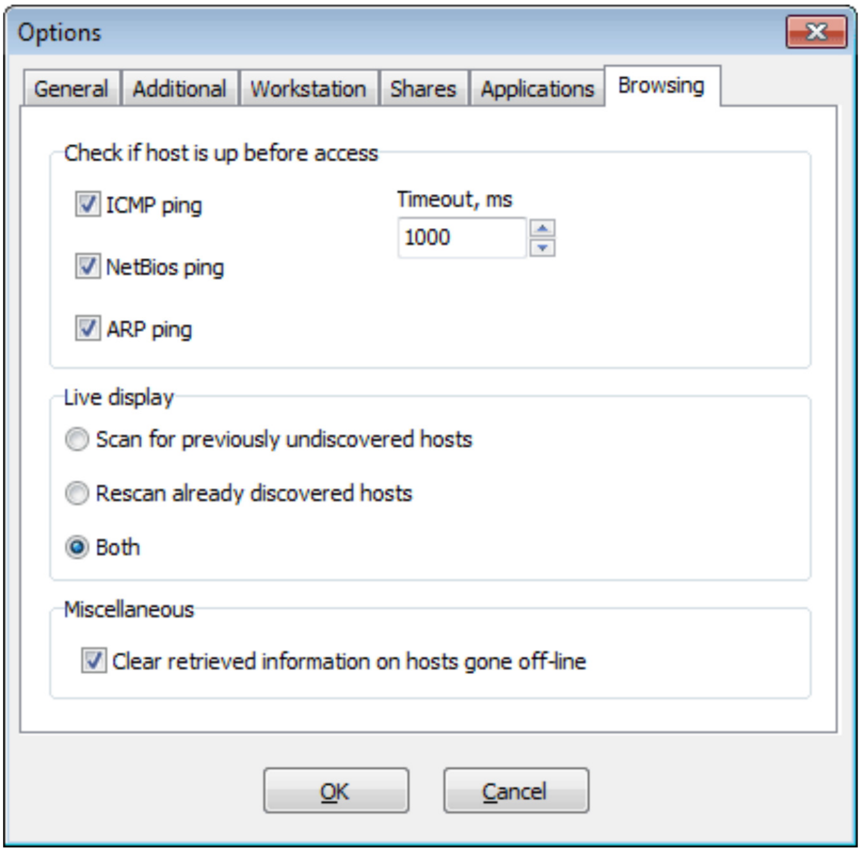
Launching this command will bring up a window where you may specify the arguments to pass to **PsExec** as shown below. Then the network scanner will launch **PsExec** with your input.



Launching PSExec

Parameter	Value
User name	Admin
Password	123456 (never use this password! :-)
Command	ipconfig.exe & pause

Finally, the **Browsing** tab enables the network scanner to check whether a host is still on-line when you attempt to explore its folders, or establish a connection to that host. This greatly speeds up some operations, as an attempt to connect an off-line computer might temporarily hang the network scanner until the connection fails You can enable one or more methods to check the availability and set a timeout. Additionally you can choose a live display mode, whether the network scanner must only find previously undiscovered nodes in background, or it must keep rescanning those already discovered, or it must do both. Don't forget to turn the live display on in the main menu **View** - **Enable Live Display**.



Check if host is up before access

☑ ICMP ping

☑ NetBios ping

☑ ARP ping

Timeout, ms: 1000

Live display

○ Scan for previously undiscovered hosts

○ Rescan already discovered hosts

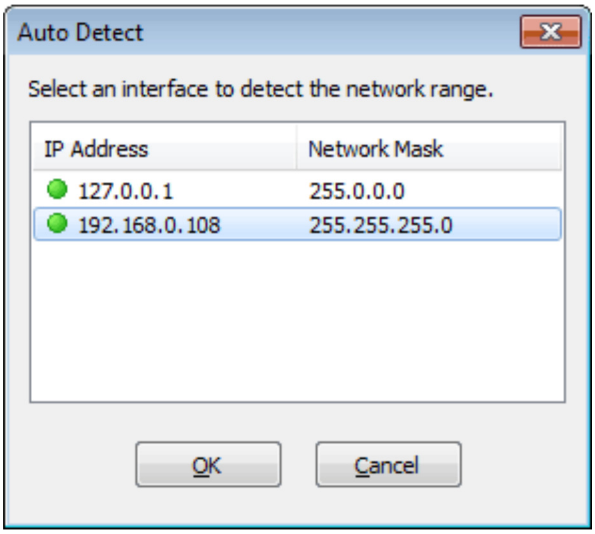
● Both

Miscellaneous

☑ Clear retrieved information on hosts gone off-line

IP range and automatic detection of network configuration

The SoftPerfect Network Scanner is able to detect your IP range automatically. Select the **Options - IP Address - Detect Local IP Range** menu item. In the following dialog, select an interface and the program will calculate the IP range of the network. If you are connected to the Internet and are behind a router or proxy server, use the **Detect External IP Address** command to determine your external IP address (requires Internet connection).

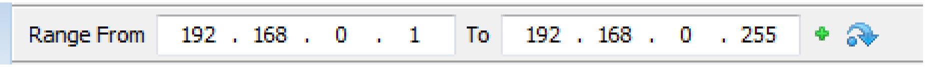


Auto Detect

Select an interface to detect the network range.

IP Address	Network Mask
● 127.0.0.1	255.0.0.0
● 192.168.0.108	255.255.255.0

In this example SoftPerfect Network Scanner has determined the range of IP addresses on the network. You are good to go!



Range From 192 . 168 . 0 . 1 To 192 . 168 . 0 . 255

You can add more IP address ranges to scan with the ✚ button.

The interpretation of your IP address range depends on the state of the ↷ button. If the button is up, the range is interpreted as a regular one. In this case the program will sequentially scan all IP addresses within the range. If it is down, the range is interpreted as a noncontiguous one. In this case the program will only scan IP addresses whose octets fall in the range. For example, if you specify a range of 10.1.254.1 to 10.9.254.5, the following octets will be scanned:

