

SAFEND AUDITOR™

USER GUIDE

Version 3.6.1

IMPORTANT NOTICE

This guide is delivered subject to the following conditions and restrictions:

- This guide contains proprietary information belonging to Safend Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized Safend Protector 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 expressed prior written permission of Safend Ltd.
- 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 guide is furnished under a license. The software may be used or copied only in accordance with the terms of that agreement.
- Information in this guide 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 with the expressed understanding that Safend Ltd. shall have no liability whatsoever to other parties in any way arising from or relating to the information or its use.

Copyright ©2005-2019
Safend Ltd. All rights reserved.
Other company and brand products and service names are trademarks or registered trademarks of their respective holders.

About This Guide

This User's Guide is comprised of the following chapters:

- ***Chapter 1, Introducing Safend Auditor***, introduces the Safend Auditor solution. It describes its features and benefits, in particular the new features.
- ***Chapter 2, Installing Safend Auditor***, describes the system requirements for installing the product and the installation process.
- ***Chapter 3, Auditing***, 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.
- ***Acquiring a License Key***, describes the steps you need to take in order to get FREE license for the product.

safend
Securing Your Endpoints

TABLE OF CONTENTS

Introducing Safend Auditor 5
The Need 6
The Safend Auditor Solution 6
Main Features 7

Installing Safend Auditor 8
System Requirements 9
Installing Safend Auditor 10
Registration 12
Uninstalling Safend Auditor 12

Auditing 13
Using Safend Auditor 14
Selecting Audit Protocol 14
Setting Credentials 15
Selecting Target Computers 15
IP Addresses Range Audit 16
Audit Filters 17
Device Port 17
Additional Filters 18
Detect Connected Devices 18
Device Types 19
Selecting Output Destination 20
Report Name 20
Reports Directory 20
Performing the Audit 21
Analyzing Audit Results 22
Viewing Audit Results 23
Audit Summary Report 23
Device Audit Report 24
Computer Audit Report 25
Viewing Audit Results in Excel 26
Exporting Audit Results 27
Viewing and Exporting Previous Audit Results ..... **Error! Bookmark not defined.**

Acquiring a License Key 28

Introducing Safend Auditor

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

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

The Need

Enterprise networks characterized by a proliferation of easily accessible computer and laptop 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 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?

The Safend Auditor Solution

With Safend Auditor 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.

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

Main Features

Safend Auditor 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.
- WMI scan protocols
- 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 "Auditor Report Viewer" and XML MS Excel reports.
- Fully complements Safend's policy enforcement product – Safend Data Protection Suite.
- 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.

Installing Safend Auditor

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

- ***System Requirements***, describes supported operating systems and installation prerequisite software.
- ***Installing Safend Auditor***, describes the installation process.
- ***Uninstalling Safend Auditor***, describes how to remove the product from your computer.

System Requirements

Operation requirements:

Client OS	❖ Windows 7 x64 ❖ Windows 8.1 x86 ❖ Windows 10 x64 ❖ Windows Server 2008 R2 x32 / x64 ❖ Windows Server 2012 R2
Domain OS	❖ Windows 2003 Server ❖ Windows 2008 Server ❖ Windows 2012 Server Safend Auditor supports an Active Domain based scan
Credentials	Credentials should allow access to the registry data on all target computers (typically, Domain Administrator privileges are preferred).

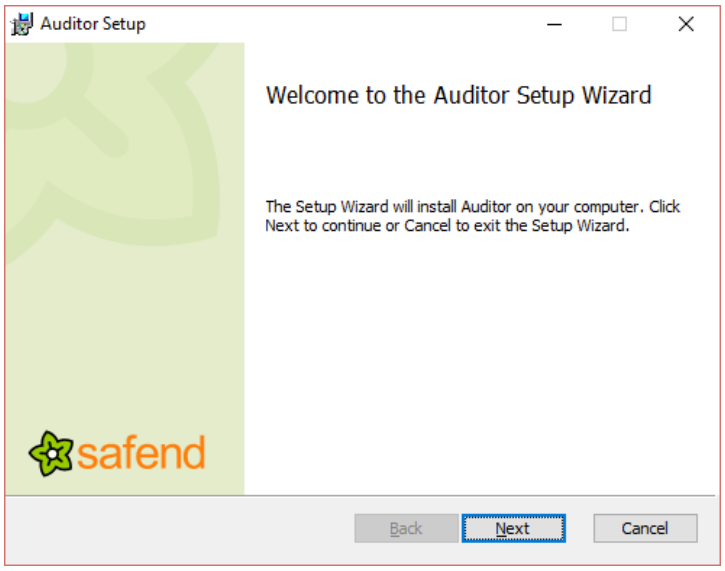
Report Viewing Requirements:

Software	❖ Microsoft .NET Framework 4.0 ❖ For viewing XML reports in MS Excel - Microsoft Excel version 2003 and up.

