

# SOPHOS

## SafeGuard PortAuditor 3.20

### User help

Document date: March 2010



## Important Notice

This user help is delivered subject to the following conditions and restrictions:

- This user help contains proprietary information belonging to Sophos. Such information is supplied solely for the purpose of assisting explicitly and properly authorized SafeGuard PortAuditor users.
- No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic or mechanical, without the express prior written permission of Sophos.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- The software described in this user help is furnished under a license. The software may be used or copied only in accordance with the terms of that agreement.
- Information in this help is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.
- The information in this document is provided in good faith but without any representation or warranty whatsoever, whether it is accurate, or complete or otherwise and on express understanding that Sophos shall have no liability whatsoever to other parties in any way arising from or relating to the information or its use.
- SafeGuard PortProtector and SafeGuard PortAuditor are OEM versions of Safend Protector and Safend Auditor from Safend. Therefore some screenshots throughout this manual may still contain the Safend branding but mean the same as within the SafeGuard OEM version.

© Copyright 2010 Sophos. All rights reserved.

Other company and brand products and service names are trademarks or registered trademarks of their respective holders.



## About This User Help

This user help is comprised of the following chapters:

- **Chapter 1, Introducing SafeGuard PortAuditor**, page 5, introduces the SafeGuard PortAuditor solution. It describes its features and benefits, in particular the new features.
- **Chapter 2, Installing SafeGuard PortAuditor**, page 8, describes the system requirements for installing the product and the installation process.
- **Chapter 3, Auditing**, page 13, describes how to perform audit scans, along with all the filters and settings available. Also described are the options for viewing scan results and explanations about the various fields in the reports.
- **Appendix A, Acquiring a License Key**, page 28, describes the steps you need to take in order to purchase and install an update for the product.
- **Appendix B, Command Line Automation**, page 30, describes how to use command line switches to automatically configure and run SafeGuard PortAuditor scans.

## Contents

1	Introducing SafeGuard PortAuditor .....	5
2	Installing SafeGuard PortAuditor .....	8
3	Auditing.....	13
4	Appendix A - Acquiring a License Key .....	28
5	Appendix B - Command Line Automation.....	30

# 1 Introducing SafeGuard PortAuditor

## About This Chapter

This chapter introduces the SafeGuard PortAuditor solution, describes how it works and outlines the main features of the product. It contains the following sections:

- **The Current Situation**, page 6, describes the threat of information leakage that has left a gaping hole in the data security of today's organizations.
- **The SafeGuard PortAuditor Solution**, page 6, describes SafeGuard PortAuditor's solution for providing enterprise-wide visibility on the usage of physical and wireless ports on endpoints.
- **Main Features**, page 7, describes the product's main features, in particular the new features added in this version.

## 1.1 The Need

Enterprise networks are currently characterized by a proliferation of easily accessible computer ports, such as USB, FireWire and PCMCIA. In addition, a variety of communication adapters (such as Bluetooth, IrDA and WiFi) and device types (such as storage devices, printers, digital cameras, smart phones and PDAs) all enable effortless access to endpoints using these ports and devices.

These devices enable optimal accessibility and productivity, but they leave endpoints wide open to infiltration. With the amount of corporate data residing on endpoints estimated at over 60%, endpoints may be the most valuable, and vulnerable, part of the enterprise network.

At this moment dozens of devices may be connected to your network. Consider the following questions:

- Do you know what is connected?
- Can you identify these devices?
- Are they permitted or are they trespassing into your company's integrity?
- Are you equipped to locate the security breach and identify the intruder?

## 1.2 The SafeGuard PortAuditor Solution

With SafeGuard PortAuditor you can immediately begin capturing critical data that provides you with instant answers to the 'who and what' regarding USB, FireWire and PCMCIA ports in your organization. It also helps you recognize which WiFi networks your endpoints have connected to.

SafeGuard PortAuditor is a non-intrusive, clientless software solution that captures the critical data that you need from each port. SafeGuard PortAuditor creates reports about devices currently connected to your network, as well as those previously connected. As an added convenience, SafeGuard PortAuditor can export these reports to MS Excel files, pre-configured with the most commonly used queries.

## 1.3 Main Features

SafeGuard PortAuditor includes the following main features:

- A Clientless Solution – with no administrative commitment, you can run it now and receive answers in a matter of minutes.
- Run the audit on your entire network or on selected computers or groups only.
- Multiple scan protocols allow easy operation in various environments (SetupDI and WMI).
- Scan for all types of devices, on both internal and external ports including WiFi networks.
- Enables reliable and precise device identification.
- Various audit filters allowing better focus on desirable types of activity.
- Immediate HTML and MS Excel reports.
- Fully complements the Sophos Group policy enforcement product – SafeGuard PortProtector.
- Easy-to-use interface - following installation, auditing your network is only one step away: just choose the computers to be queried, and start the audit.

## 2 Installing SafeGuard PortAuditor

### About This Chapter

This chapter first describes the process of installing the product on your computer:

- **System Requirements**, page 9, describes supported operating systems and installation prerequisite software.
- **Installing SafeGuard PortAuditor**, page 10, describes the installation process.
- **Uninstalling SafeGuard PortAuditor**, page 12, describes how to remove the product from your computer.

## 2.1 System Requirements

### Operation requirements:

- Client OS**
- Windows 2000 Professional (Service Pack 3-4)
  - Windows 2000 Server (Service Pack 3-4)
  - Windows 2000 Advanced Server (Service Pack 3-4)
  - Windows XP Professional (Service Pack 0-2)
  - Windows 2003 Server (Service Pack 0-1, R2)
  - Windows Vista

- Domain OS**
- Windows 2000 Server (Service Pack 0-4)
  - Windows 2000 Advanced Server (Service Pack 0-4)
  - Windows 2003 Server (Service Pack 0-1, R2)
- SafeGuard PortAuditor supports an Active Domain based scan

- Credentials**
- Credentials should allow access to the registry data on all target computers (typically Domain Administrator privileges)

### Report Viewing Requirements:

- Software**
- Internet Explorer version 6.0 and up
  - For viewing reports in MS Excel - Microsoft Excel version 2003 and up

