safend
Securing Your Endpoints

Safend Auditor 3.0 Security Analysis
Quick Reference Guide for Partners

GENERAL FAQ

1. **What is Safend Auditor?**
    Safend Auditor is a lightweight, clientless software utility that provides organizations with the visibility needed to identify and manage endpoint vulnerabilities. Safend Auditor transparently and rapidly queries all organizational PCs – over every network, finding every device and documenting all devices that are or have been historically or are currently locally connected.

2. **What is an "end-point"?**
    End-point refers to all enterprise workstations, laptops, and kiosks. Safend protects end-points by securing ports at end points, including 1) Local, physical communications port such as USB, Firewire, PCMCIA, printer, serial, and other laptop or desktop interface, 2) Wireless ports such as WiFi, Bluetooth and IrDA.

3. **What kind of devices does Safend Auditor typically find?**
    Safend Auditor actively searches and reports back on any device connected to USB, Firewire, and PCMCIA ports. These include media players, cameras, handhelds, Smart Phones, printers, scanners, multi-function peripherals (scan/fax/print), Disk on Keys, CD/DVD-RWs, removable hard-drives, other portable storage devices, and more.

4. **What specific information does Safend Auditor provide?**
    Safend Auditor will generate a summary table that displays computer name, user, device class, and device serial number, and whether or not the device is currently connected. Safend Auditor will also indicate how many end-points were scanned, audited, and are protected by Safend.

5. **Why should customers care?**
    Most organizations adequately protect TCP/IP ports, but peripheral devices are often overlooked despite presenting a serious risk: 1) Large amounts of sensitive information can be stolen through end-points, leading to costly data leakage, 2) Malicious code including viruses, worms and Trojan horses can infiltrate through end-points, and 3) Personal information may be exposed, leading to a break in compliance with data privacy laws such as HIPAA. Safend Auditor helps customers identify these vulnerabilities at end-points, while Safend Protector helps customers secure their end-points.

safend
Securing Your Endpoints

6. **How can channel partners benefit from Safend Auditor?**
Many organizations today are simply not aware of the threat end-points present. To raise awareness and get a foot in the door, partners can offer a "free security analysis" utilizing Safend Auditor. When prospects see the number of devices that have been connected, the risk becomes tangible and clear. This inevitably leads to a desire for an end-point security solution such as Safend Protector. Safend Auditor demonstrations lead to Safend Auditor and Safend Protector sales, and can lead to complementary product sales, too. Safend Auditor provides a good lead-in for a complete security discussion with clients = great revenue opportunity for partners.

7. **How difficult is Safend Auditor to use? How long does it take?**
Safend Auditor is very easy to use. Installation of the management software is straightforward, and as clientless solution there is no need to install software on each and every client machine. Depending on the size of the organization, it can take as little as 15-minutes to run an audit query, and generate a report: Once an audit begins it takes only seconds to start compiling a report.

8. **Is performing a Safend Auditor audit disruptive to end users?**
No, Safend Auditor is totally non-intrusive: End users will not be disrupted in any way.

9. **Is running Safend Auditor safe?**
Safend Auditor is reliable and safe. It was designed by experts, has been rigorously tested, is clientless, and has been recognized as a best-of-breed product by industry analysts, the media, channel partners, and customers.

10. **Does Safend Auditor need to be installed on each computer being audited?**
No, Safend Auditor is clientless – no software needs to be installed on the computers being audited. Safend Auditor only needs to be installed on one laptop or computer connected to a network, and have a user that has network administrator rights with full control.

11. **Is Safend Auditor only relevant for domain environments?**
No, Safend Auditor can run an audit on domain-less computers so long as they are networked. An audit can be performed using an IP range or computer name list to specify the computers that should be included in the audit.

12. **Does Safend Auditor work with Microsoft Active Directory? What about other domain management software?**
Yes, Safend Auditor works seamlessly with Microsoft Active Directory. Safend Auditor also works with other domain management software such as NT and Novel Netware through an IP range scan option.