Installing Safend Auditor

➢ **To install Safend Auditor:**

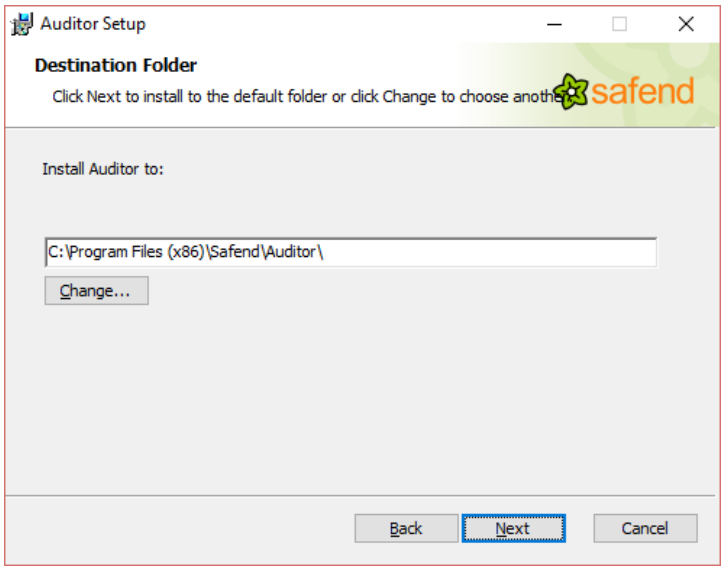
1 Double-click *'Auditor.en-US.msi'* to install the Safend Auditor on the local computer. The *Welcome* window opens:



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

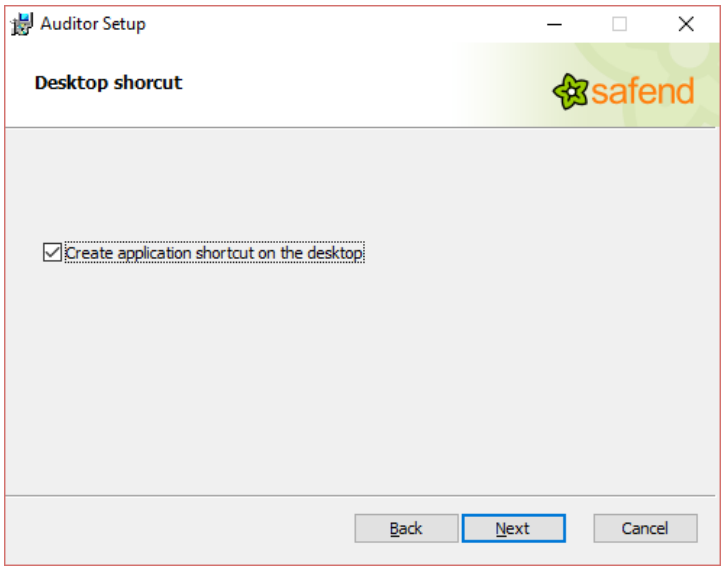


3 Check the license agreement check box and click **Next**. The *Destination Folder* window appears:



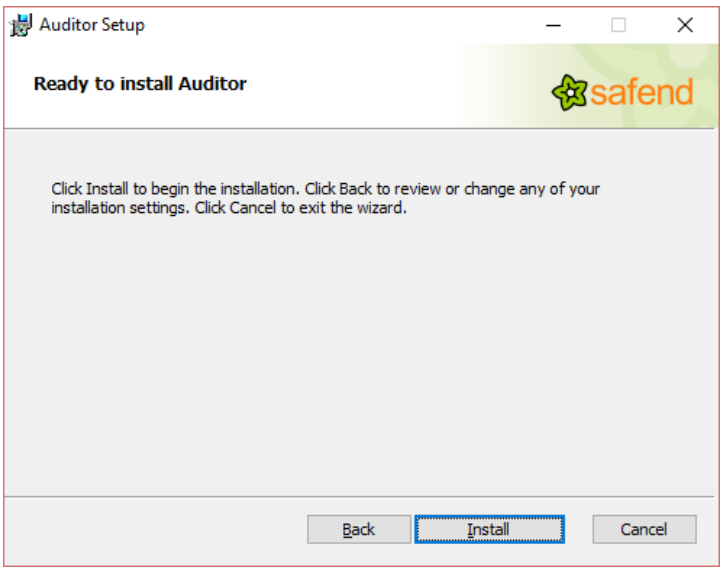
4 If you wish to change the destination folder, click **Change** and select a folder.

5 Click **Next**. The *Desktop shortcut* window opens:



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

7 Click **Next**. The *'Ready to install Auditor'* window opens:



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 Click **Finish** to complete the installation.

Registration

The Auditor installation is valid for 30 days before FREE registration.
To acquire a license key, please contact your local reseller or contact us at support@safend.com

Refer to *Acquiring a License Key* to learn about how to acquire a FREE license key.