## 2.2 Installing SafeGuard PortAuditor

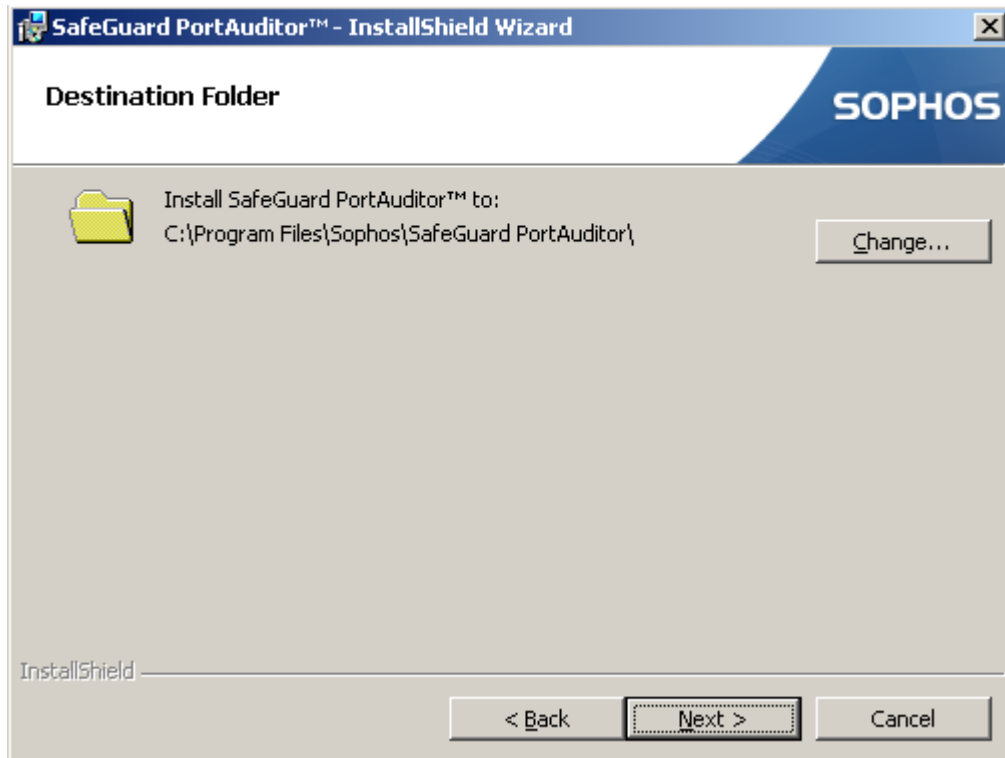
To install SafeGuard PortAuditor:

- 1 Locate the 'SafeGuardAuditor.msi' file on the SafeGuard PortAuditor CD.
- 2 Double-click it to install the SafeGuard PortAuditor on the local computer. The *Welcome* window opens:

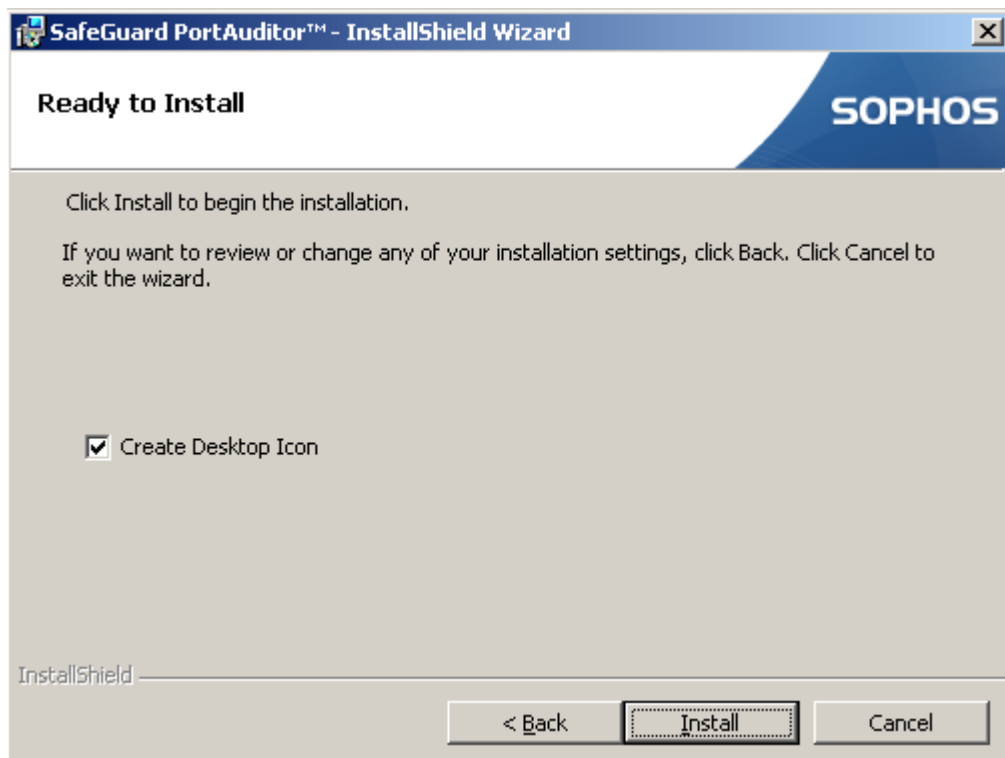


- 3 In the Welcome window, click Next. The *License Agreement* window opens.

- 4 Check the license agreement check box and click Next. The *Destination Folder* window appears:



- 5 If you wish to change the destination folder, click **Change** and select a folder.
- 6 Click **Next**. The *Ready to Install* window opens:



- 7 If you wish, check the **Create Desktop Icon** checkbox.

- 8 Click **Install** to begin the installation. A progress bar is displayed until the installation process is completed, at which point the *InstallShield Wizard Completed* window opens.
- 9 You may check or uncheck the **Launch SafeGuard PortAuditor** checkbox, then click **Finish** to complete the installation.

### 2.2.1 Registration

Depending on how you obtained your copy, the Auditor installation is valid for 30 days or 5 uses before registration. After 30 days/5 uses, a registration is required.

To acquire a license key, please contact your local reseller or contact us at [sales@sophos.com](mailto:sales@sophos.com).

Refer to *Appendix A*, page 28 to learn about how to acquire a license key.

## 2.3 Uninstalling SafeGuard PortAuditor

In order to uninstall SafeGuard PortAuditor, you can either select **Uninstall SafeGuard PortAuditor** from your computers **Start** menu → **Programs**, use **Add or Remove Programs** in your Control Panel or double-click the *SafeGuardAuditor.msi* file on the CD.