13. **Can Safend Auditor query individual computers only?**
Yes, Safend Auditor can audit an entire OU in a domain or can be configured to audit individual computer(s) only by name or IP address.

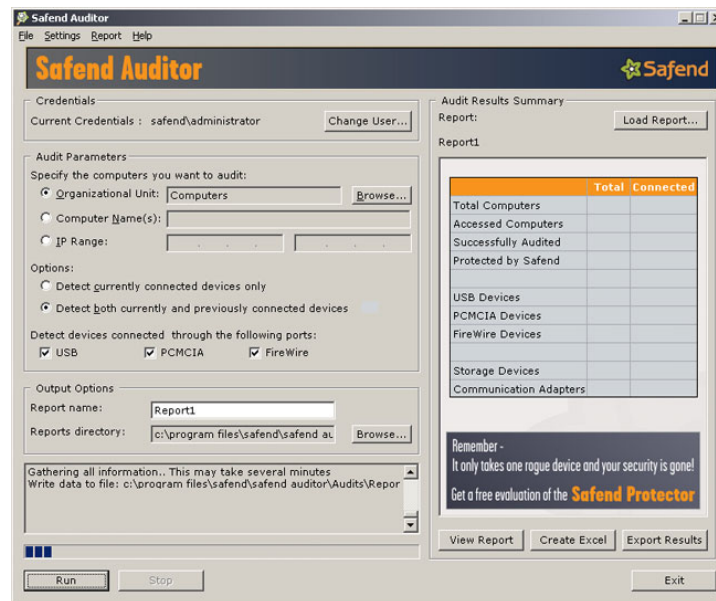14. **Can Safend Auditor export reports?**
Yes, Safend Auditor can export reports in MS Excel-compatible format and XML and is fully integrated with the Safend Protector.

15. **Does Safend Auditor have the ability to stop devices that have been discovered?**
No, Safend Auditor only provides visibility into what devices are connected. To gain control, Safend Protector is needed.

SCREENSHOTS

Steps 1 & 2: Select whether to audit all computers in an OU, or computers by name or IP Range, then select desired options and ports to audit:

Step 3: View on-screen report. *Optional:* Export report to Microsoft Excel or XML.
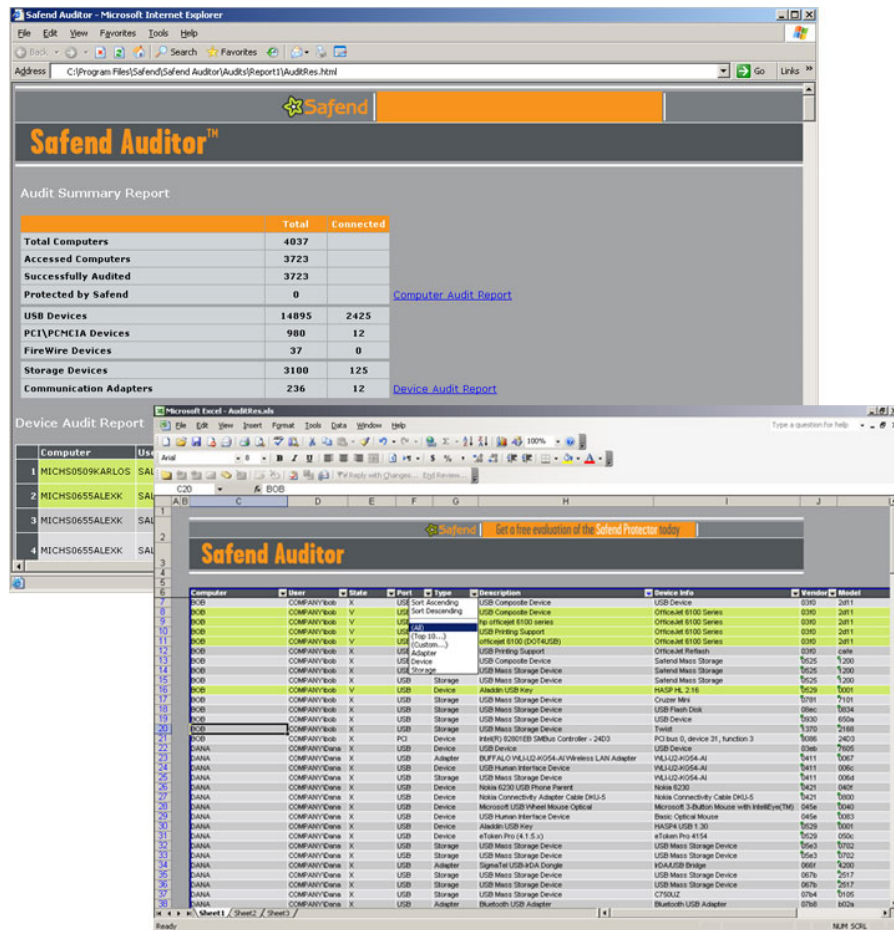
POSITIONING AN AUDIT WITH CUSTOMERS