Uninstalling Safend Auditor

In order to uninstall Safend Auditor, open "**Programs and features"** Right click on "**Auditor**" and choose "**Uninstall**"

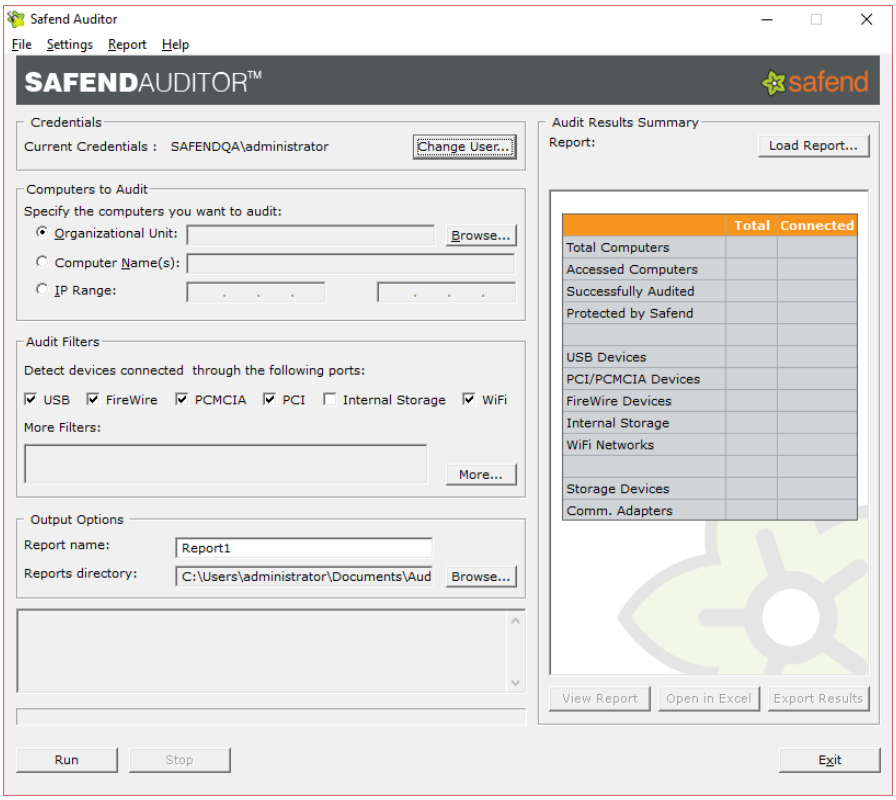
Auditing

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

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

Using Safend Auditor

After launching Safend Auditor (either by double-clicking its desktop shortcut or via your computer's *Windows* 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.

Audit Protocol

In order to perform the audit scans remotely on endpoints, Safend Auditor needs to communicate with these endpoints using remote access protocols which allow it to remotely access the registry of Microsoft 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)

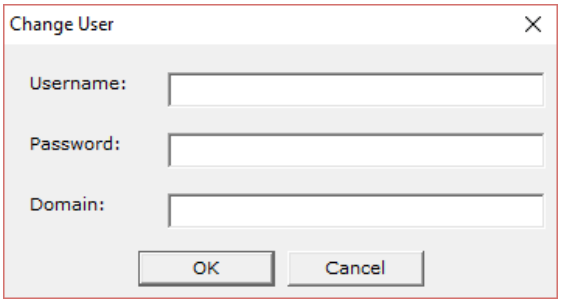
- Local administrative privileges on the endpoint

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.

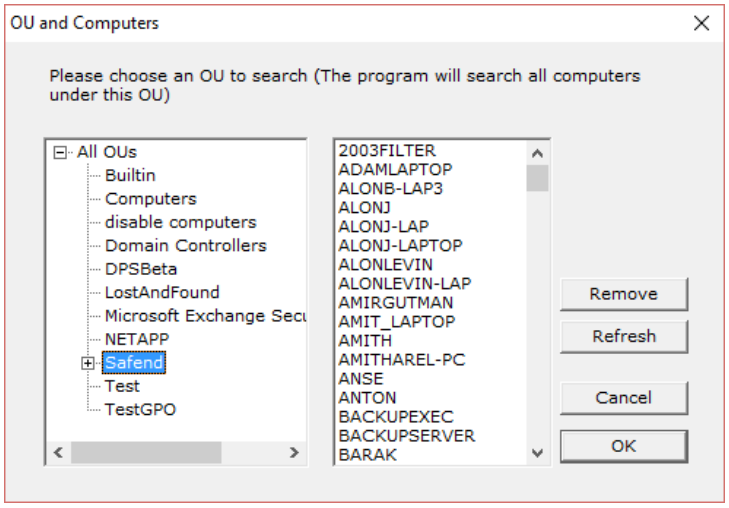
Selecting Target Computers

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 haven't 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).

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.

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 does from the *Audit Filters* section, as described below.

Device Port

Safend Auditor 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

It is not possible to distinguish between devices connected over PCMCIA and PCI.

IMPORTANT

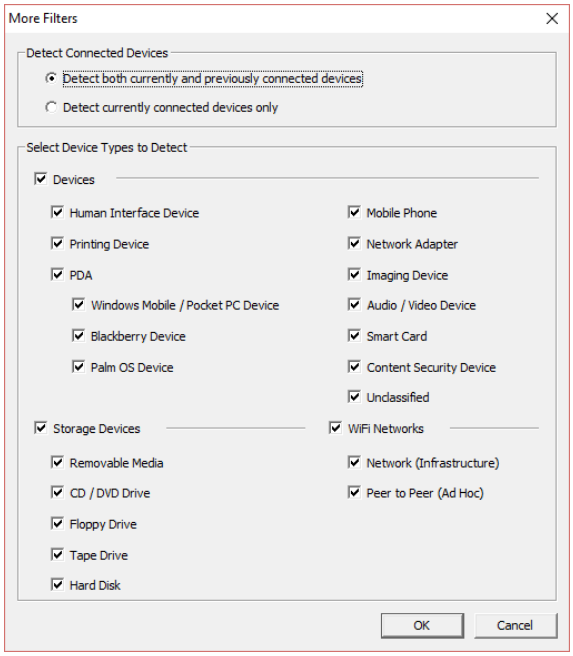
It is not possible to distinguish between WiFi networks that the computer is currently connected to and those to which it was connected in the past. For this reason the audit results doesn't display any indication in the "Connected" field.