To complete the uninstall procedure follow the instructions in the window that opens.

## 3 Auditing

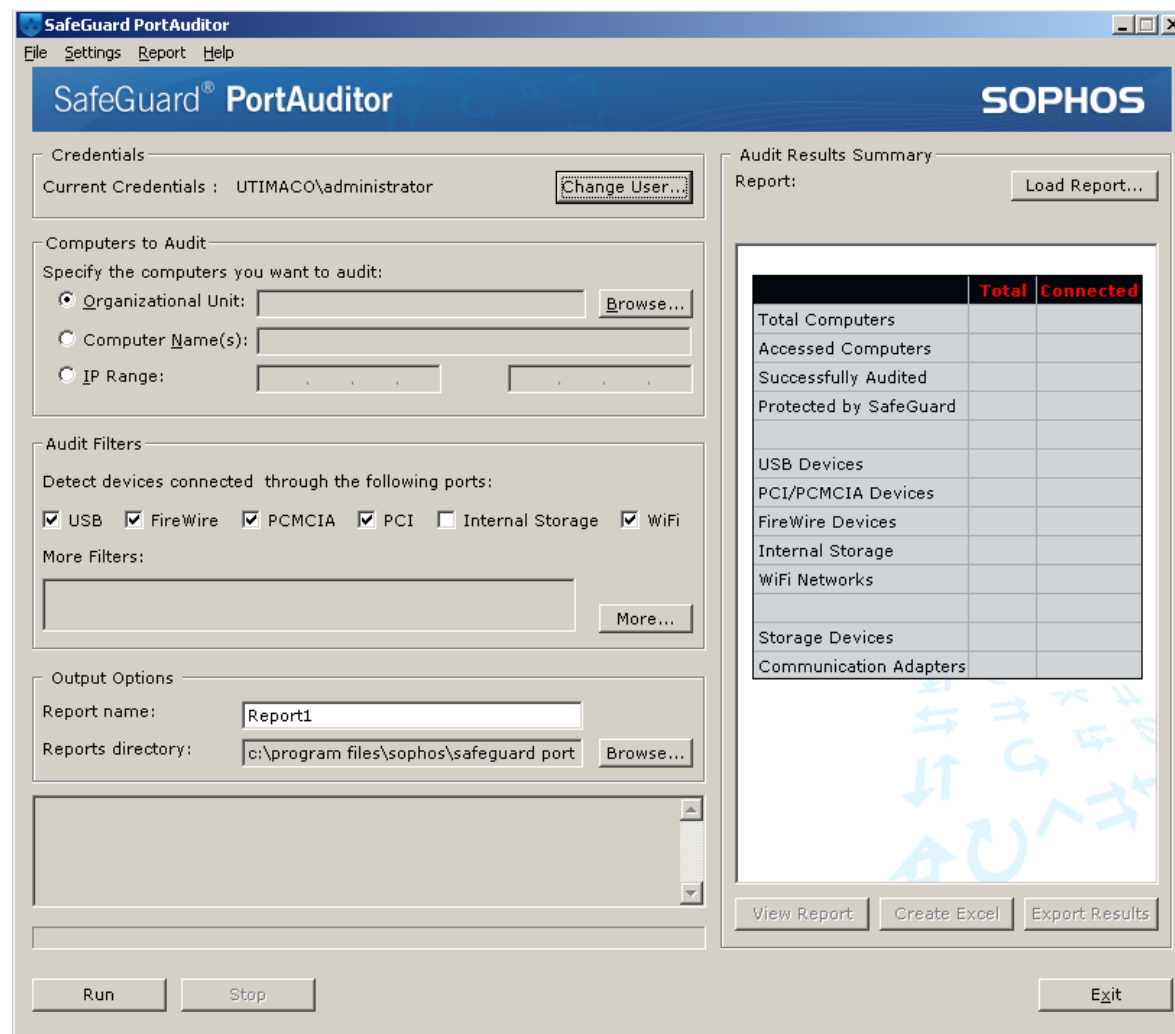
### About This Chapter

This chapter describes how to use SafeGuard PortAuditor to scan for devices in your network. It contains the following sections:

- **Using SafeGuard PortAuditor**, page 14, provides an overview of the application's main window.
- **Selecting Audit Protocol**, page 14, describes the audit protocols you can choose from.
- **Setting Credentials**, page 15, describes how to set the user account to one with sufficient privileges.
- **Selecting Target Computers**, page 16, describes how to determine the computers to be included in the scan.
- **Audit Filters**, page 17, describes the various audit filters available. These help you optimize the scan so as to include only relevant data.
- **Selecting Output Destination**, page 20, describes how to change the default audit output folder.
- **Performing the Audit**, page 20, describes how to initiate and track an audit.
- **Analyzing Audit Results**, page 22, describes the available audit report types.
- **Exporting Audit Results**, page 26, describes how to export the audit results in order to import them to SafeGuard PortProtector Management Console.

### 3.1 Using SafeGuard PortAuditor

After launching SafeGuard PortAuditor (either by double-clicking its desktop shortcut or via your computer's Start menu), the main window opens:



The left part of the window is for audit options settings and audit execution. The right part of the window is for the scan summary and result viewing.

### 3.2 Selecting Audit Protocol

In order to perform the audit scans remotely on endpoints, SafeGuard PortAuditor needs to communicate with these endpoints using remote access protocols which allow it to remotely access the registry of Microsoft Windows based machines.

The default scan protocol is **Setup API**. This protocol is typically enabled on computers, and requires the following:

- **Remote Registry** service running on the endpoints
- **File and print sharing** enabled on the endpoints' network cards
- Port 445 (TCP) OR port 139 (TCP) open in the firewall/personal firewall
- Local administrative privileges on the endpoint

**Note:** The SetupAPI protocol is not suitable to audit Windows Vista endpoints. Use WMI instead.

An additional scan protocol, WMI, may be useful if the endpoints in your network do not allow File and print sharing or do not run the Remote Registry service. This is the main protocol used today for controlling and monitoring Windows based machines. WMI requires the following:

- WMI service running on the endpoints
- WMI communications open on the firewall/personal firewall (these require port 135 and a randomly picked port from a set of ports defined in the registry of the endpoint)
- Local administrative privileges on the endpoint

It is recommended that you perform a test scan in order to determine which of the protocols is most suitable for your environment.