Octet 1: 10 - 10
Octet 2: 1 - 9
Octet 3: 254 - 254
Octet 4: 1 - 5

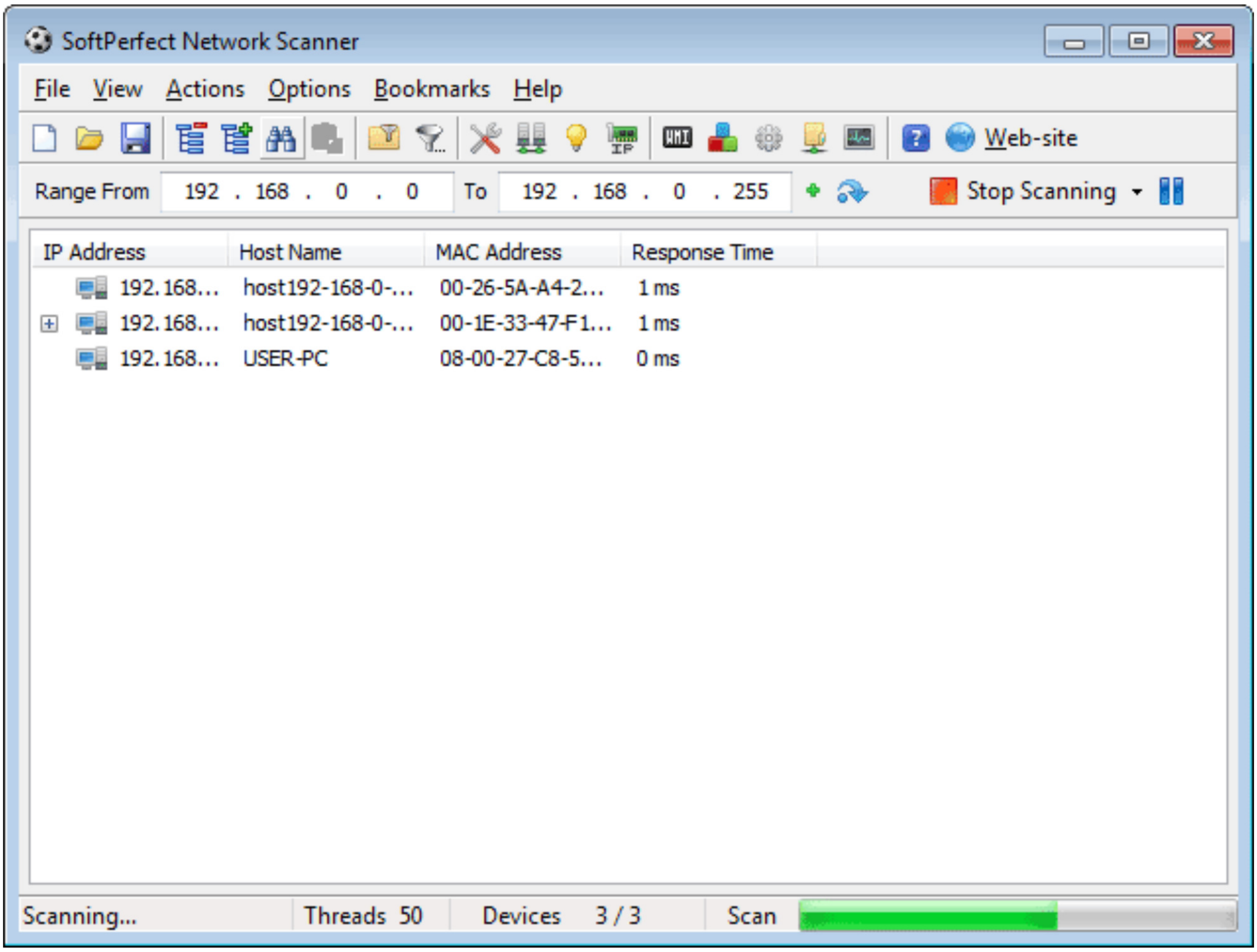
Therefore, the program will scan

10.**1**.254.**1**, 10.**1**.254.**2**, 10.**1**.254.**3**, 10.**1**.254.**4**, 10.**1**.254.**5**
10.**2**.254.**1**, 10.**2**.254.**2**, 10.**2**.254.**3**, 10.**2**.254.**4**, 10.**2**.254.**5**
10.**3**.254.**1**, 10.**3**.254.**2**, 10.**3**.254.**3**, 10.**3**.254.**4**, 10.**3**.254.**5**
...
10.**9**.254.**1**, 10.**9**.254.**2**, 10.**9**.254.**3**, 10.**9**.254.**4**, 10.**9**.254.**5**

This can be useful if you have got a large network and you want to scan specific devices in each subnet.

Scanning

To begin scanning click the **Start Scanning** button



SoftPerfect Network Scanner
File View Actions Options Bookmarks Help
Web-site
Stop Scanning

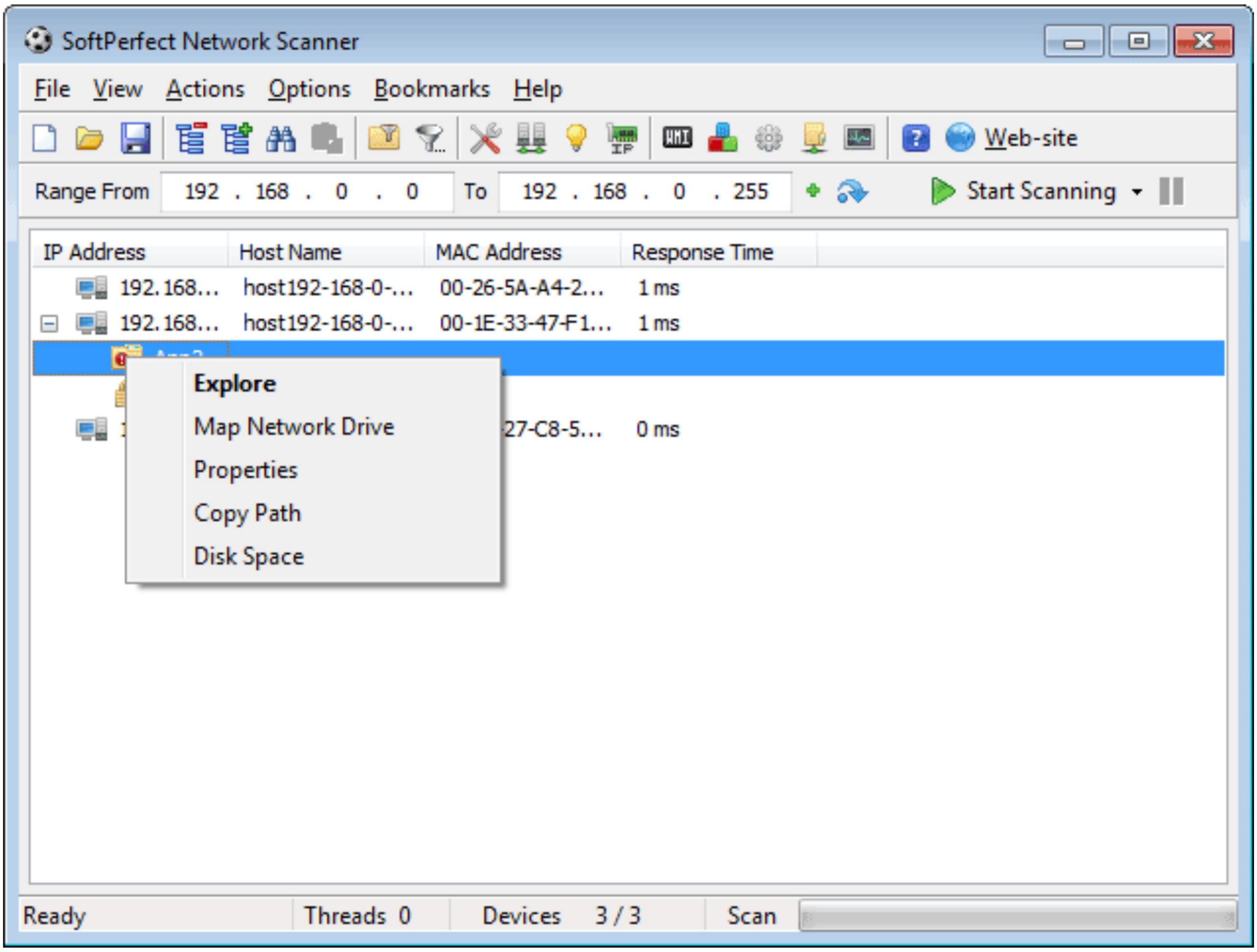
Range From 192 . 168 . 0 . 0 To 192 . 168 . 0 . 255

IP Address	Host Name	MAC Address	Response Time
192.168...	host192-168-0-...	00-26-5A-A4-2...	1 ms
192.168...	host192-168-0-...	00-1E-33-47-F1...	1 ms
192.168...	USER-PC	08-00-27-C8-5...	0 ms

Scanning... Threads 50 Devices 3 / 3 Scan

Scan results

When scanning has finished, you will be able to browse the results, save to a file, map a network drive, explore folders, etc.