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:



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.

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

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.

Report Name

Each time you perform a scan and create an audit report, Safend Auditor 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 as XML called AuditRes.xml which is found in the report folder. By default, the report (and folder) name is set to 'Report1'.

At any time, you can use the AuditRes.xml file to load report in the Auditor for reviewing it again. Click "**Load Report...**" choose the saved AuditRes.xml and data will be re-loaded.

NOTE

Saving a report under an existing name overwrites the data.

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:\Users\USERNAME\Documents\Audits*.

➢ **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 "Auditor Report Viewer" or as XML in Excel format.

NOTE

Only the AuditRes XMLs that are created after the Auditor complete the "Run" procedure, are available to be loaded.

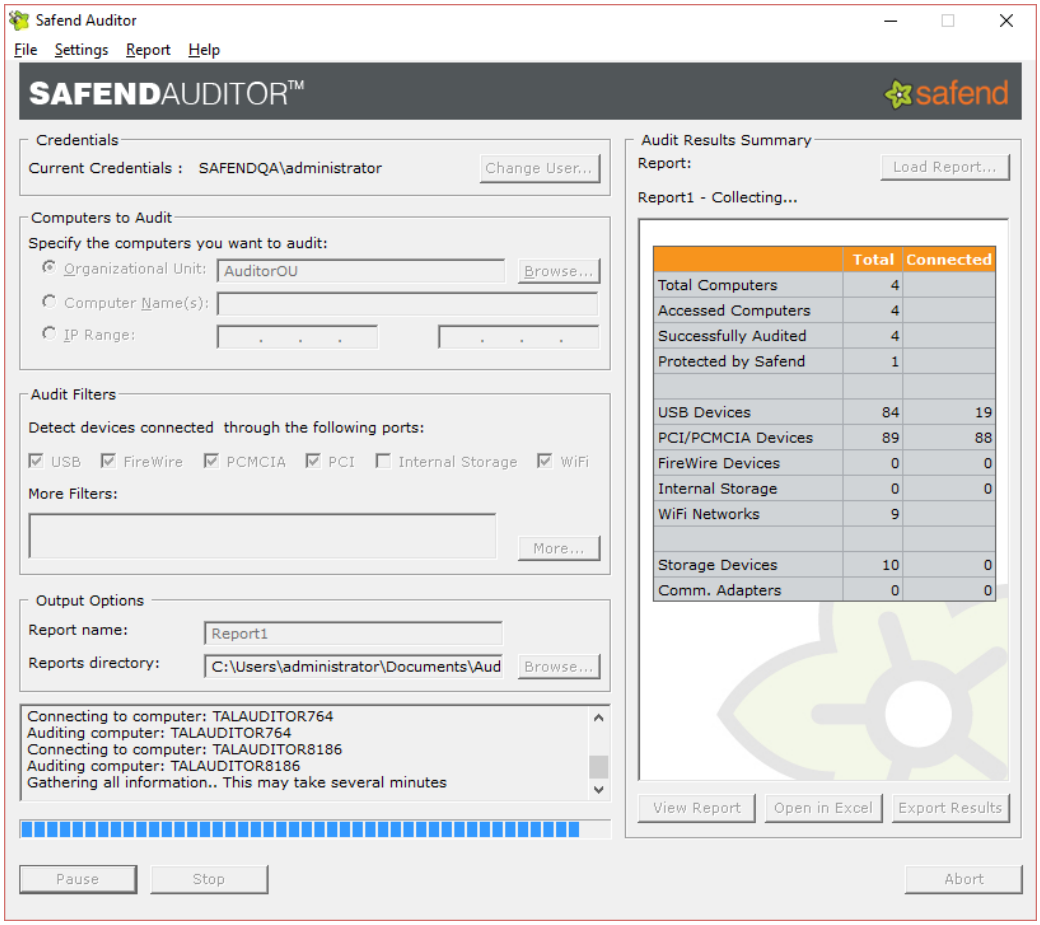
Performing the Audit

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

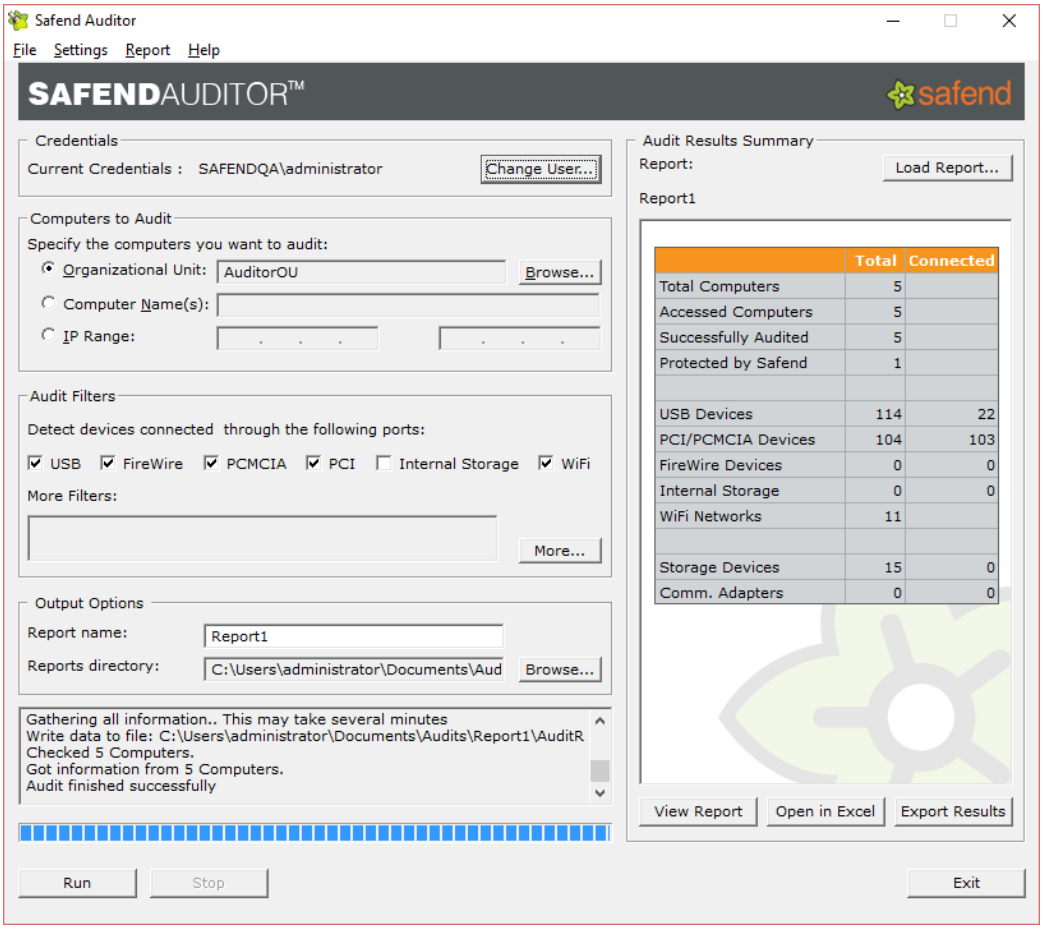
While the scan is in progress, **Pause, Resume and Stop** may take several seconds to take effect.

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 with the Auditor Reporter (**View Report** button), create a customizable XML Excel report (**Open in 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.

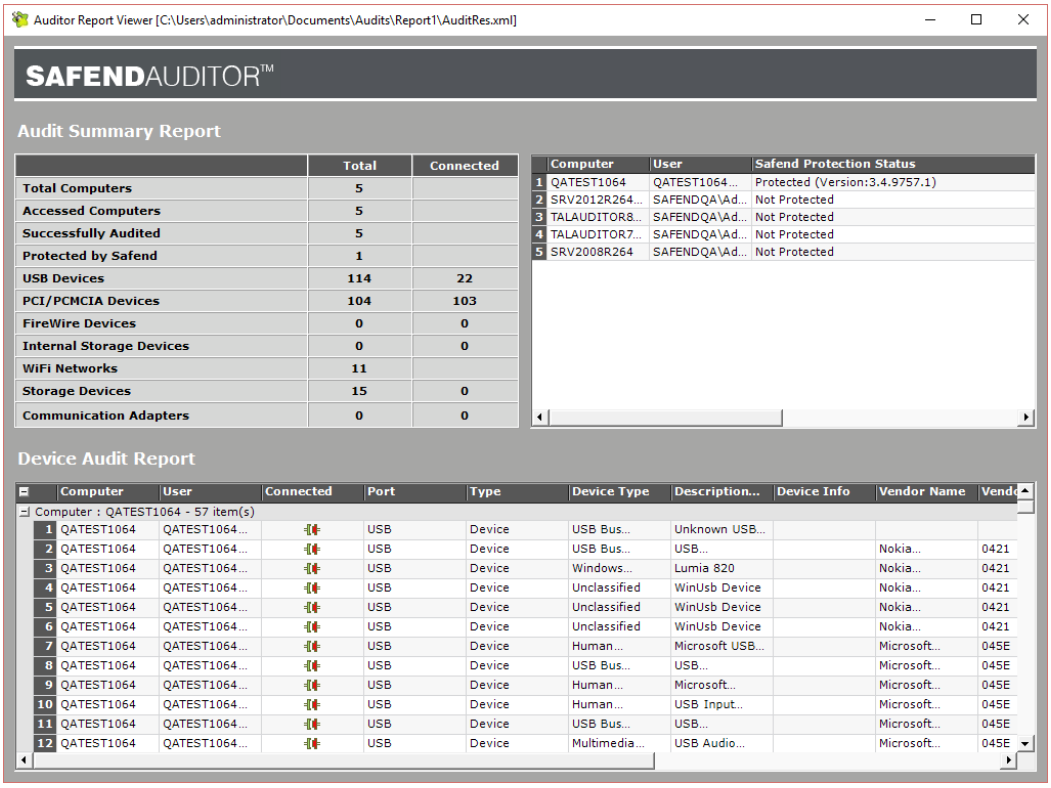


Viewing Audit Results

The simplest way to view the audit results is using "Auditor Reporter Viewer".