**To set the audit protocol:**

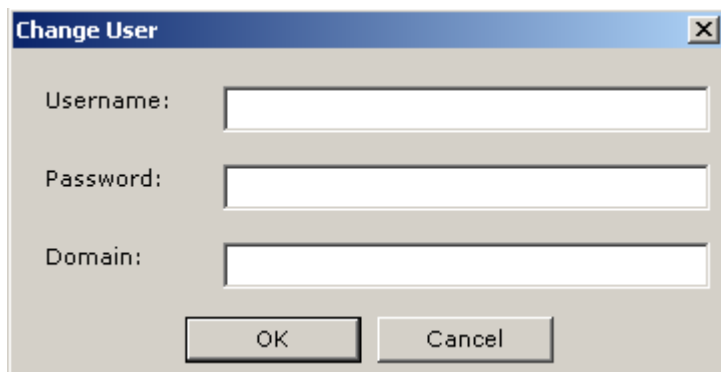
From the *Settings* menu, select **Scan Protocol** and check the desired protocol.

### 3.3 Setting Credentials

Credentials should allow access to registry information on all the target endpoint computers. Without proper credentials, data collection will fail. A typical user that would have such access is the Domain Administrator.

**To change credentials:**

- 1 In the *Credentials* section of the main window, click **Change User**, or select **Change User** from the *Settings* menu. The *Change User* window opens:



- 2 Enter the Username, Password and Domain, and click **OK**. The new credentials are now in effect.

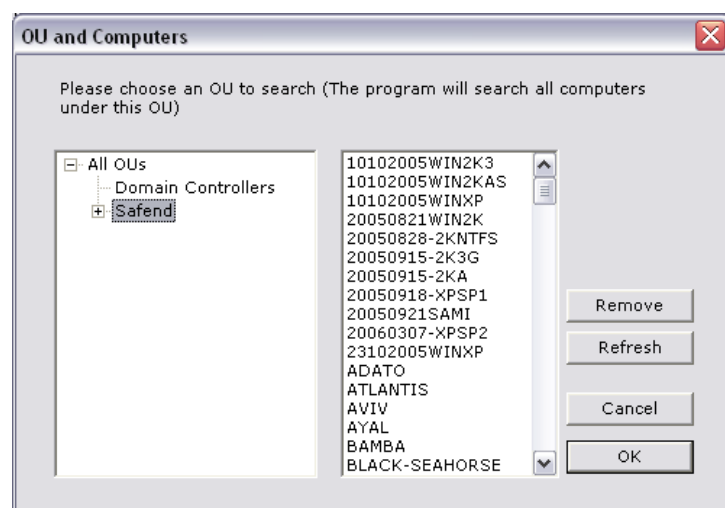
### 3.4 Selecting Target Computers

The next step after setting proper credentials is to select the endpoint computers to be audited. This is done in the *Computers to Audit* section of the main window. Three types of audits are available:

- By Organizational Unit (OU)
- By specific computer(s)
- By IP range

**To audit by organizational unit:**

- 1 Click the *Organizational Unit* radio button (or press **Alt+O**) and click **Browse**. The *OU and Computers* window is displayed.



**Note:** You may need Domain Administrator credentials in order to access this tree and view it. If you have not done so already, change the credentials and try again.

A list of all the available Organizational Units is displayed on the left pane, while the right one displays the computers belonging to the selected OU.

You may exclude certain computers within a selected OU from being audited by selecting them and then clicking **Remove**. The audit will be performed on the entire organizational unit excluding computers that were removed.

- 2 Click **OK** to complete the OU selection.

**To audit by specific computers:**

Click the *Computer Name(s)* radio button (or press **Alt+N**) and type in the names of the computers you wish to audit, separated by commas.

If you wish to audit the computer from which you are running the audit, type in the word "local" (before you type in any names, "local" appears by default).

### 3.4.1 IP Addresses Range Audit

Click the **IP Range** radio button (or press **Alt+I**) and type in the IP range you would like to audit in the two fields that follow (lowest address on the left, highest address on the right).

**Note:** When scanning by IP range, this may include certain IP addresses that are not currently assigned. Upon scanning, the Auditor ignores such IP addresses and moves on to the next one in the range.

## 3.5 Audit Filters

After selecting the target computers you can further filter the auditing process to include or exclude specific ports, previously connected devices or specific device types/WiFi network types. This is done from the *Audit Filters* section, as described below.

### 3.5.1 Device Port

SafeGuard PortAuditor supports scanning of the following endpoint ports:

- USB
- FireWire
- PCMCIA
- PCI
- Internal Storage - includes internal hard disks connected over IDE, SATA, SCSI etc.
- WiFi – includes all the networks to which the endpoint has connected (SSID, MAC of the Access Point and encryption/authentication schemes)

By default when you open the application, USB, FireWire, PCMCIA and WiFi are selected to be audited.

**To include/exclude a port from the audit:**

Check/uncheck the port checkbox.

**Note:** When using WMI for auditing it is not possible to distinguish between devices connected over PCMCIA and PCI.

**Important:** WiFi auditing only includes networks that are/were connected through Windows standard WiFi support (WZC). Endpoints with non-Windows managed WiFi cards cannot be audited (i.e. will not produce any results).

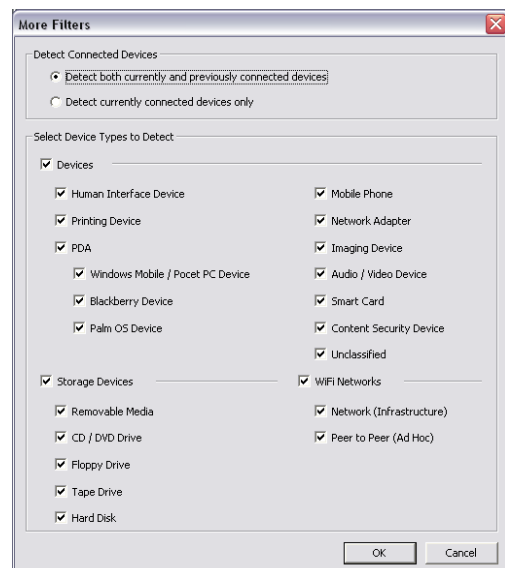
It is also not possible to distinguish between WiFi networks that the computer is currently connected to and those to which it was connected in the past. For this reason the audit results display "n/a" in the "connected" field.