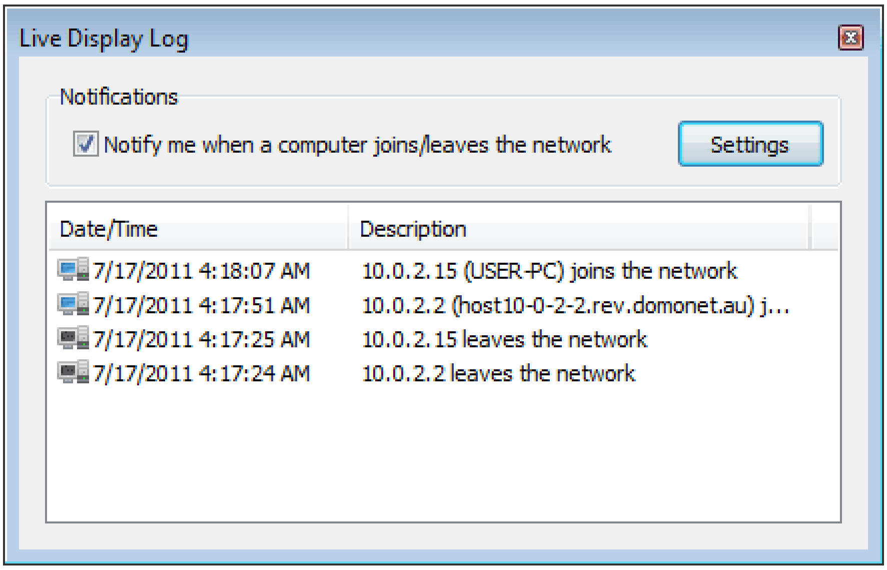
Range From 192 . 168 . 0 . 0 To 192 . 168 . 0 . 255

IP Address	Host Name	MAC Address	Response Time
192.168…	host192-168-0-…	00-26-5A-A4-2…	1 ms
192.168…	host192-168-0-…	00-1E-33-47-F1…	1 ms
1		27-C8-5…	0 ms

Ready Threads 0 Devices 3 / 3 Scan

Live display

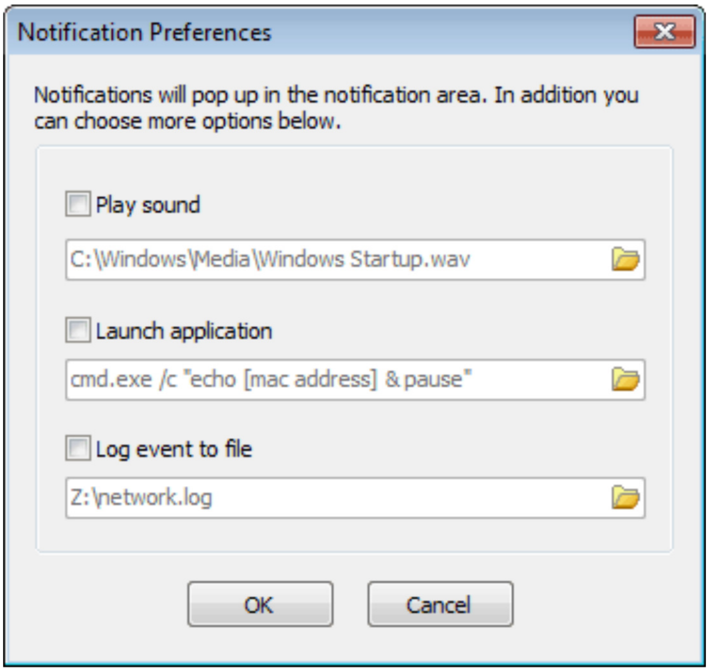
If you enable the **Live Display** option (choose **View - Live Display** from the main menu), the network scanner will constantly update scan results to reveal the latest changes in the network. If a new host joins or leaves the network, it will be reflected in the main window. There is also a live display log keeping track of computers joining and leaving the network. When the live display is active, choose **View - Show Live Display Log** from the main menu to access it.



☑ Notify me when a computer joins/leaves the network

Date/Time	Description
7/17/2011 4:18:07 AM	10.0.2.15 (USER-PC) joins the network
7/17/2011 4:17:51 AM	10.0.2.2 (host10-0-2-2.rev.domonet.au) j…
7/17/2011 4:17:25 AM	10.0.2.15 leaves the network
7/17/2011 4:17:24 AM	10.0.2.2 leaves the network

You can specify what happens when a computer joins or leaves the network. If the **Notify me...** option is ticked, a balloon will popup in the notification area. In addition you can choose one or more actions in the settings: play a sound, launch another application or save the event to a file. It is also possible to pass the contents of any column to the application by specifying it in the square brackets as shown below.



Notification Preferences

Notifications will pop up in the notification area. In addition you can choose more options below.

□ Play sound

C:\Windows\Media\Windows Startup.wav

□ Launch application

cmd.exe /c "echo [mac address] & pause"

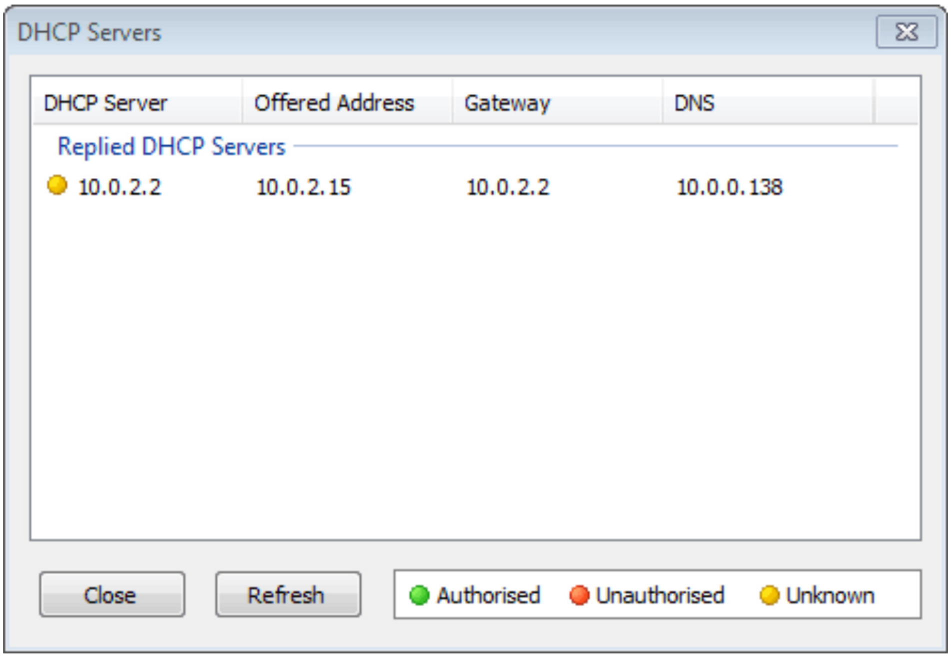
□ Log event to file

Z:\network.log

Rogue DHCP server detection

There is a built-in tool searching for active DHCP servers in a LAN segment. It does not require a scan as such. Instead it broadcasts a DHCP discovery message and collects replies from all available DHCP servers. These may be either normal DHCP servers, or rogue servers that are not under administrative control of the network staff. The latter may disrupt connectivity or may be used for network attacks.

In order to see all active DHCP servers, choose **Actions** - **DHCP Server Discovery** from the main menu. In a few moments, you will see a list of all the servers along with offered DNS and gateway addresses.