➢ **To view audit results with the "Auditor Report Viewer":**

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



	Total	Connected
Total Computers	5	
Accessed Computers	5	
Successfully Audited	5	
Protected by Safend	1	
USB Devices	114	22
PCI/PCMCIA Devices	104	103
FireWire Devices	0	0
Internal Storage Devices	0	0
WiFi Networks	11	
Storage Devices	15	0
Communication Adapters	0	0

	Computer	User	Safend Protection Status
1	QATEST1064	QATEST1064...	Protected (Version:3.4.9757.1)
2	SRV2012R264...	SAFENDQA\Ad...	Not Protected
3	TALAUDITOR8...	SAFENDQA\Ad...	Not Protected
4	TALAUDITOR7...	SAFENDQA\Ad...	Not Protected
5	SRV2008R264	SAFENDQA\Ad...	Not Protected

	Computer	User	Connected	Port	Type	Device Type	Description...	Device Info	Vendor Name	Vende
⊟ Computer : QATEST1064 - 57 item(s)										
1	QATEST1064	QATEST1064...		USB	Device	USB Bus...	Unknown USB...			
2	QATEST1064	QATEST1064...		USB	Device	USB Bus...	USB...		Nokia...	0421
3	QATEST1064	QATEST1064...		USB	Device	Windows...	Lumia 820		Nokia...	0421
4	QATEST1064	QATEST1064...		USB	Device	Unclassified	WinUsb Device		Nokia...	0421
5	QATEST1064	QATEST1064...		USB	Device	Unclassified	WinUsb Device		Nokia...	0421
6	QATEST1064	QATEST1064...		USB	Device	Unclassified	WinUsb Device		Nokia...	0421
7	QATEST1064	QATEST1064...		USB	Device	Human...	Microsoft USB...		Microsoft...	045E
8	QATEST1064	QATEST1064...		USB	Device	USB Bus...	USB...		Microsoft...	045E
9	QATEST1064	QATEST1064...		USB	Device	Human...	Microsoft...		Microsoft...	045E
10	QATEST1064	QATEST1064...		USB	Device	Human...	USB Input...		Microsoft...	045E
11	QATEST1064	QATEST1064...		USB	Device	USB Bus...	USB...		Microsoft...	045E
12	QATEST1064	QATEST1064...		USB	Device	Multimedia...	USB Audio...		Microsoft...	045E

The report includes three tables:

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

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 Safend** – The number of computers on which Safend Protector is installed.
- **USB Devices -** Number of devices on that used via USB port.
- **PCI/PCMCIA Devices -** Number of devices on that used via PCI/PCMCIA port.
- **FireWire Devices -** Number of devices on that used via FireWire port.
- **Internal Storage –** Number of devices connected on the internal "port" on the computer Bus, for example internal CD /DVD over IDE or Hard disk connected over SCSI etc…
- **WiFi Networks –**Numbers of WiFi the computer is and was connected to.
- **Storage Devices** – Number of the Storage devices connected via any port.
- **Comm. Adapters –**Number of the Adapters connected to the various ports.

The summary table includes two *columns*:

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

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 Name** – The actual name of the Vendor.
- **Vendor** – Vendor ID number extracted from the device.
- **Model** – Product ID number extracted from the device.

- **Distinct ID** – A 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.

Computer Audit Report

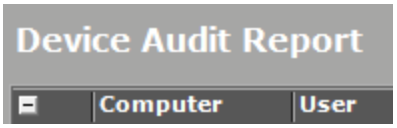
Each record in the table includes the following:

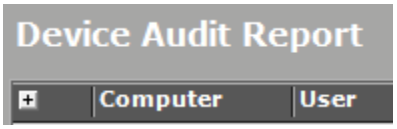
- **Computer** – The name of the audited computer.
- **User** – The last user logged on to the audited computer.
- **Safend Protection Status** – here you can see whether or not the computer is protected by Safend Protector and whether or not the computer was available for auditing:

- **Protected** – The computer was successfully audited and Safend Protector is installed.
- **Not Protected** – The computer was successfully audited and Safend protector is not installed.
- **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).
- **Unreachable** – The computer was completely unavailable (switched off, offline, does not exist, etc.).

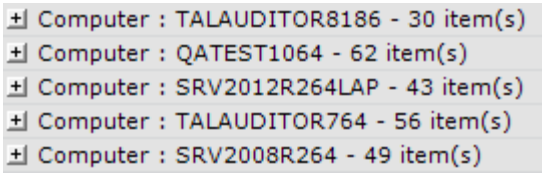
You may sort the results based on any one of the columns by clicking its heading in the header row. An additional click toggles the sort order from ascending to descending and back.

By default, the "Auditor Report Viewer" after scan all computers will be presented in expand mode. You can use the disclosure widget to collapse or expand the computer results.