## 3.5.2 Additional Filters

You can specify additional filters (device types, storage device types, WiFi networks) for your audit. You do this in the *More Filters* window.

**To specify additional filters:**

Click **More...** The *More Filters* window appears:



### 3.5.2.1 Detect Connected Devices

You can choose the audit report to include only devices connected to endpoints at the time of the scan, or devices previously connected as well.

**To include only the devices currently connected:**

In the *Detect Connected Devices* section, click the **Detect currently connected devices only** radio button.

**To include both currently connected and previously connected devices:**

In the *Detect Connected Devices* section, click the **Detect both currently and previously connected devices** radio button (this radio button is selected by default).

**Note:** This definition does not filter WiFi networks, since it is not possible to distinguish between WiFi networks that the computer is currently connected to and those to which it was connected in the past.

### 3.5.2.2 Device Types

You can further limit the audit results to include only specific device types or WiFi networks. This is useful when you are only interested in specific device/network types (e.g. removable media), or not interested in a specific device type (e.g. keyboard and mouse).

Device types include:

- Devices (non-storage)
  - 1 Human Interface Device (keyboards, mice, joysticks etc.)
  - 2 Printing Device
  - 3 PDA
  - 4 Windows Mobile / Pocket PC Device
  - 5 Blackberry Device
  - 6 Palm OS Device
  - 7 Mobile Phone
  - 8 Network Adapter
  - 9 Imaging Device
  - 10 Audio/Video Device
  - 11 Smart Card
  - 12 Content Security Device (tokens and dongles aimed for software licensing etc.)
  - 13 Unclassified (to include devices which do not fall under any of the above categories)
- Storage Devices
  - 1 Removable Media (includes Disk On Keys and removable hard disks)
  - 2 CD/DVD Drive
  - 3 Floppy Drive
  - 4 Tape Drive
  - 5 Hard Disk (internally attached)
- WiFi Networks
  - 1 Network (infrastructure)
  - 2 Peer to Peer (ad hoc)

To exclude a device type or a WiFi network type:

Uncheck the checkbox for the devices/storage device/networks you wish to exclude, and click OK. If you have made any changes to the default selection (all selected) the message "Detect only selected device types" appears in *Audit Filters* section's **More Filters** field.

## 3.6 Selecting Output Destination

Before you perform the audit, you must set a folder in which the output data and the formatted results will be stored. You do this in the *Output Options* section.

### 3.6.1 Report Name

Each time you perform a scan and create an audit report, SafeGuard PortAuditor also creates a folder in which to store all the report's files and data. The folder takes its name from the name you assign to the report. The results are saved in an HTML page called *AuditRes.html* which is found in the report folder. By default, the report (and folder) name is set to 'Report1'.

Near this file you can find the *AuditRes.xml* file, which can be used when creating a security policy with the Sophos policy enforcement product – SafeGuard PortProtector. By uploading the file to the Protector Management Console you can determine which of the devices in it should be approved and which should be blocked for use.

**Note:** Saving a report under an existing name overwrites the data.

### 3.6.2 Reports Directory

This field allows you to choose the directory in which the report folders and reports will be created. By default, the Auditor uses – *C:\Program Files\Sophos\SafeGuard PortAuditor\Audits*.

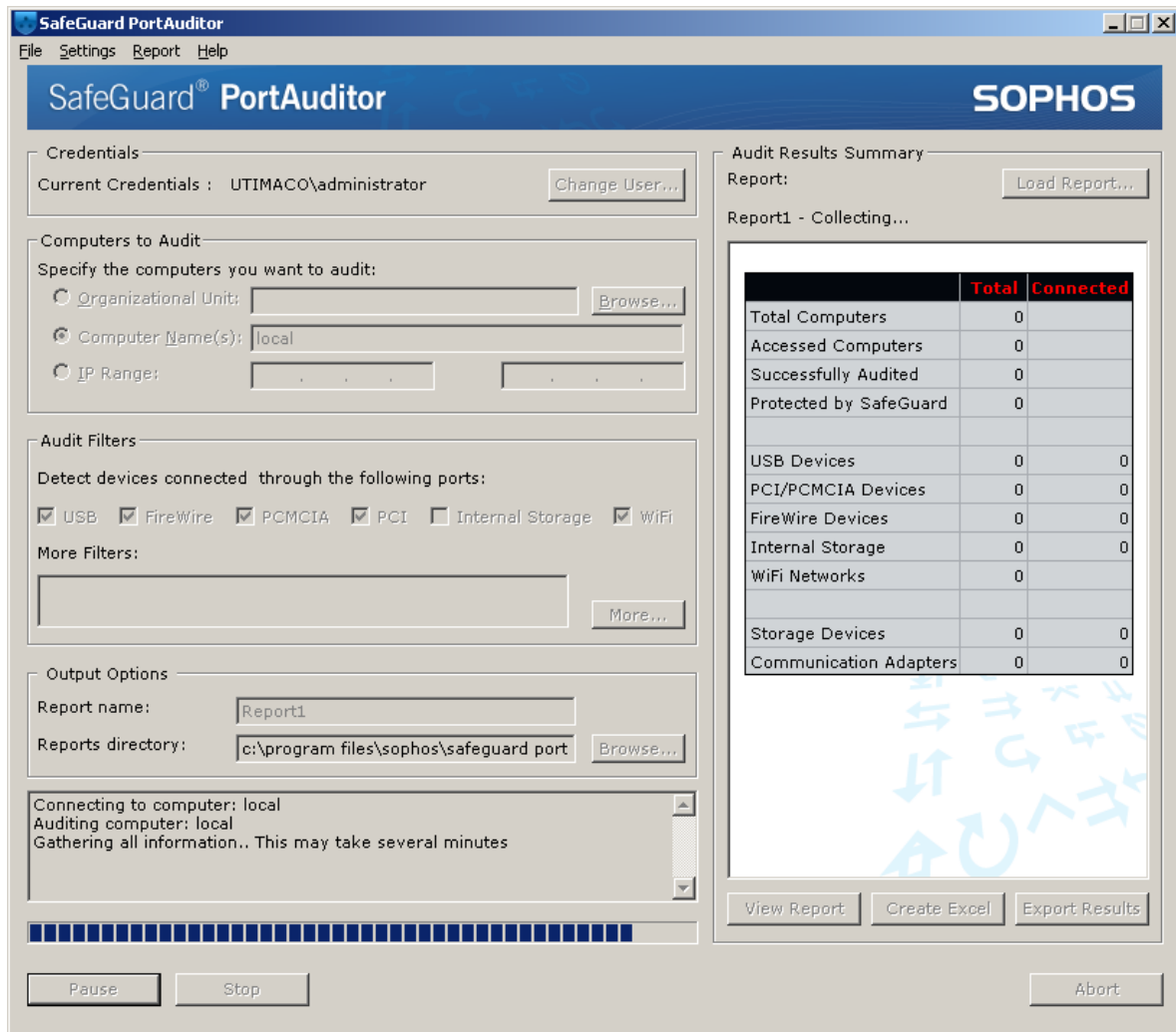
## 3.7 Performing the Audit

Once you have defined target computers, audit filters and output destination, you are ready to begin the audit.

