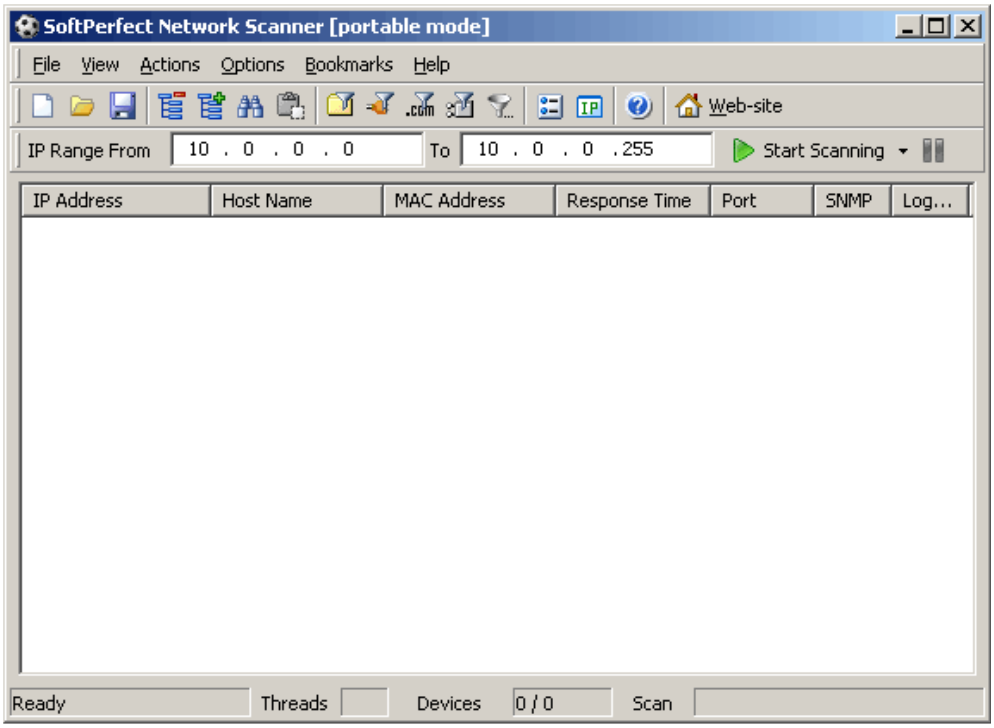
SoftPerfect Network Scanner Online Manual

Product Page / Download

Getting started

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



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

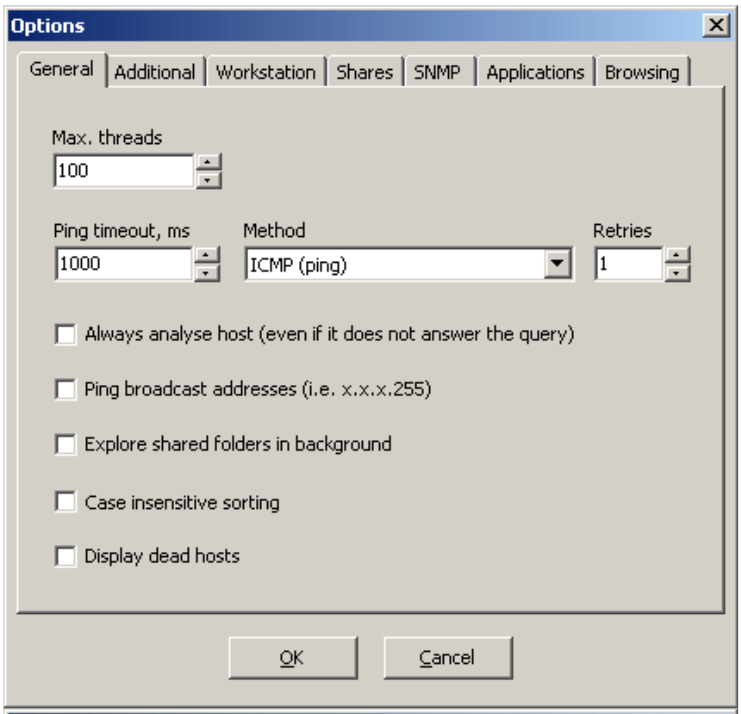
- Clear the display
- Load the scan results from a XML file.
- Save the scan results to a file.
- Expand the results tree.
- Collapse the results tree.
- Search the results tree.
- Paste IP address from the clipboard.
- Apply the shares filter. Only computers with available shared folders are shown.
- Apply the ports filter. Only computers with an open TCP port are shown.
- Apply the host name filter. Only computers with a valid host name are shown.
- Apply the SNMP filter. Only computers with a running SNMP service are shown.
- Open advanced filter panel.
- Program options.