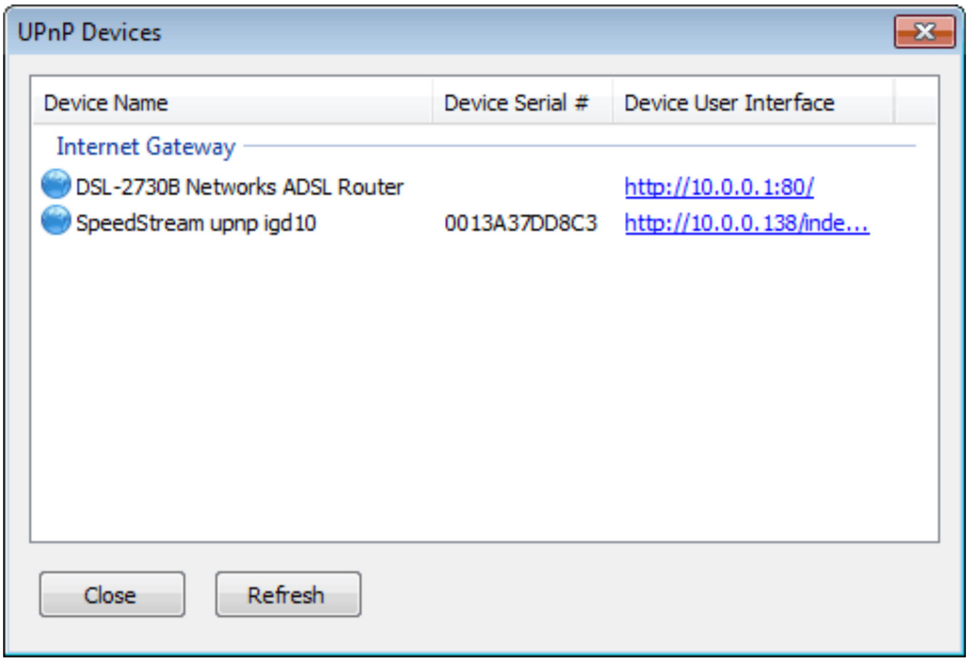


DHCP Servers

DHCP Server	Offered Address	Gateway	DNS
Replied DHCP Servers			
● 10.0.2.2	10.0.2.15	10.0.2.2	10.0.0.138

UPnP device detection

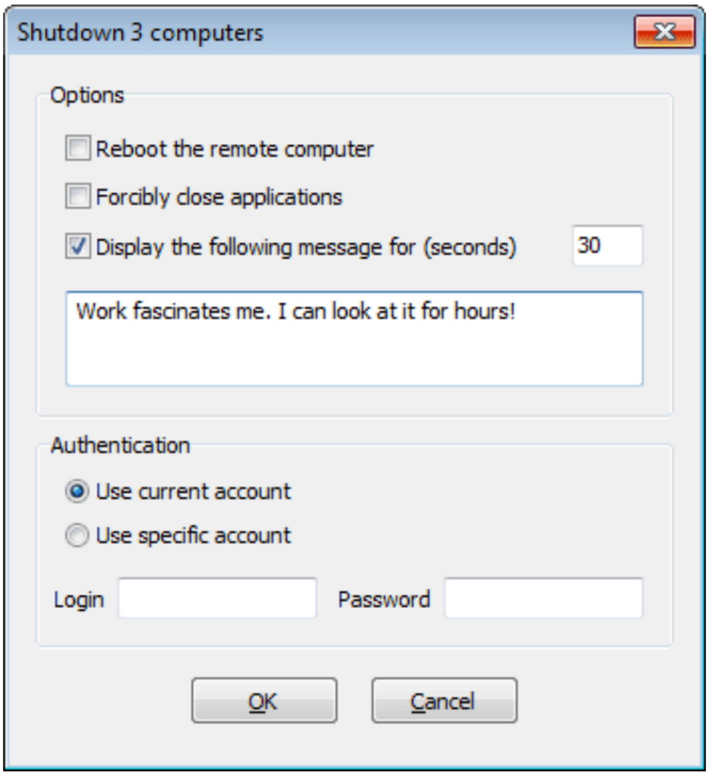
Furthermore, the application can discover Universal Plug and Play (UPnP) devices in your network such as media servers, routers and printers. Similarly to the DHCP discovery, it broadcasts a UPnP discovery message and collects replies from compatible devices. In order to see your UPnP devices, choose **Actions** - **UPnP Device Discovery** from the main menu. Click a **Device User Interface** URL to access the device.



Device Name	Device Serial #	Device User Interface
Internet Gateway		
DSL-2730B Networks ADSL Router		http://10.0.0.1:80/
SpeedStream upnp igd10	0013A37DD8C3	http://10.0.0.138/inde...

Wake-on-LAN and remote shutdown

To send a 'magic' wake up packet to a remote computer (its MAC address must be known), choose **Actions - Wake-On-LAN** from the main menu. To shutdown or reboot a remote PC, choose **Actions - Remote Shutdown**. You can also suspend or hibernate a remote computer by choosing **Actions - Remote Suspend/Hibernate.**



Options

□ Reboot the remote computer

□ Forcibly close applications

☑ Display the following message for (seconds) 30

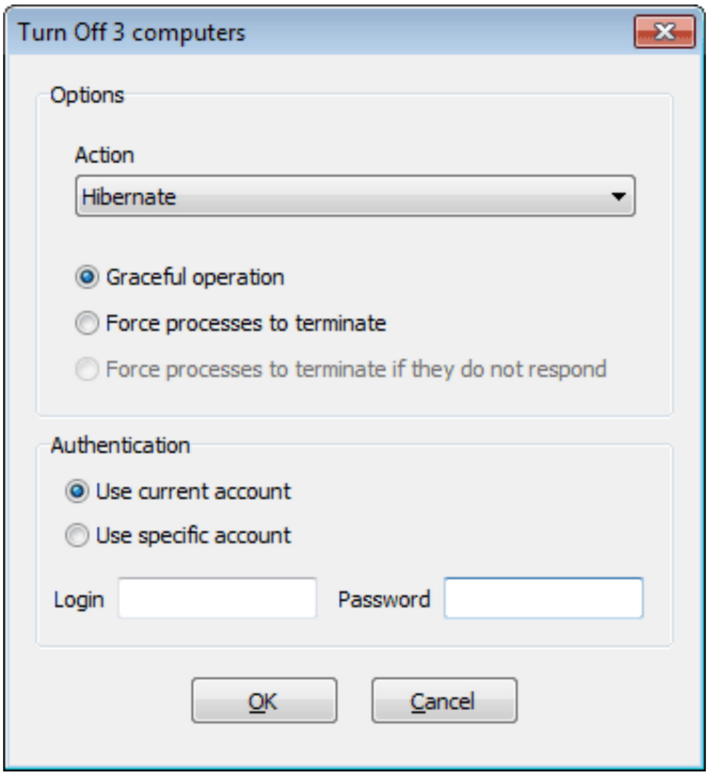
Work fascinates me. I can look at it for hours!