**To begin the audit:**

After you have selected the computer/computers to be audited and the report name and destination, click **Run**.

The audit process begins and the Auditor starts retrieving the data from the selected computers. This process may take seconds or minutes, depending on the size of your network and the number of audited computers. You may view the audit progress in the audit log in the *Output Options* section on the left hand side and in the audit progress bar at the bottom of in the main window. You will also notice that the *Audit Results Summary* section on the right hand side of the main window is updated as the audit progresses.



After the audit process begins, the **Run** button changes to **Pause**. You may click it to temporarily stop the audit process. After you click the **Pause** button it changes to **Resume**. Click it to continue the audit process. While the audit is in progress you may click the **Stop** button to completely cease the audit process. The audit results are available for viewing (and exporting) once the audit process is complete (whether or not you used the **Stop** button) and while the audit is paused.

**Note:** While the scan is in progress, **Pause**, **Resume** and **Stop** may take several seconds to take effect.

### 3.8 Analyzing Audit Results

While the audit is in progress, the *Audit Results Summary* section on the right hand side of the main window is constantly updated, displaying the current audit data. When the audit is completed (or stopped/paused) you may view the results over Internet Explorer (**View Report** button), create a customizable Excel report (**Create Excel** button) or export the result to XML file for further use (**Export Results** button).

**Note:** These three buttons are available only when the audit is complete, stopped or paused.

The screenshot shows the SafeGuard PortAuditor application window. The main window title is "SafeGuard PortAuditor" and the logo "SOPHOS" is visible in the top right. The interface is divided into several sections:

- Credentials:** Current Credentials: UTIMACO\administrator. A "Change User..." button is present.
- Computers to Audit:** Specify the computers you want to audit. Options include:
  - Organizational Unit: (empty field) with a "Browse..." button.
  - Computer Name(s): local (selected).
  - IP Range: (empty fields).
- Audit Filters:** Detect devices connected through the following ports:
  - USB
  - FireWire
  - PCMCIA
  - PCI
  - Internal Storage
  - WiFi
 More Filters: (empty field) with a "More..." button.
- Output Options:**
  - Report name: Report1
  - Reports directory: c:\program files\sophos\safeguard port (with a "Browse..." button)
- Status Log:**
  - Gathering all information.. This may take several minutes
  - Write data to file: c:\program files\sophos\safeguard portauditor\Audits\Report1
  - Checked 1 Computers.
  - Got information from 1 Computers.
  - Audit finished successfully
- Audit Results Summary:**
  - Report: Report1 (with a "Load Report..." button)
  - A table showing the results of the audit:

The table in the Audit Results Summary section is as follows:

	Total	Connected
Total Computers	1	
Accessed Computers	1	
Successfully Audited	1	
Protected by SafeGuard	0	
USB Devices	1	0
PCI/PCMCIA Devices	9	8
FireWire Devices	0	0
Internal Storage	0	0
WiFi Networks	0	
Storage Devices	0	0
Communication Adapters	1	1

At the bottom of the Audit Results Summary section, there are three buttons: "View Report", "Create Excel", and "Export Results".

At the bottom of the main window, there are "Run" and "Stop" buttons on the left, and an "Exit" button on the right.

### 3.8.1 Viewing Audit Results

The simplest way to view the audit results is in HTML format.

To view audit results in HTML format:

On the bottom of the right hand side pane, click **View Report**. A browser window appears, with the full report data:

The screenshot shows a browser window titled "SafeGuard PortAuditor - Microsoft Internet Explorer". The address bar shows the path to the report file. The report content includes a header with the Sophos logo and the product name "SafeGuard® PortAuditor". Below this is an "Audit Summary Report" table and a "Device Audit Report" table.

**Audit Summary Report**

	Total	Connected
Total Computers	1	
Accessed Computers	1	
Successfully Audited	1	
Protected by SafeGuard	0	
USB Devices	1	0
PCI/PCMCIA Devices	9	8
FireWire Devices	0	0
Internal Storage Devices	0	0
WiFi Networks	0	
Storage Devices	0	0
Communication Adapters	1	1

[Computer Audit Report](#)

[Device Audit Report](#)

Device Audit Report [Show each device / WiFi network only once](#)

Computer	User	Connected	Port	Type	Device Type	Description / Network	Device Info	Vendor Name	Vendor	Model
1 local	UTIMACO\administrator	+	USB	Device	Smart Card	CardMan 3x21	Smart Card Reader USB	OmniKey AG	076B	3021
2 local	UTIMACO\administrator	+	PCI/PCMCIA	Device	Unclassified	LSI Logic PCI-X Ultra320 SCSI Host Adapter	PCI bus 0, device 16, function 0	Speed Tech Corp.	1000	0030
3 local	UTIMACO\administrator	+	PCI/PCMCIA	Adapter	Network	VMware Accelerated AMD PCNet Adapter	PCI bus 0, device 17, function 0	Shinko Shoji Co., Ltd	1022	2000
4 local	UTIMACO\administrator	+	PCI/PCMCIA	Device	Unclassified	Multimedia Audio Controller	PCI bus 0, device 18, function 0		1274	1371
5 local	UTIMACO\administrator	+	PCI/PCMCIA	Device	Unclassified	VMware SVGA II	PCI bus 0, device 15,		15AD	0405

**Note:** Internet Explorer 6.0 or a newer version must be installed in order to view the results in HTML.

**Note:** If you are using Windows XP SP2 and above, the active content of the report may be blocked by your browser. To view the report, click on the warning bar that appears in your browser and select **Allow Blocked Content**. Your security will not be compromised in any way.