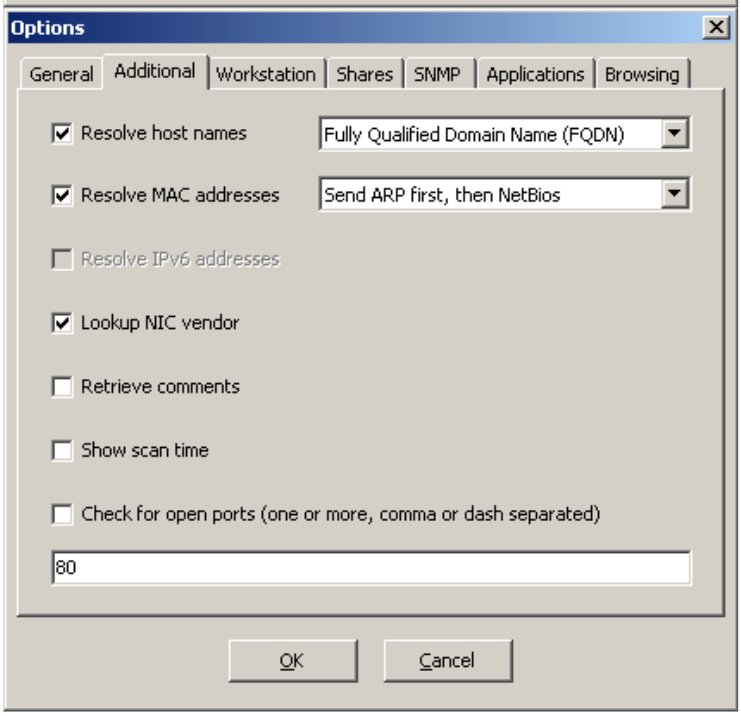
Automatically detect the network configuration.

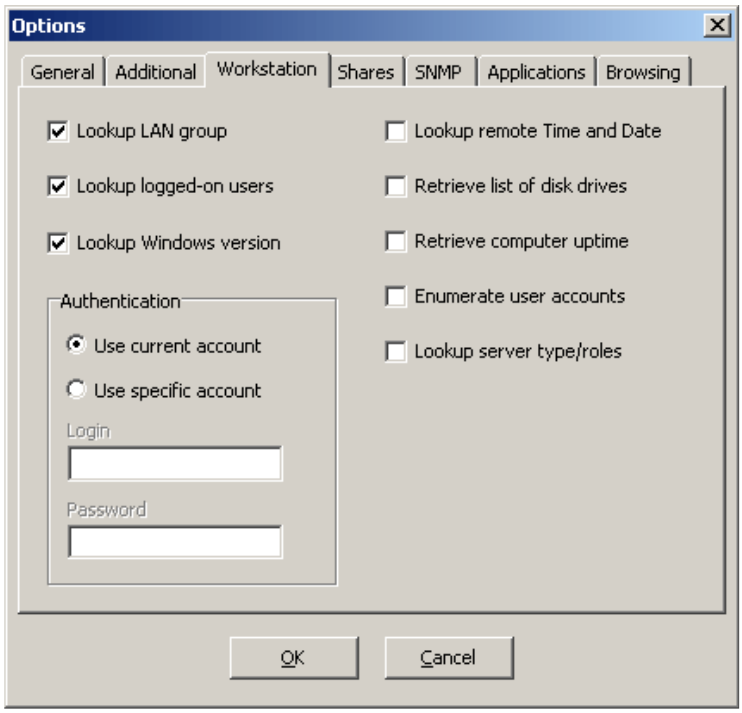
Online Help (this web page).

Program options

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


Options
General
Additional
Workstation
Shares
SNMP
Applications
Browsing
Max. threads
100
Ping timeout, ms
1000
Method
ICMP (ping)
Retries
1
Always analyse host (even if it does not answer the query)
Ping broadcast addresses (i.e. x.x.x.255)
Explore shared folders in background
Case insensitive sorting
Display dead hosts
OK
Cancel


Options
General
Additional
Workstation
Shares
SNMP
Applications
Browsing
Resolve host names
Fully Qualified Domain Name (FQDN)
Resolve MAC addresses
Send ARP first, then NetBios
Resolve IPv6 addresses
Lookup NIC vendor
Retrieve comments
Show scan time
Check for open ports (one or more, comma or dash separated)
80
OK
Cancel



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.

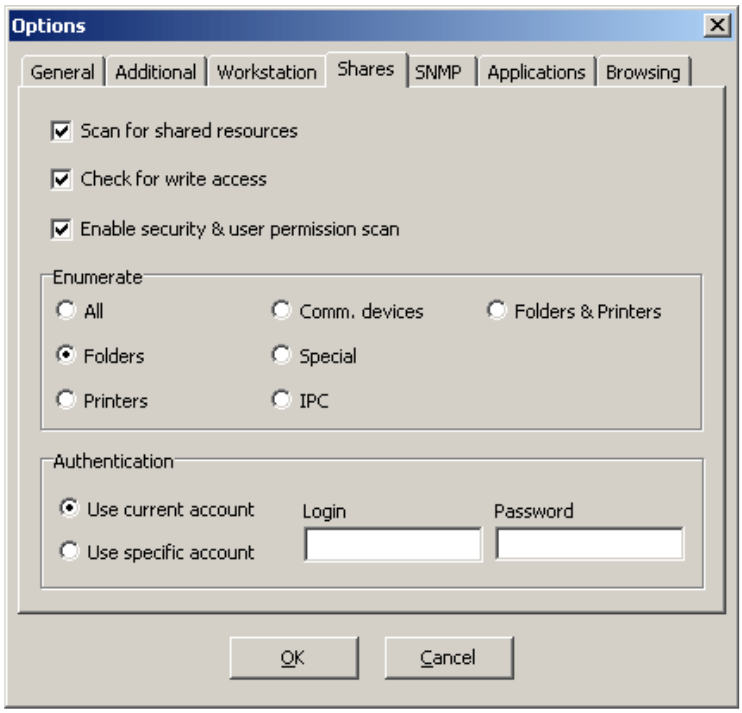
On the **Additional** tab:

- **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.
- **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.
- **Check for open ports** - when enabled, the program will attempt connection to the specified TCP port (you can specify several ports separated by a comma or dash, e.g. 21,80,110-115).
- **Retrieve comments** - displays a comment assigned to a Windows workstation.
- **Show scan time** - shows the time when the host was last scanned.