How should I position doing an end-point audit using Safend Auditor with customers?
- ✓ **Fast** – as little as 15 minutes, depending on the size of the organization
- ✓ **Free** – only requirement by customers is a short investment in time
- ✓ **Risk-Free** – totally non-intrusive, clientless audit means end-users will not be disrupted at all
- ✓ **Powerful** – complete visibility into end-point connections being made, past & present
- ✓ **Expert Analysis** – as a Safend partner, you will be able to guide customers through the entire process from installation, to audit, to report, to insight into what the report means.

What specific arguments can be presented to different stakeholders to encourage them to let you perform a Safend Auditor audit?

Business Decision Maker	Technical Decision Maker
1. See how your corporate data and intellectual property is exposed at end-points – is your competitive advantage being threatened?	1. Be recognized as a corporate hero by identifying areas where your company is exposed and recommending a great solution such as Safend Protector
2. Discover where there are holes in your corporate security policy that could be a major liability and result in legal action (possibly even for negligence) or a publicity crisis.	2. Limit exposure to personal negligence by incrementing the security policy you defined and oversee to include end-point protection
3. Ensure compliance with strict legislative standards for data security, such as Sarbanes-Oxley, HIPAA, and Basel II	3. Maximize the efficiency and lower the cost of network resources by preventing users from utilizing them for non-business-related activities (eg; clogging hard drives or file/email/LOB servers with media files uploaded from portable media players or storage devices)
4. Identify who is using removable, high-capacity storage devices and quickly check to ensure they have a legitimate use – are corporate documents being stolen or exposed to theft by unwitting employees?	4. Ensure you never have to deal with a virus, worm or Trojan horse that got in through the back door via an end-point
5. Identify areas where investment in new technologies such as WiFi could lead to new threats including unprotected access of viruses or hackers to your entire network	5. Protect trade secrets and intellectual property to ensure your company's competitive advantages remain intact
6. See who is using corporate resources or clock-time for personal use	6. Ensure your written policy is enforced
7. And More…"	7. And More…

Why would a customer want me to do an audit instead of just doing it themselves?
As an expert, you will help the customer learn the software quickly, provide deep analysis of the risks, and recommend the best ways to address not just end-points, but potentially other areas that may be vulnerable, too. You are also the source for the best solution to end-point security vulnerabilities - *Safend Protector*!

What if the customer says no? In short, don't give up:

"I don't have the time."	• "Performing a basic audit will take 15 minutes or less. Are you sure you can't find the time – my schedule is flexible." • "Perhaps there is a subordinate I can perform the audit with, and then provide you with a detailed report?" • "Perhaps there is a better time… can I call you in a few weeks?" • "Given the risks, you really can't afford not to take the time." • Point to the Safend web-site for the free auditor & let them run the scan at their leisure
"I don't have the budget."	• Auditing is free!! • "Did you know that adding end-point protection can cost as little as $10-40 per seat?" • "Perhaps I can perform the audit with you now so that you can justify including an end-point solution in your next budget

	ask?" • "When do you anticipate having additional budget?" • "If any special promotions or price discounts come about, is it okay to call you and let you know about these offers?"