The report includes three tables:

- Audit Summary Report
- Device Audit Report
- Computer Audit Report

### 3.8.1.1 Audit Summary Report

The summary report includes the following *rows*:

- **Total Computers** – The total number of computers specified to be audited.
- **Accessed Computers** – The number of computers that were online and reachable.
- **Successfully Audited** – The number of computers in which the audit process was feasible and executed.
- **Protected by SafeGuard** – The number of computers on which SafeGuard PortProtector is installed.
- The total number of devices/WiFi networks connected to the various ports (**USB, PCI/PCMCIA, FireWire, Internal Storage, WiFi**).
- The total number of **Storage Devices** and **Communication Adapters** connected to the various ports.

The summary table includes two *columns*:

- **Total** – total number of devices/WiFi networks/storage devices/network adapters connected both previously and at the time of the audit.
- **Connected** - total number of devices/WiFi networks/storage devices/network adapters connected at the time of the audit.

### 3.8.1.2 Device Audit Report

Each record in the report includes the following:

- **Computer** – The name of the audited computer
- **User** – The last user logged on to the audited computer (at audit time)
- **Connected** – Whether or not the device is currently connected. Currently connected devices are highlighted in green.
- **Port** – USB, FireWire, PCMCIA/PCI, Internal Storage ports, WiFi
- **Type** – Device (non-storage), storage, WiFi, Adapter (communication)
- **Device Type** – Device type (e.g. human interface device, removable media)
- **Description/Network** – Device description, as taken from the device itself. In the case of WiFi, this field contains the network name (SSID)
- **Device Info** – Additional information available on the device.
- **Vendor** – Vendor ID number extracted from the device.
- **Vendor Name** - Vendor Name, based on the Vendor ID extracted from the device
- **Model** – Product ID number extracted from the device.
- **Distinct ID** –unique serial number extracted from the device. In the case of WiFi, this field contains the MAC address of the access point.
- **Details** – In the case of devices, displays the port subtype in PCMCIA and FireWire. In the case of WiFi, displays the encryption/authentication schemes.

### 3.8.1.3 Computer Audit Report

Each record in the table includes the following:

- **Computer** – The name of the audited computer
- **User** – The last user logged on to the audited computer
- **SafeGuard Protection Status** – here you can see whether or not the computer is protected by SafeGuard PortProtector and whether or not the computer was available for auditing:
  - 1 **Protected** – The computer was successfully audited and SafeGuard PortProtector is installed.
  - 2 **Not Protected** - The computer was successfully audited and SafeGuard PortProtector is not installed.
  - 3 **Audit Failed** – The computer was visible and online, but the audit could not be performed, either because credentials were insufficient or because it was blocked by the audited computer (e.g. by the audited computer's firewall).
  - 4 **Unreachable** – The computer was completely unavailable (switched off, offline, does not exist etc.)

You may sort the results based on any one of the columns by clicking its heading in the header row. An additional click toggles the sort order from ascending to descending and back.

Additionally, the HTML report allows you to filter results to display each device only once. Click the **Show each device/WiFi network only once** link above the table to filter the report. To revert back to the full report, click **Show every occurrence of device/WiFi network**.

### 3.8.2 Viewing Audit Results in Excel

The Auditor may export the collected results to a formatted Microsoft Excel file, which allows you to analyze the audit results using the full power of Excel.

**To view the Excel report:**

Click **Create Excel**. An Excel file with the name AuditRes.xls is created in the folder where the results of the current scan are stored.

**Note:** This feature requires Microsoft Excel 2003 to be installed on the same machine on which the report is generated.

**Note:** It is important to allow the Excel creation process to fully complete and not to interfere with it. This process may take several seconds or minutes, depending on the number of records in your report.

Once the process is complete, the Excel report opens:

Computer	User	Connected	Port	Type	Device Type	Description / Network	Details
Hayh	HA\YHray	X	USB	Storage	Removable Media	USB Mass Storage Device	
Hayh	HA\YHray	X	USB	Storage	Removable Media	USB Mass Storage Device	
Hayh	HA\YHray	X	USB	Adapter	Network	Wireless USB Adapter	
Hayh	HA\YHray	X	USB	Device	Human Interface Device	Microsoft USB Wheel Mouse Optical	
Hayh	HA\YHray	X	USB	Device	Human Interface Device	USB Human Interface Device	
Hayh	HA\YHray	X	USB	Device	Unclassified	USB Composite Device	
Hayh	HA\YHray	X	USB	Device	Audio / Video Device	USB Audio Device	
Hayh	HA\YHray	X	USB	Device	Human Interface Device	USB Human Interface Device	
Hayh	HA\YHray	X	USB	Device	Unclassified	USB Composite Device	
Hayh	HA\YHray	X	USB	Device	Audio / Video Device	USB Audio Device	
Hayh	HA\YHray	X	USB	Device	Human Interface Device	USB Human Interface Device	
Hayh	HA\YHray	X	USB	Device	Unclassified	Aladdin USB Key	
Hayh	HA\YHray	X	USB	Device	Unclassified	Hitachi Pro (4.1.5.3)	
Hayh	HA\YHray	X	USB	Storage	Removable Media	USB Mass Storage Device	
Hayh	HA\YHray	X	USB	Storage	Removable Media	USB Mass Storage Device	
Hayh	HA\YHray	X	USB	Storage	Removable Media	USB Mass Storage Device	
Hayh	HA\YHray	X	USB	Adapter	Network	SigmaTel USB-UDA Dongle	
Hayh	HA\YHray	X	USB	Storage	Removable Media	USB Mass Storage Device	
Hayh	HA\YHray	X	USB	Storage	Removable Media	USB Mass Storage Device	
Hayh	HA\YHray	X	USB	Storage	Removable Media	USB Mass Storage Device	
Hayh	HA\YHray	X	USB	Storage	Removable Media	USB Mass Storage Device	
Hayh	HA\YHray	X	USB	Storage	Removable Media	USB Mass Storage Device	
Hayh	HA\YHray	X	USB	Adapter	Network	Motorola SurfBoard 4200 USB Cable Modem	
Hayh	HA\YHray	X	USB	Storage	Removable Media	USB Mass Storage Device	
Hayh	HA\YHray	X	USB	Storage	Removable Media	Siigalink USB personal storage device	

The tables in the Excel report are identical to those of the HTML view, although they are arranged in a different order.