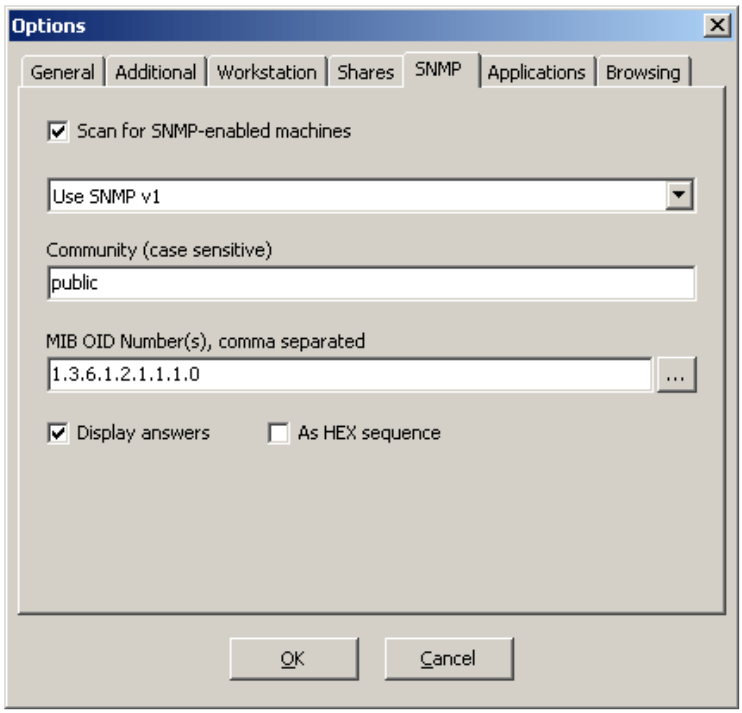
On the **Workstation** tab:[1]

- **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.

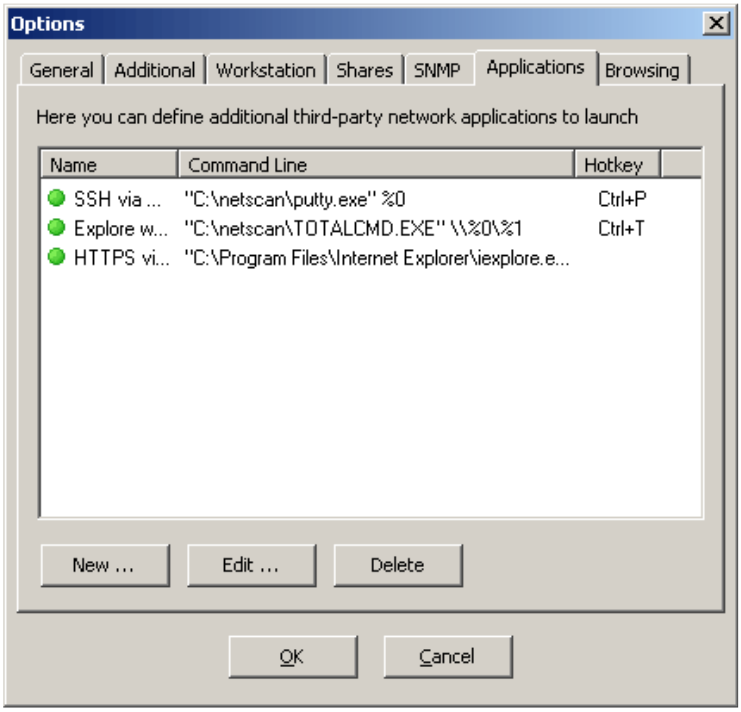


- **Scan for shared resources** - enables scanning of shared resources. Below are all the possible types of shared resources.
- **Check for write access** - when enabled, the program determines if the shared folder is writable or not (read only).
- **Enable security & user permission scan** - with this 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.
- **All** - all resources.
- **Folders** - shared folders or drives.
- **Printers** - shared print devices.
- **Comm. device** - a communication device.
- **Special** - special share reserved for interprocess communication (IPC$) or remote administration of the server (ADMIN$). It can also be used for administrative shares such as C$, D$, E$, etc.
- **IPC** - interprocess communication (IPC).