Authentication

● Use current account

○ Use specific account

Login Password



Turn Off 3 computers

Options

Action: Hibernate

● Graceful operation

○ Force processes to terminate

○ Force processes to terminate if they do not respond

Authentication

● Use current account

○ Use specific account

Login

Password

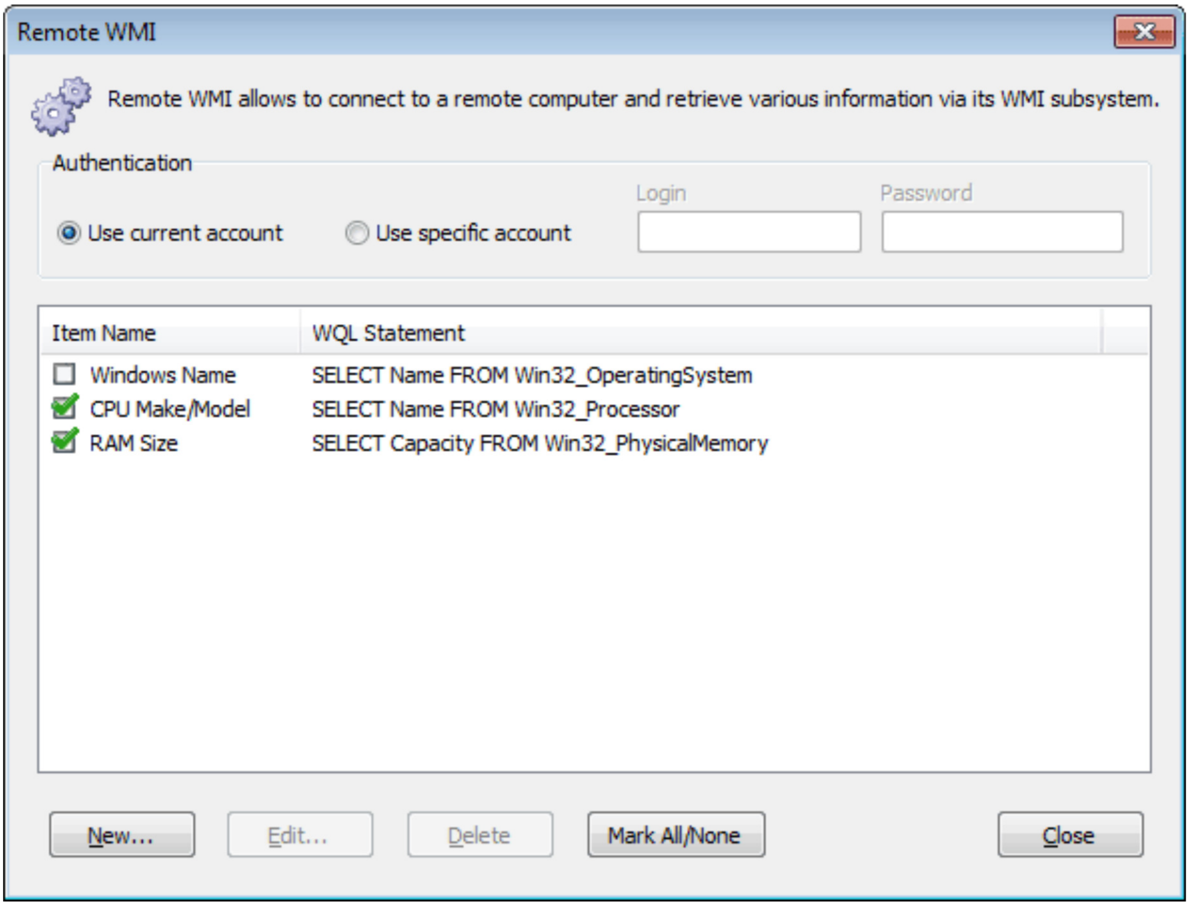
In order to shutdown or suspend a remote computer, several criteria must be met:

- Administrative shares are enabled.
- Administrator has got a non-empty password.
- Simple file sharing is turned off.
- Administrative shares IPC$ and ADMIN$ are accessible.

Otherwise you may encounter either the error *Access is denied* or *Network path not found*.

WMI Query builder and scanning

The network scanner is capable of running WMI (Windows Management Instrumentation) queries against hosts being scanned. In order to create a WMI query, choose **Options - WMI** from the main menu. Queries are written in a special language called WQL, similar to SQL.



Remote WMI

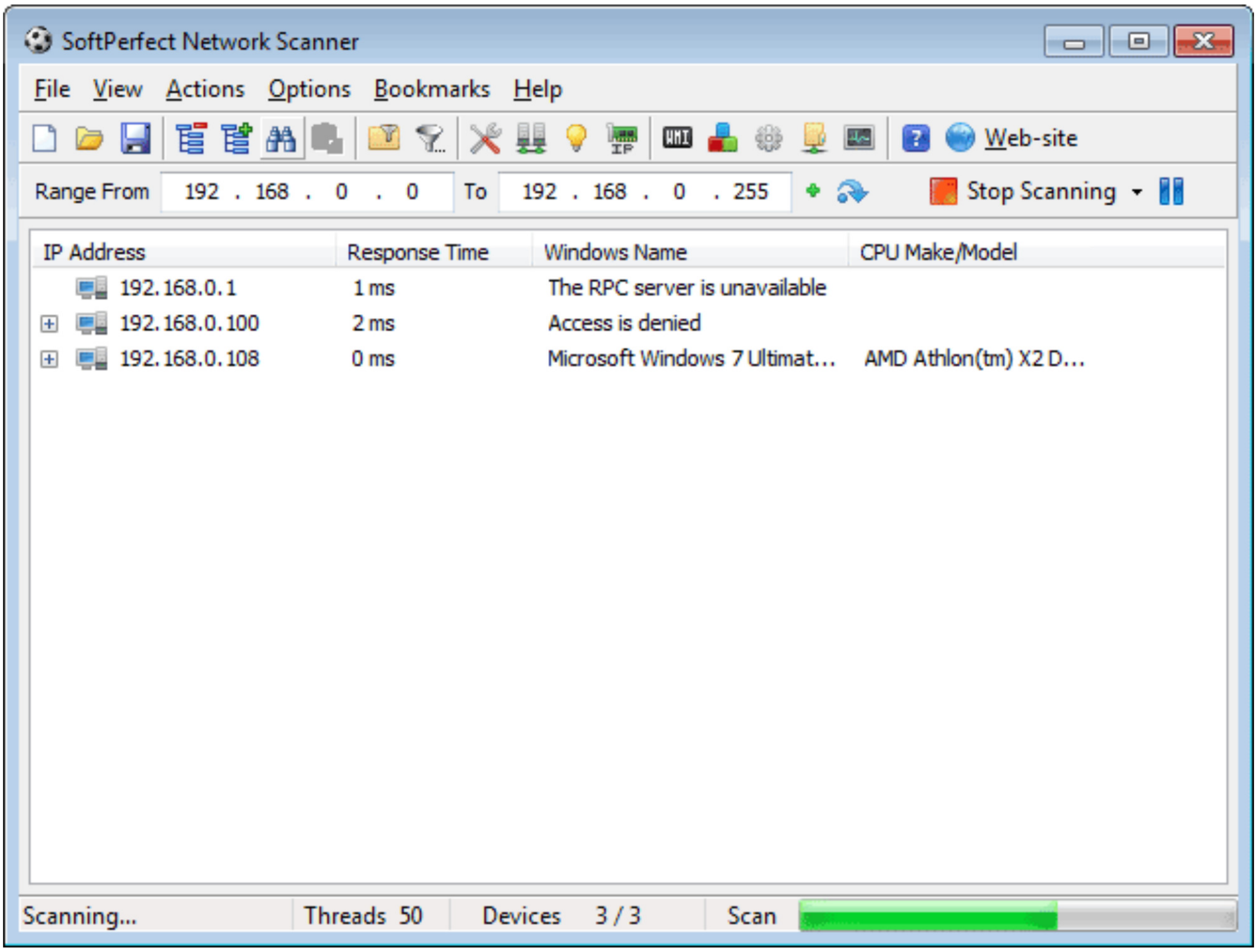
Remote WMI allows to connect to a remote computer and retrieve various information via its WMI subsystem.