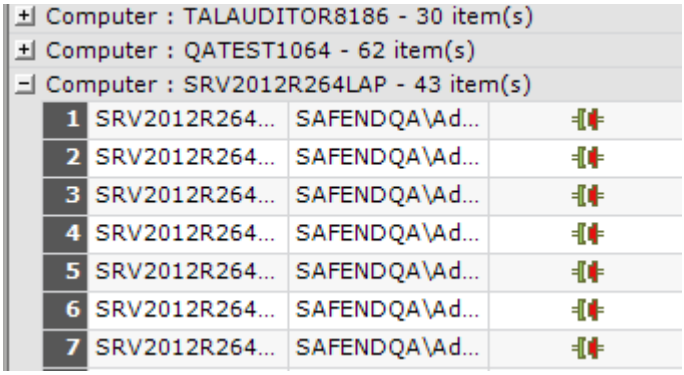




Each computer has its own disclosure widget which can expand or collapse specific computer results



In the following example you can see one computer that is expanded while the others are colloapsed.



Viewing Audit Results in Excel

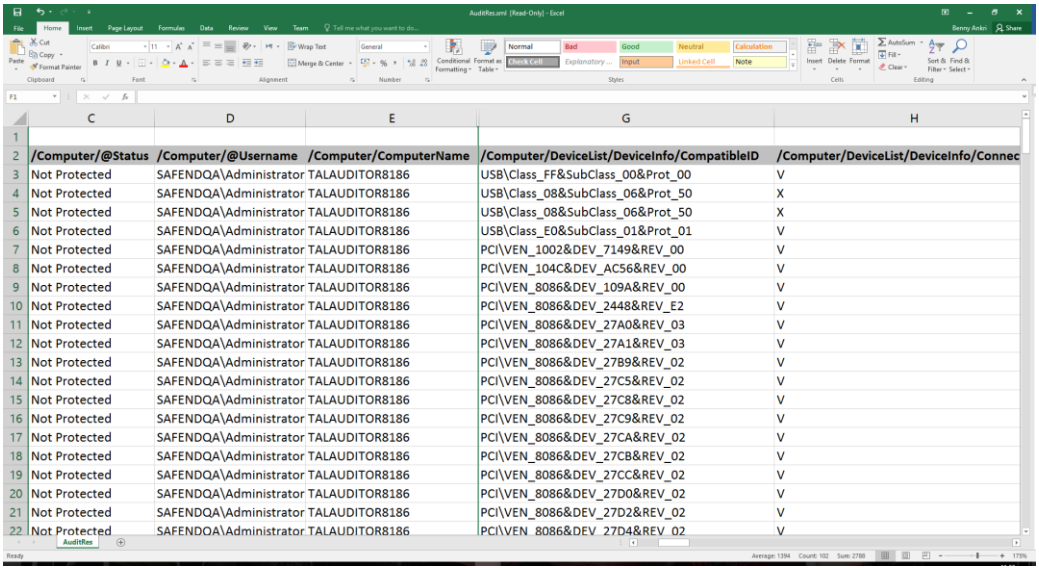
The Auditor may export the collected results to a formatted Microsoft Excel file, which allows you to analyze the audit results using the full power of Excel.

- **To view the Excel report:**

  Click **Open in Excel**. The Excel will open the XML file that used by the "Auditor Report Viewer".

> NOTE
>
> This feature requires Microsoft Excel to be installed on the same machine on which the report is requested to be open.

Once the process is complete, the XML report opens:



	C	D	E	G	H
1					
2	/Computer/@Status	/Computer/@Username	/Computer/ComputerName	/Computer/DeviceList/DeviceInfo/CompatibleID	/Computer/DeviceList/DeviceInfo/Connec
3	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	USB\Class_FF&SubClass_00&Prot_00	V
4	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	USB\Class_08&SubClass_06&Prot_50	X
5	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	USB\Class_08&SubClass_06&Prot_50	X
6	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	USB\Class_E0&SubClass_01&Prot_01	V
7	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	PCI\VEN_1002&DEV_7149&REV_00	V
8	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	PCI\VEN_104C&DEV_AC56&REV_00	V
9	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	PCI\VEN_8086&DEV_109A&REV_00	V
10	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	PCI\VEN_8086&DEV_2448&REV_E2	V
11	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	PCI\VEN_8086&DEV_27A0&REV_03	V
12	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	PCI\VEN_8086&DEV_27A1&REV_03	V
13	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	PCI\VEN_8086&DEV_27B9&REV_02	V
14	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	PCI\VEN_8086&DEV_27C5&REV_02	V
15	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	PCI\VEN_8086&DEV_27C8&REV_02	V
16	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	PCI\VEN_8086&DEV_27C9&REV_02	V
17	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	PCI\VEN_8086&DEV_27CA&REV_02	V
18	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	PCI\VEN_8086&DEV_27CB&REV_02	V
19	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	PCI\VEN_8086&DEV_27CC&REV_02	V
20	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	PCI\VEN_8086&DEV_27D0&REV_02	V
21	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	PCI\VEN_8086&DEV_27D2&REV_02	V
22	Not Protected	SAFENDQA\Administrator	TALAUDITOR8186	PCI\VEN_8086&DEV_27D4&REV_02	V

The tables in the Excel report are identical to those of the "Auditor Report Viewer", although they are arranged in a different order.