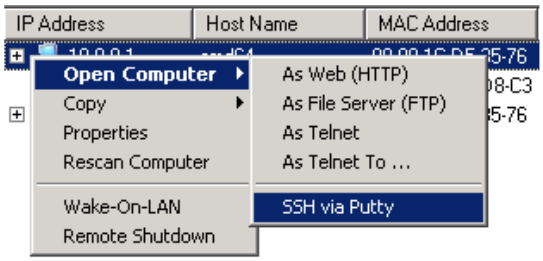


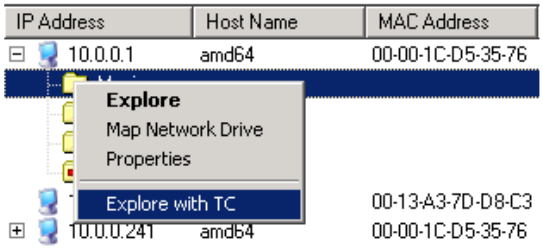
Use this tab to setup scanning for machines that have an SNMP service running. You can specify a community (e.g. public or private) and a MIB OID number. Multiple communities and/or OIDs are to be comma separated. This data will

be used for an SNMP query. Set the **Display answers** option if you would like to see replies from the SNMP enabled machines. The **As HEX sequence** option prints an SNMP answer as a string of hexadecimal numbers rather than a raw string output.



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.

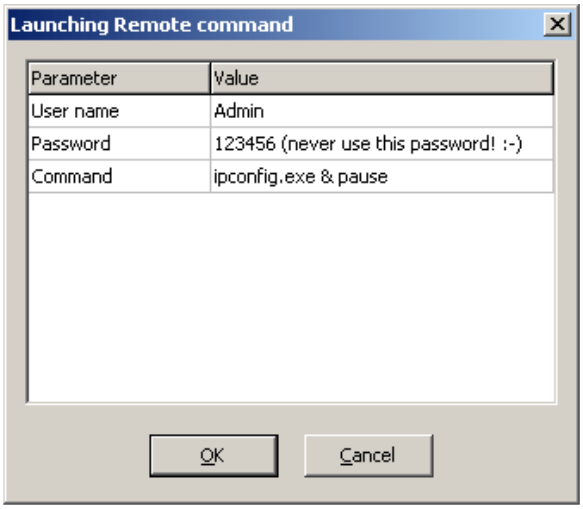




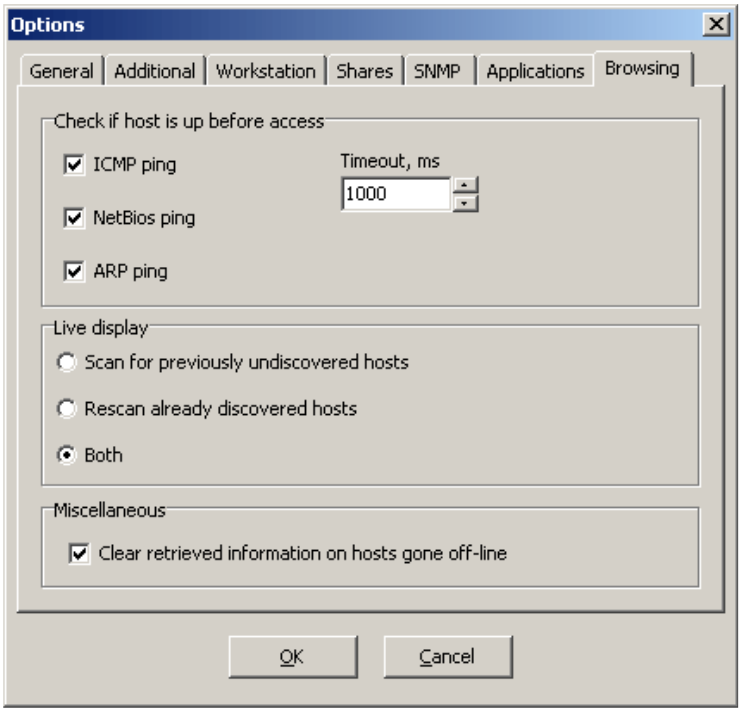
Should you require to pass extra arguments upon launching an application, you can use user-prompted parameters specified in braces. As an example, the following line lets you quickly execute commands on the remote system with **PsExec** from SysInternals.

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.

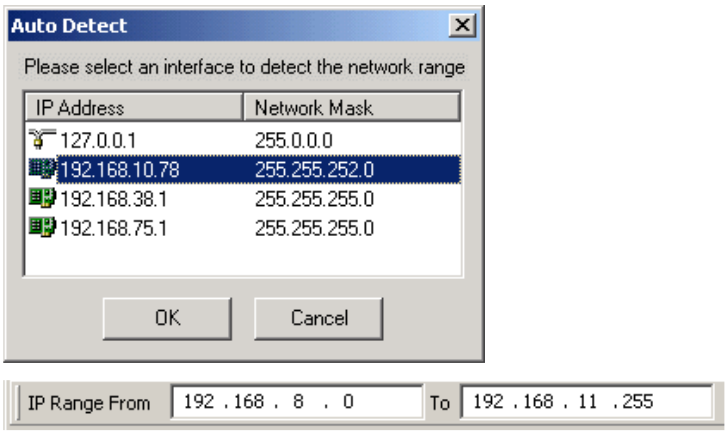


Finally, the **Browsing** tab enables the network scanner to check whether a host is still on-line when you attempt to explore its folders, or establish a connection to that host. This greatly speeds up some operations, as an attempt to connect an off-line computer might temporarily hang the network 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.