Authentication

● Use current account ○ Use specific account Login Password

Item Name	WQL Statement
□ Windows Name	SELECT Name FROM Win32_OperatingSystem
☑ CPU Make/Model	SELECT Name FROM Win32_Processor
☑ RAM Size	SELECT Capacity FROM Win32_PhysicalMemory

The **New** button allows you to easily construct simple WQL queries. It merely connects to your computer's WMI subsystem and lets you pick a WMI class and parameter to be used in the query. When you have one or more WMI queries enabled, there will be additional columns shown in the scan results.



SoftPerfect Network Scanner

Range From 192 . 168 . 0 . 0 To 192 . 168 . 0 . 255

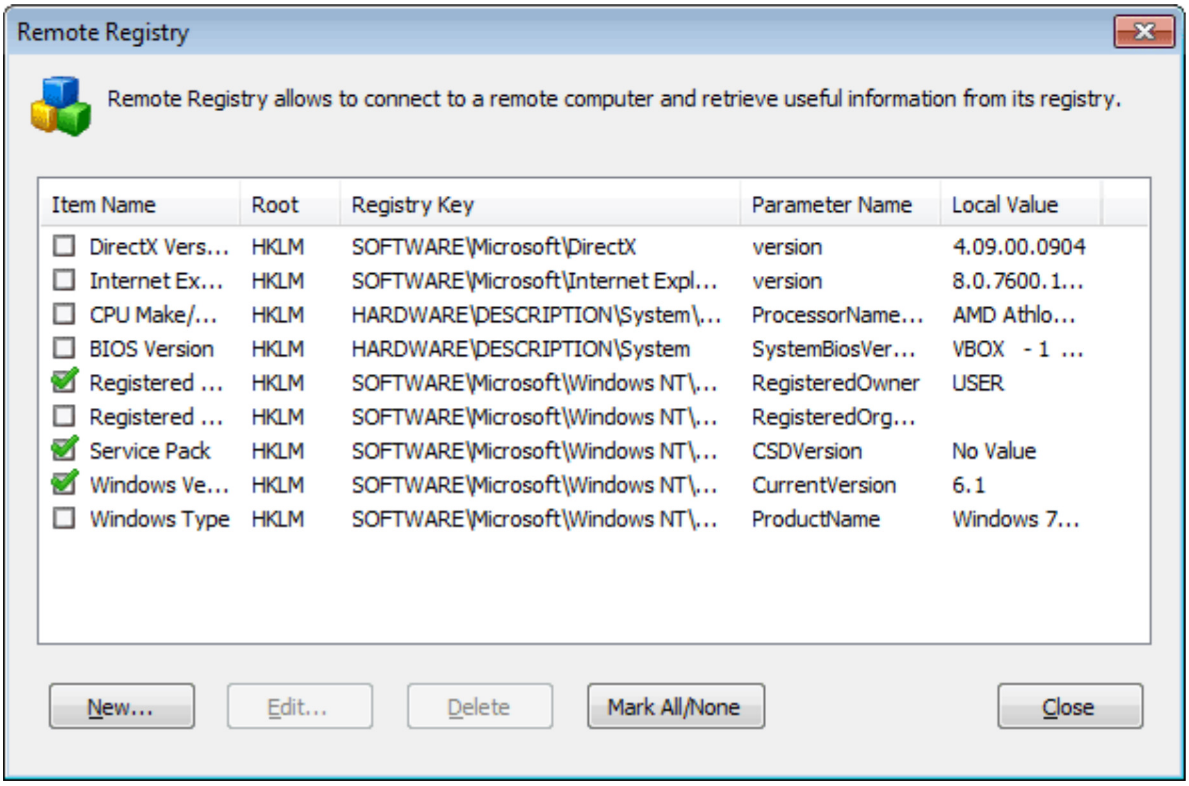
IP Address	Response Time	Windows Name	CPU Make/Model
192.168.0.1	1 ms	The RPC server is unavailable	
⊞ 192.168.0.100	2 ms	Access is denied	
⊞ 192.168.0.108	0 ms	Microsoft Windows 7 Ultimat...	AMD Athlon(tm) X2 D...

Scanning... Threads 50 Devices 3 / 3 Scan

Remote file, registry and services

Firstly, the application can connect to the remote registry of remote PCs running Windows, provided the remote registry service is started. Secondly, it can also connect to the their file system via administrative shares (C$, D$, E$, etc) and retrieve information about a specific file. Thirdly, it can connect to the remote service manager and query the status of one or more service. These features are useful mainly for network administrators maintaining large networks and can be accessed by choosing **Options - Remote Registry**, **Options - Remote File** or **Options - Remote Services** from the main menu.

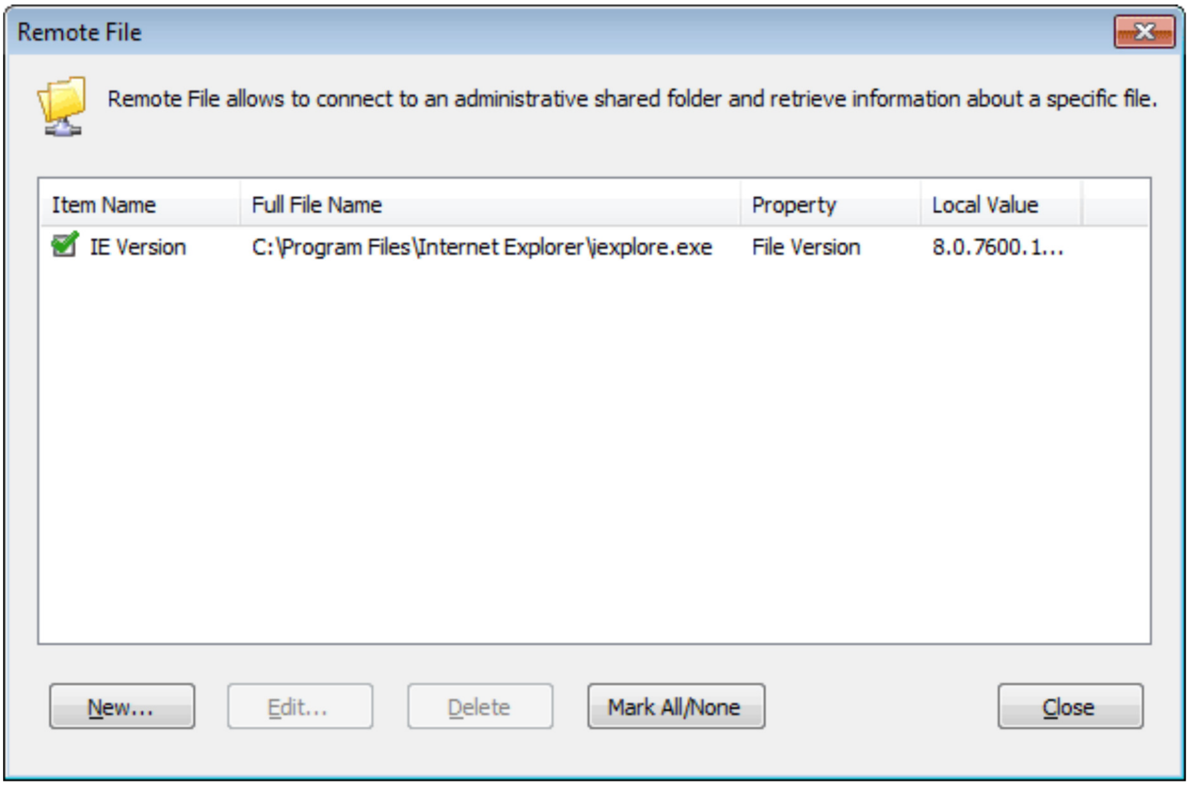
There are several predefined entries in the list and you can easily add new items to retrieve data about hardware and software specific to your environment. The columns are as follows: **Item Name** is a name of the entry. **Root** represents one of the root registry hives. **Registry key** contains the path to a value of interest. **Parameter Name** is the value name to be retrieved. Finally, **Local Value** merely shows the value in the local registry on your computer. On this screenshot three items are chosen to be retrieved from remote computers.