Exporting Audit Results to Safend DPS

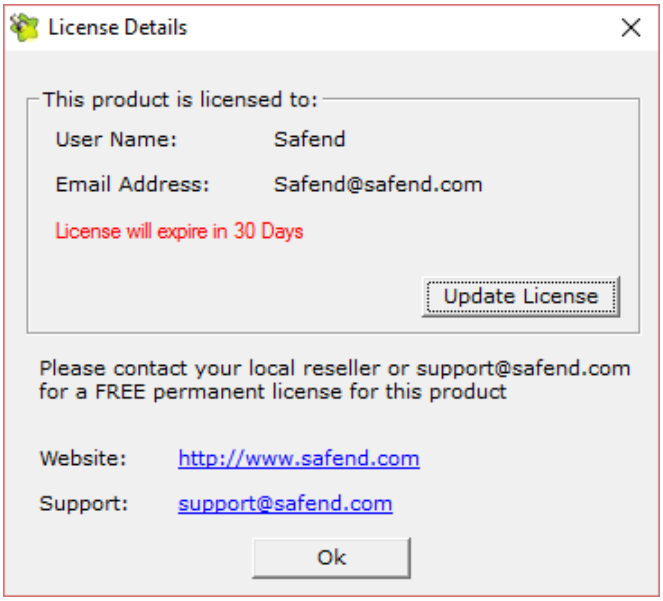
Safend Auditor enables you to create XML file by clicking the "Export Results" button which can be used when creating a security policy with Safend's policy enforcement product – Safend Data Protection Suite. By uploading the file to the Protector Management Console you can determine which of the devices in it should be approved and which should be blocked for use.

➢ **To export audit results:**

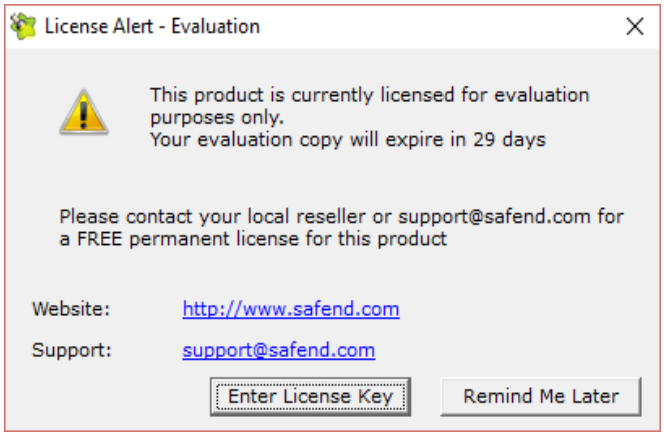
1. Click **Export Results**. The *Export Results* window opens.
2. In the *Export Results* window, select the destination folder, type in the file name and click **Save**.

Acquiring a License Key

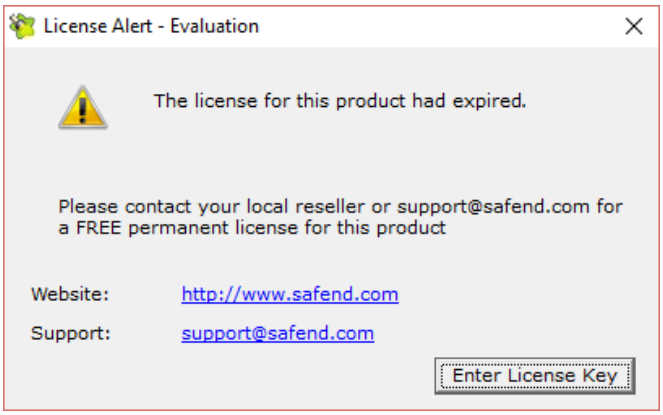
The Auditor installation is valid for 30 days before registration.



After 30 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:



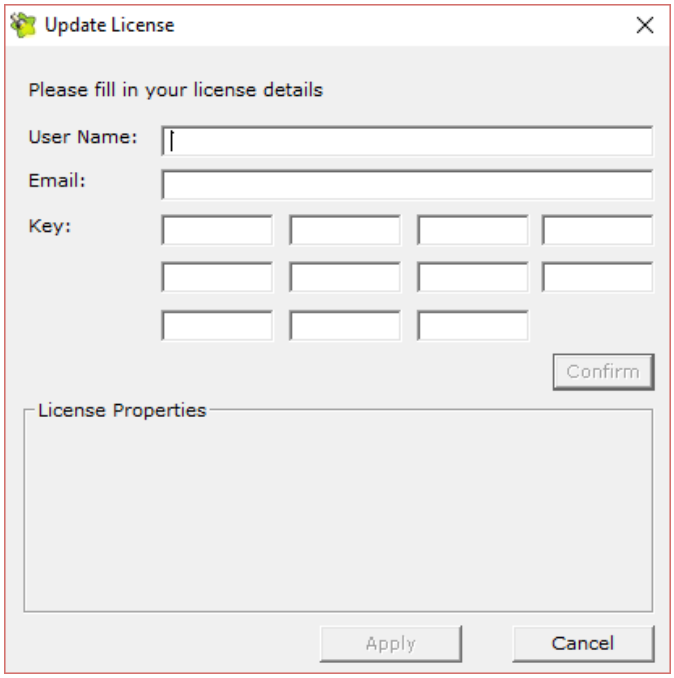
You may check your license status at any given time in the *Help* menu, under **License**.

➢ **To acquire FREE license key:**

Contact your local reseller or contact us at support@safend.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

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