Auto-detect the network configuration

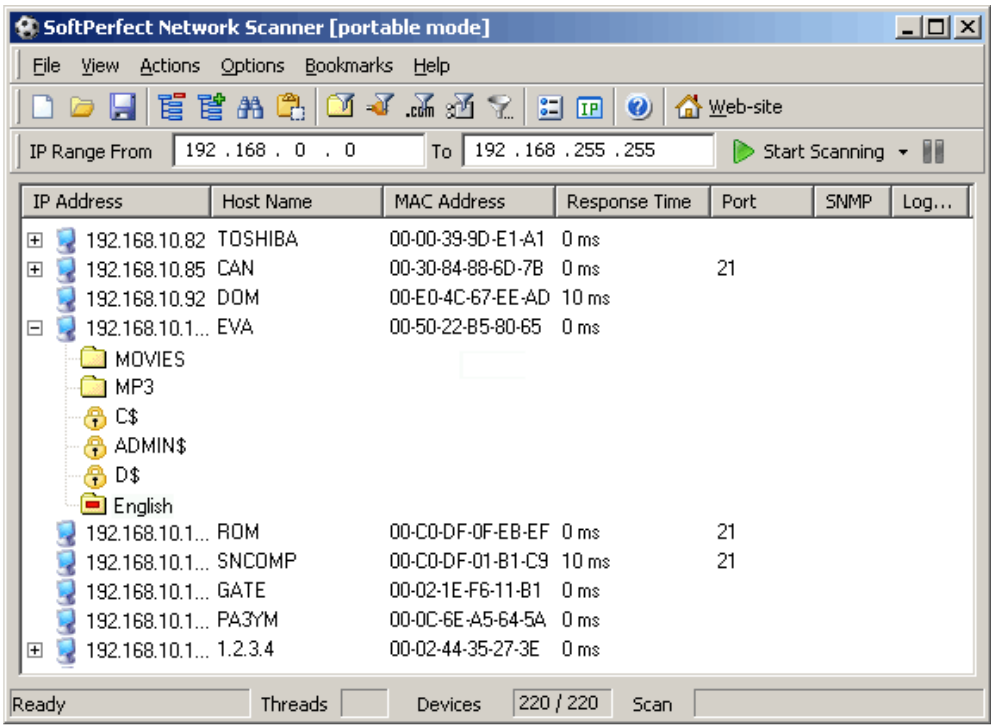
The SoftPerfect Network Scanner is able to detect your IP range automatically. Select the **Options - IP Address - Detect Local IP Range** menu item. In the following dialog, select an interface and the program will calculate the IP range of the network. If you are connected to the Internet and are behind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



In this example SoftPerfect Network Scanner has determined the range of IP addresses on the network

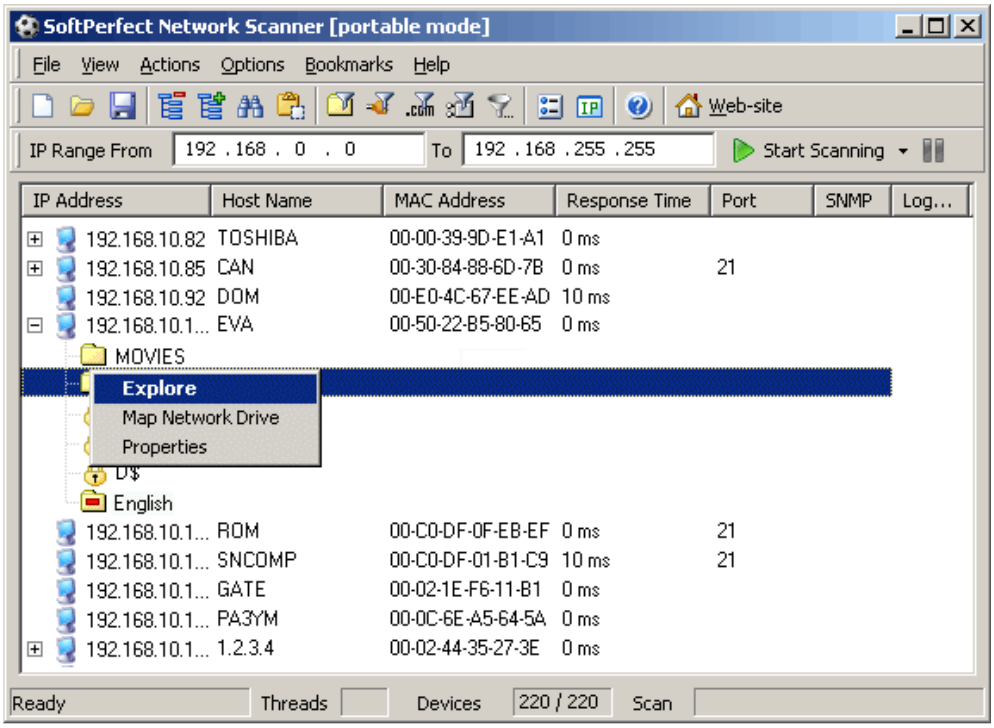
Scanning

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



Scan results

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

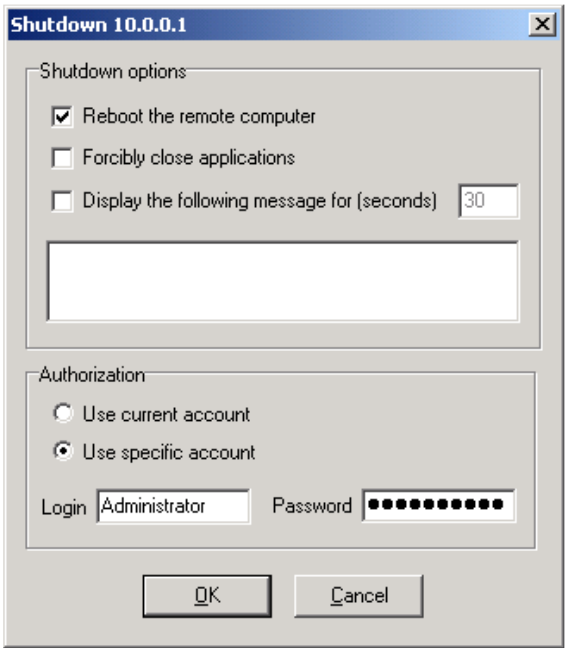


Live display

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 logged in the display window.