Remote Registry allows to connect to a remote computer and retrieve useful information from its registry.

Item Name	Root	Registry Key	Parameter Name	Local Value
☐ DirectX Vers...	HKLM	SOFTWARE\Microsoft\DirectX	version	4.09.00.0904
☐ Internet Ex...	HKLM	SOFTWARE\Microsoft\Internet Expl...	version	8.0.7600.1...
☐ CPU Make/...	HKLM	HARDWARE\DESCRIPTION\System\...	ProcessorName...	AMD Athlo...
☐ BIOS Version	HKLM	HARDWARE\DESCRIPTION\System	SystemBiosVer...	VBOX - 1 ...
☑ Registered ...	HKLM	SOFTWARE\Microsoft\Windows NT\...	RegisteredOwner	USER
☐ Registered ...	HKLM	SOFTWARE\Microsoft\Windows NT\...	RegisteredOrg...	
☑ Service Pack	HKLM	SOFTWARE\Microsoft\Windows NT\...	CSDVersion	No Value
☑ Windows Ve...	HKLM	SOFTWARE\Microsoft\Windows NT\...	CurrentVersion	6.1
☐ Windows Type	HKLM	SOFTWARE\Microsoft\Windows NT\...	ProductName	Windows 7...

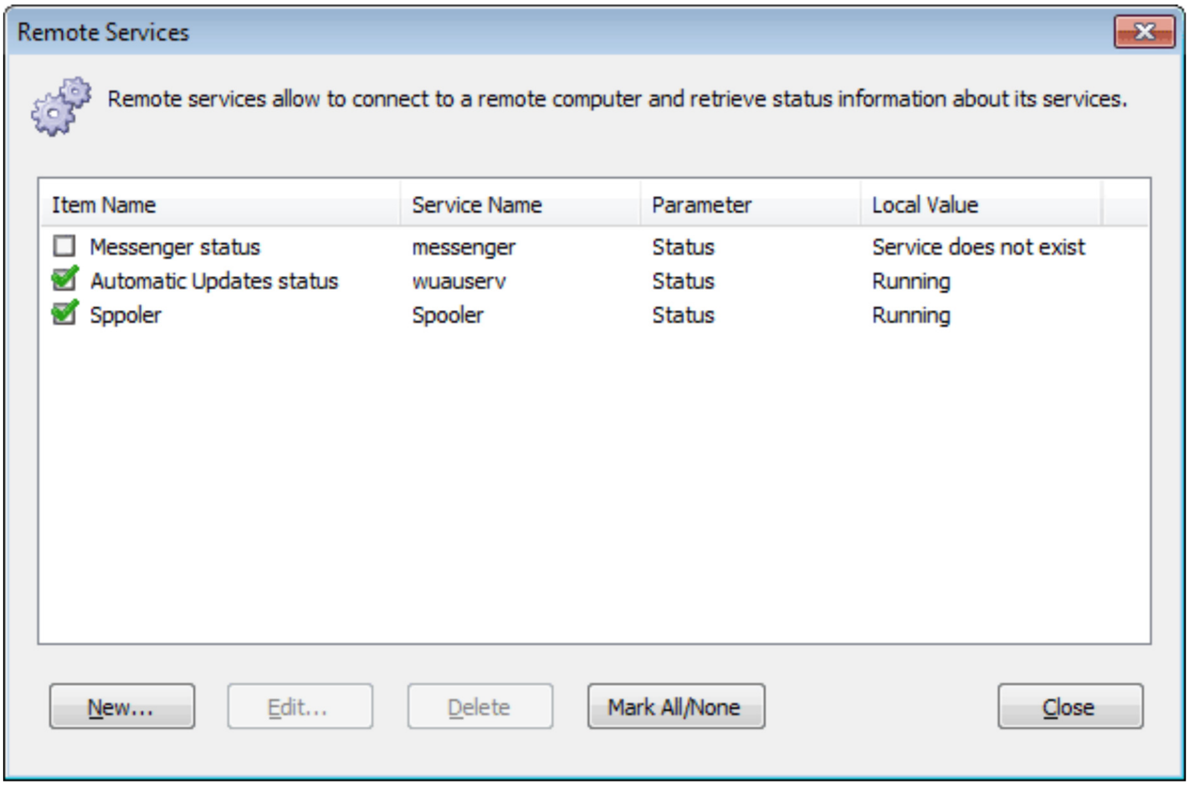
Likewise, provided the administrative shares are enabled and accessible, you can pull out information about a specific file on remote computers. For example, you want to find out the version of Internet Explorer, or when a log file changed, or how large a particular file is. To do so, enter the full name of a file and choose what property you would like to retrieve. On the following screenshot, the application is configured to access the Internet Explorer executable and display its version. Drive letters get substituted to the relevant administrative shared folders. For example, if you scan a range of 10.0.0.1 to 10.0.0.10 with these settings, the application will attempt to display the version information embedded in the files \\10.0.0.1\C$\Program Files\Internet Explorer\iexplore.exe, **10.0.0.2**\C$\Program Files\Internet Explorer\iexplore.exe, etc.



Remote File allows to connect to an administrative shared folder and retrieve information about a specific file.

Item Name	Full File Name	Property	Local Value
☑ IE Version	C:\Program Files\Internet Explorer\iexplore.exe	File Version	8.0.7600.1...

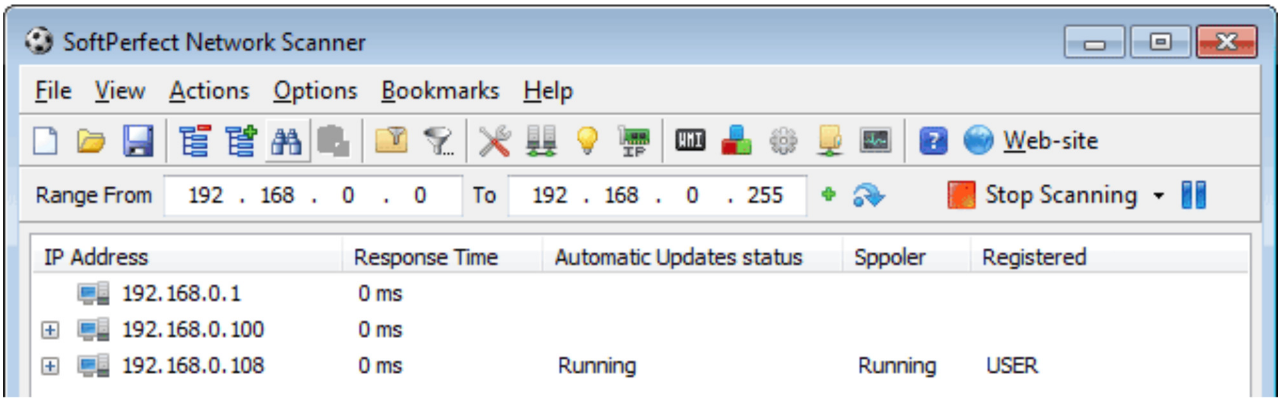
Lastly, you can retrieve information about the status and configuration of a service on remote computers. For example, if you want to make sure that the **messenger** service is up and running, turn the pre-defined item on as shown below. The network scanner will then connect to each computer's service manager and query the information requested.