You may easily filter the data based on any of the available columns, using the  button in the column heading in the header row (mark the header row to make the button appear).

### 3.9 Exporting Audit Results

SafeGuard PortAuditor enables you to export audit results to an XML file and store the file wherever you wish. This file can be opened by Microsoft Excel and any other XML reader application.

To export audit results:

Click **Export Results**. The *Export Results* window opens.

In the *Export Results* window, select the destination folder, type in the file name and click **Save**.

- 1 Click *Export Results*. The *Export Results* window opens.
- 2 In the *Export Results* window, select the destination folder, type in the file name and click **Save**.

**Note:** Exporting a report is very useful when performing large audits, since it can save you the time needed to open the results in Excel.

**Note:** If you wish to use an audit report for importing devices to SafeGuard PortProtector Management Console, please refer to *Selecting Output Destination*.

### 3.10 Viewing and Exporting Previous Audit Results

In addition to viewing the latest report, with the latest scan results, you can also view reports generated earlier. In order to do so, you need to load the report (if you simply want to view the report in HTML format, you can also do so by simply double-clicking it from Internet Explorer).

To load previously created reports:

- 1 From the top of the right pane, click **Load Report**

OR

From the *File* menu, select **Load report**.

- 2 The report is loaded into the Auditor, and can now be viewed in HTML/Excel format or exported, as explained above.

**Note:** Only the HTML reports are available for loading.

## 4 Appendix A - Acquiring a License Key

Depending on the way you obtained your copy, the Auditor installation is valid for 30 days or 5 uses before registration. After 30 days/5 uses, a registration key is required (as shown in the image below).

As long as you are not registered, this message appears notifying you how much time you have before the evaluation period is over. Once the evaluation expires, the following window appears:



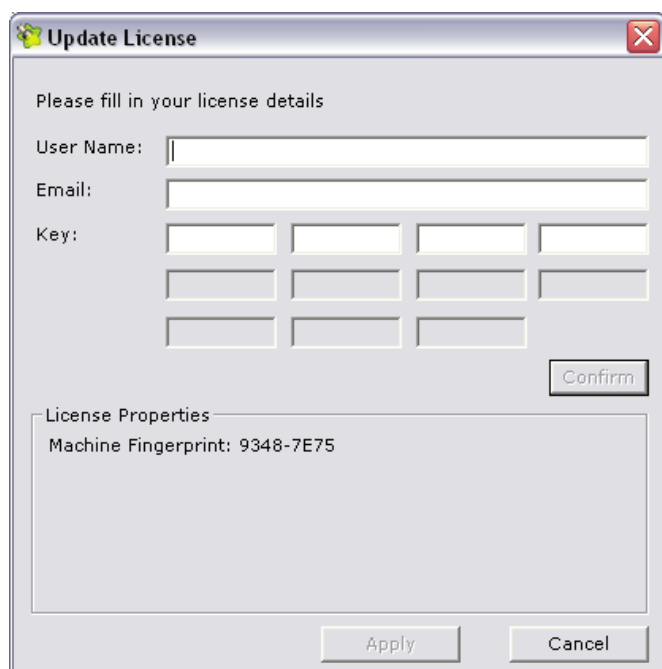
You may check your license status at any given time in the *Help* menu, under **License**.

### To acquire a license key:

Contact your local reseller or contact us at [sales@sophos.com](mailto:sales@sophos.com). Once you have obtained your license key, you can enter it.

### To enter a license key:

- 1 In the *License Alert – Evaluation* window, click **Enter License Key**.  
The *Update License* window opens:



2 In the *Update License window*, enter the following details which you have received with your license:

- User Name
- Email Address
- Key

**Note:** If you have obtained your copy of the product via the Sophos web site, or received an evaluation CD, you may be required to provide a machine fingerprint (see previous figure) in order to acquire a license.

3 Click **Confirm**. A license confirmation message appears and your product is licensed.

## 5 Appendix B - Command Line Automation

On some occasions, you may want to run the Auditor with a pre-configuration or to schedule audits.

This can be achieved by running the Auditor from the command line. Find the Auditor.exe file on your computer (typically installed in c:\Program Files\Sophos\SafeGuard PortAuditor) and run it from the command line with the following switches.

Syntax:

```
Auditor.exe [/ip | /ou | /comp] [options]
```

The following options are available:

<u>Switch</u>	<u>Description</u>
<i>/a</i>	Start scan automatically
<i>/comp computer1, computer2, ...</i>	List of computers to scan
<i>/ip lower_ip:upper_ip</i>	IP range to scan
<i>/ou name</i>	Scan an OU (e.g. /ou SOPHOS\Computers)
<i>/nousb</i>	Don't scan USB devices
<i>/nopcmcia</i>	Don't scan PCMCIA devices
<i>/nofirewire</i>	Don't scan FireWire devices
<i>/nowifi</i>	Don't scan wireless network
<i>/pci</i>	Scan PCI devices
<i>/connected</i>	Scan only connected devices (default is off)
<i>/internal</i>	Scan internal storage devices

<i>/filter type1, type2, ...</i>	Do not scan the specified device types
<i>/u user:password@domain</i>	Scan using specified credentials
<i>/wmi</i>	Scan using WMI (default is Setup API)
<i>/report path</i>	Path to report file

Available filter types (localizable, case insensitive):

<u>Type</u>	<u>Description</u>
Device	Filter all devices
HID	Filter human interface devices
Printing	Filter printing devices
PDA	Filter all PDAs
PocketPC	Filter PocketPC PDAs
Blackberry	Filter Blackberry PDAs
Palm	Filter Palm OS PDAs
Phone	Filter mobile phone devices
Network	Filter network devices
AV	Filter audio/video devices
Imaging	Filter imaging devices
SmartCard	Filter Smart Card devices

<b>Content</b>	Filter content security devices
<b>Unclassified</b>	Filter unclassified devices
<b>Storage</b>	Filter all storage devices
<b>Removable</b>	Filter removable storage devices
<b>CD</b>	Filter CD/DVD drives
<b>Floppy</b>	Filter floppy drives
<b>Tape</b>	Filter tape drives
<b>Disk</b>	Filter hard disk drives
<b>Wifi</b>	Filter all WiFi network types
<b>AP</b>	Filter Access Point WiFi Networks
<b>P2P</b>	Filter Peer to Peer WiFi Networks