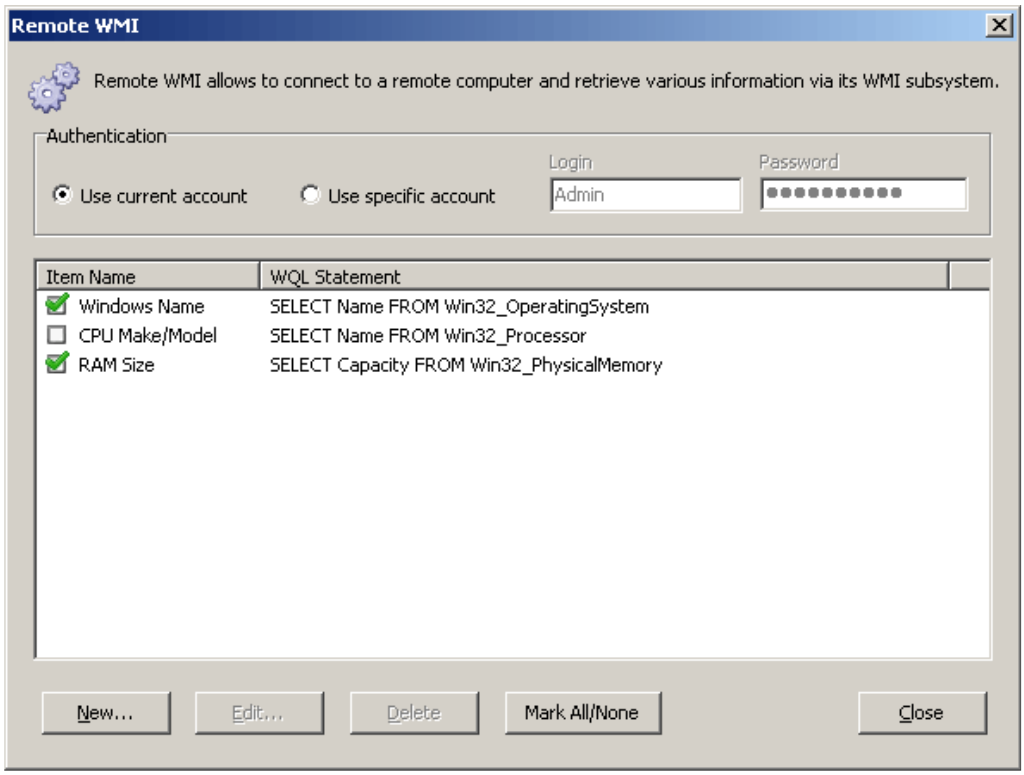
Wake-on-LAN and remote shutdown

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**.

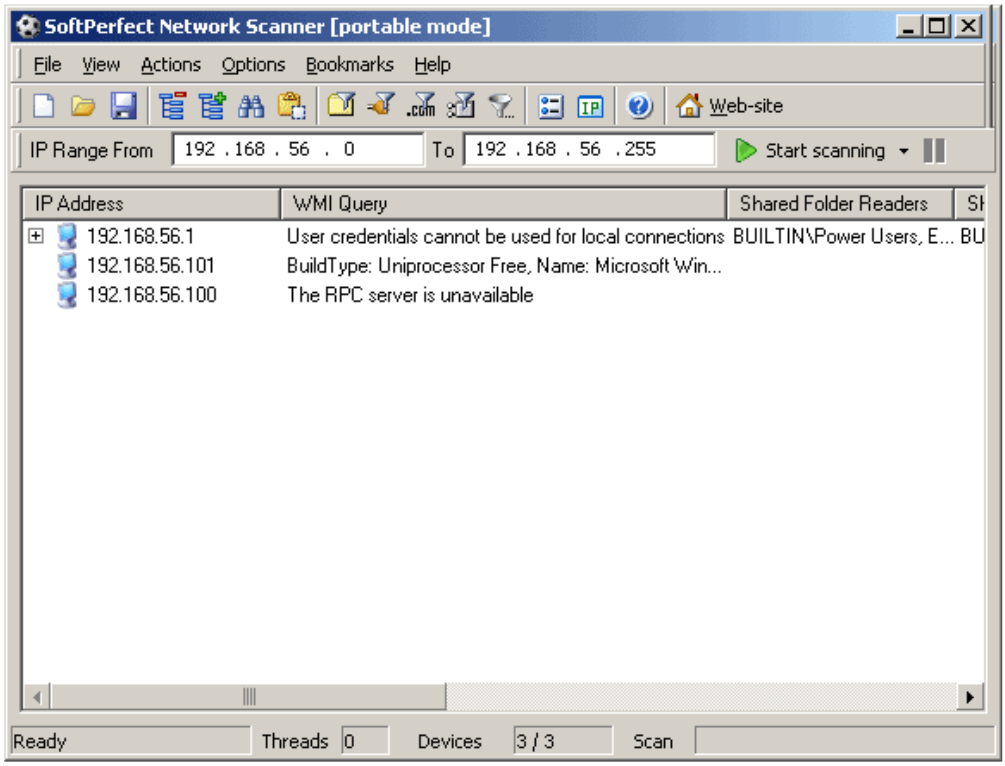


WMI Query builder and scanning

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.