Remote services allow to connect to a remote computer and retrieve status information about its services.

Item Name	Service Name	Parameter	Local Value
☐ Messenger status	messenger	Status	Service does not exist
☑ Automatic Updates status	wuauserv	Status	Running
☑ Sppoler	Spooler	Status	Running

There will be additional columns showing the information retrieved.

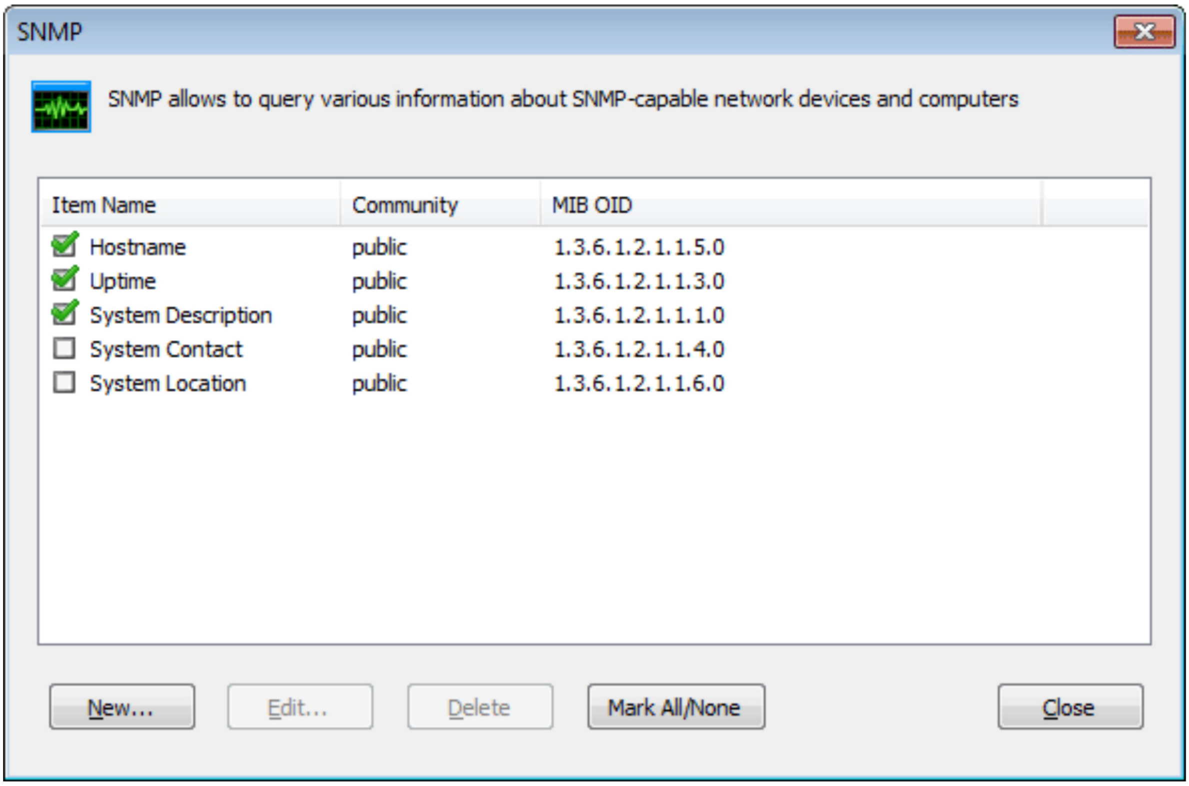

SoftPerfect Network Scanner
File View Actions Options Bookmarks Help
Web-site
Stop Scanning

Range From 192 . 168 . 0 . 0 To 192 . 168 . 0 . 255

IP Address	Response Time	Automatic Updates status	Sppoler	Registered
192.168.0.1	0 ms			
⊞ 192.168.0.100	0 ms			
⊞ 192.168.0.108	0 ms	Running	Running	USER

Remote SNMP query

Network scanner can look for machines that have an SNMP service running. You can specify a community (e.g. public or private) and a MIB OID number. The application automatically determines the type of data received and displays it in a readable form.



SNMP allows to query various information about SNMP-capable network devices and computers

Item Name	Community	MIB OID
☑ Hostname	public	1.3.6.1.2.1.1.5.0
☑ Uptime	public	1.3.6.1.2.1.1.3.0
☑ System Description	public	1.3.6.1.2.1.1.1.0
□ System Contact	public	1.3.6.1.2.1.1.4.0
□ System Location	public	1.3.6.1.2.1.1.6.0

Command line switches

You can use the following switches as **netscan.exe /switch1 /switch2 ... switchN**.

/auto:<filename.[txt|htm|xml|csv]> runs scan with global settings and exports the results to a file, i.e. **/auto**:"c:\desktop\result.txt". Specify a corresponding extension to produce a file of that type. In order to run a scan automatically without exporting to a file, specify **/auto:** with a colon, but without a file name. For example:

```
netscan.exe /hide /auto:"c:\desktop\result.txt"
netscan.exe /hide /auto:"c:\desktop\result.htm"
netscan.exe /hide /auto:"c:\desktop\result.csv"
```

/config:filename.xml loads the specified XML configuration file in the application.

/hide does not show the main window (silent mode).

/load:filename.xml loads the specified XML result set in the application. It is possible to rescan it with the /auto switch.

/cols:col1;col2;col3 applies to the /auto command and exports only the specified columns to a file. Otherwise all visible columns are exported. Example: **/cols**:"Host Name;MAC Address".

/range:From-To Sets an IP address range for scanning. Example: **/range**:192.168.0.1-192.168.10.254.

/append applies to the /auto command for text and CSV files. Appends the results to a file rather than overwrites it.

/wol:MAC sends a Wake-On-LAN magic packet to the specified MAC address and immediately exits. Example: **/wol**:AABBCCDDEEFF.

/wolfile:filename.txt allows you to specify a text file with MAC addresses to wake-up, e.g. **/wolfile**:c:\myfile.txt where the file is a plain text file containing one MAC address per line.

/wakeall sends a WOL packet to all computers configured in the WOL manager and immediately quits.

The two switches below are mutually exclusive and have no effect if the application is launched from a USB stick or other removable device.

/ini forces the scanner to load and save its settings to an INI file instead of the registry by default (see a note below). This switch is obsolete.

/xml forces the scanner to load and save its settings to a XML file instead of the registry by default. However, when the network scanner is launched from a removable drive, such as a USB stick, it does not use the registry. Instead, it stores settings in a XML file, so you need **not** specify this switch to make it portable. Also, If you used the **/ini** or **/xml** switch once, you need not specify it every time. After first use the application will create a configuration file on the disk and will use that file rather than the registry in the future.

/file:filename.txt loads the specified text file and feeds in IP addresses to be scanned. There must be one address or range per line in one of the following notations. Any mismatching lines in the file will be discarded.

Line	Intrerpretatioin
x.x.x.x	Plain IP address
x.x.x.x-y.y.y.y	IP address range
x.x.x.x/y	IP address/mask
x.x.x.x/y.y.y.y	IP address/dotted mask

Product Page / Download