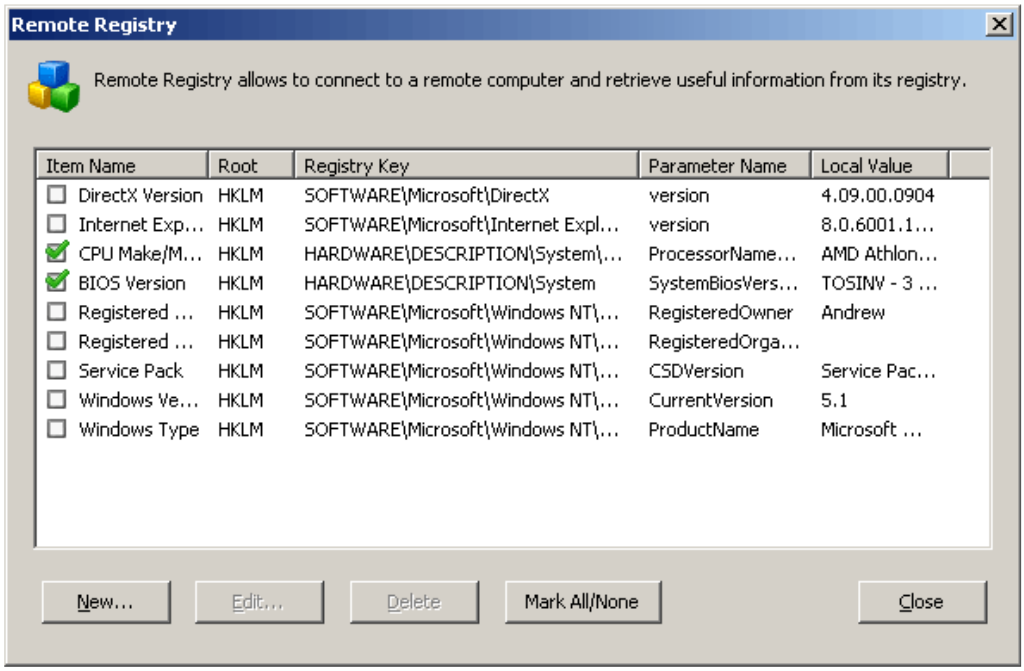
The **New** button allows you to easily construct simple WQL queries. It merely connects to your computer's WMI subsystem and lets you pick a WMI class and parameter to be used in the query. When you have one or more WMI queries enabled, there will be additional columns shown in the scan results.



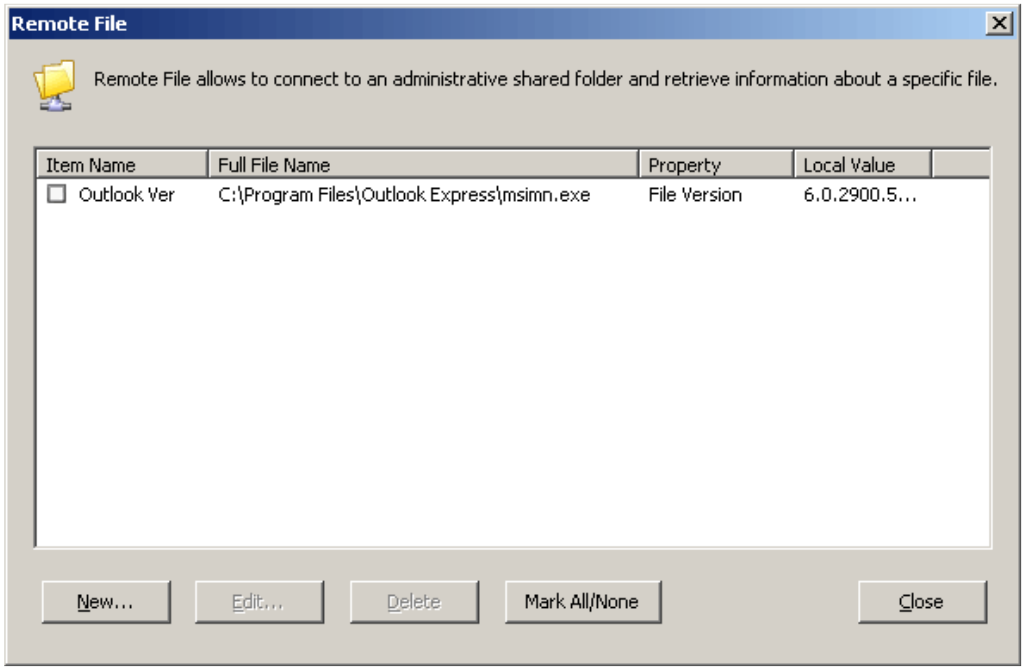
Remote file, registry and services

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.

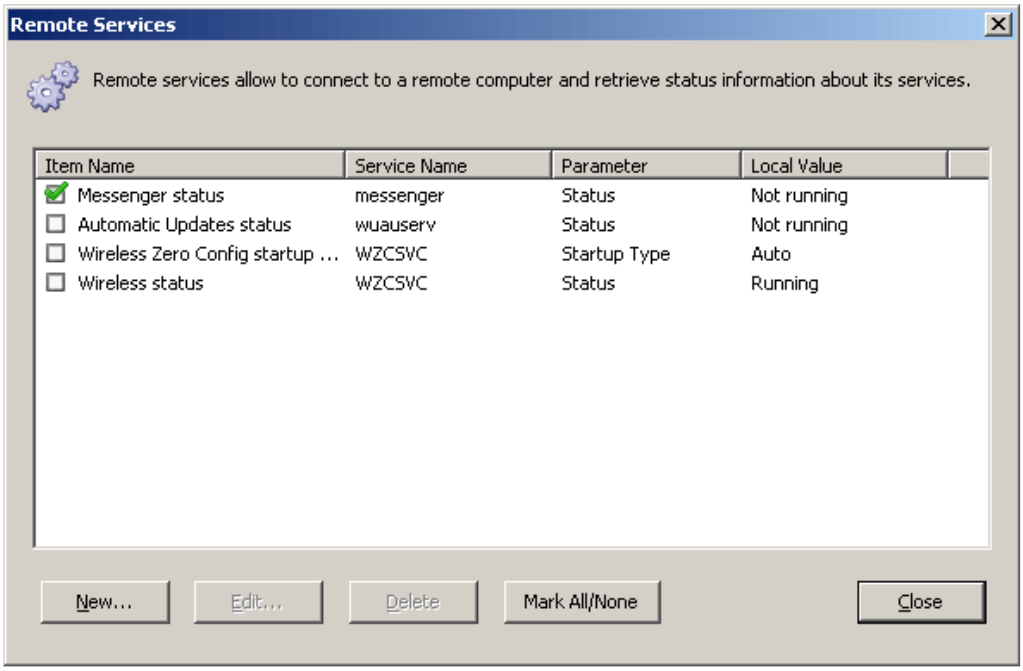
There are several predefined entries in the list and you can easily add new items to retrieve data about hardware and software specific to your environment. The columns are as follows: **Item Name** is a name of the entry. **Root** represents one of the root registry hives. **Registry key** contains 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 two items are chosen to be retrieved from remote computers.



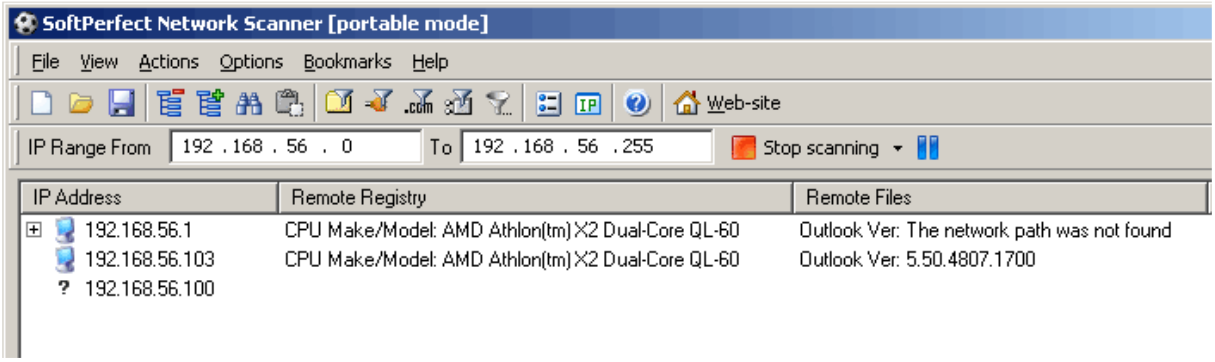
Likewise, provided the administrative shares are enabled and accessible, you can pull out information about a specific file on remote computers. For example, you want to find out the version of Internet Explorer, or when a log file changed, or how large a particular file is. To do so, enter the full name of a file and choose what property you would like to retrieve. On the following screenshot, the application is configured to access the Outlook Express 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$\Program Files\Outlook Express\msimn.exe, **10.0.0.2**\C$\Program Files\Outlook Express\msimn.exe, etc.



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.



There will be additional columns showing the information retrieved.



Remote shutdown and power off

In order to shutdown or power off 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*.

Command line switches

You can use the following switches as **netscan.exe /switch1 /switch2 ... switchN**. For instance, if you need to scan your network and export the list to the file, use the following command line:
netscan.exe /hide /auto:"c:\desktop\result.txt"

/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 the .htm extension in order to produce a HTML report. Specify the .xml extension in order to to export the results to a XML file. Specify the .csv extension to in order to export the results to a CSV file. In order to run a scan automatically without exporting to a file, specify **/auto:** with a colon, but without a file name.

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

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

/addr applies to the /auto command and exports only the MAC and IP address columns to a file.

/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.

These two switches below are mutually exclusive and have no effect if the application is launched from a USB stick or other removable device. Use a shortcut to apply either switch at all times if it is needed.

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

/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 uses a XML file to save/load its settings, so you need **not** specify this switch to make it portable.

Product Page / Download