"I have it covered without you."	• "I understand. That's often the impression with customers before they see the clear and present danger after receiving an audit report. For 15 minutes of your time, I'm sure it's worth knowing for certain whether or not you're protected".
	 • "Do you already have an end-point solution in place?
	    o If yes, perhaps you'd be interested in seeing how Safend compares. I'm confident after taking a closer look you will be able to see clearly that Safend Auditor and Safend Protector offers more visibility, better protection, more flexibility, greater control, improved usability, all while being very cost competitive."
	
	 <table><tr><td>**Audit the customer's existing end-point solution!**</td></tr><tr><td>"One way we can compare is for us to perform a free Safend Auditor audit and compare the results with your existing solution's reporting. This will help you see whether or not your existing solution is working as planned, and identify where tampering could be a problem."</td></tr></table>
	    o If no, I'm curious how familiar you are with the growing problem of end-point security. Perhaps I could spend a few minutes either on the phone with you now, another time, or in person – the audit process is so simple, I could do it for you as we went over the industry data and media coverage that speaks to the issue."
	
	 <table><tr><td>**Ask if they can tell you off-hand how many devices are currently connected to end-points!**</td></tr><tr><td>"Do you know exactly how many storage devices, media players and other devices are connected to your network via end-points right now? We have found that many customers know how many desktop and laptop computers are connected, but they don't have any visibility into end-point devices. When we ask customers to guess, we usually find out there's 4-5 times as many devices as they suspected!"</td></tr></table>

PERFOMING THE END-POINT SECURITY ANALYSIS

The Safend Auditor report is on-screen. Now what?

1. **Let who you're selling do the driving**
2. **Quickly highlight summary findings: "Wow, that's a lot of devices"…**
   - Devices currently connected
   - Devices connected in the recent past
   - Total devices found, past + currently
   - Look for iPod's & other dangerous devices
   - Computers that have had the most devices connected
3. **Ask who you're selling to scroll to their computer name**
   - Can they identify all the devices listed?
   - Is the list what they would expect to see?
   - Are there any unknown devices that make them wonder? (Should John Doe employee be using an Ipod or Webcam?)
4. **Export to Excel:** Use Excel's auto-filter function to easily sort the device list
5. **Dive deeper on certain devices discovered:**
   - How many storage devices are there?
   - How many non-business-related devices are connected (media players; cameras)?
   - Find the computer that has the most devices connected – "I wonder why they have made so many device connections?"
6. **Ask if they can identify each of the devices on the list**
   - Are they all legitimate connections?
   - "If you could turn any of these connections off right now, would you?"
   - "Wouldn't you rather turn off all of the unknown connections and then turn them back on if shown to be legitimate?"
7. **Offer to take the export data to do a more in-depth analysis**
   - Summarize your discussion on paper, including a summary table
   - Add a graphic representation of the data
   - Suggest looking at other areas of their business where you might have a good solutions
   - Suggest a solution to their end-point woes…
8. **Go for the close for *Safend Protector*!**
   - Safend Protector adds comprehensive control of all end-points
   - Seamless integration between Safend Auditor and Safend Protector means policies can be easily defined (eg; quickly mark audited devices to safe 'whitelists' to allow connectivity)

SYSTEM REQUIREMENTS

The following environment components are required for the operation of the Safend Auditor and in order to view the audit results:

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

Domain OS (optional): Windows 2000 Server (Service Pack 0-4); Windows 2000 Advanced Server (Service Pack 0-4); Windows 2003 Server

User information: The user running the Auditor must have local administration rights on the machine. The audit user must have domain administrator credentials. The user used to run the audit must have write permissions to the target report folder. (The audit user is either the current logged in user, if it was not changed from within the Auditor, or the new user after the Change User functionality was used).

Viewing requirements: Software Internet Explorer version 6.0 and up –or- Microsoft Excel version 2003 and up

INSTALLATION INSTRUCTIONS

The following is a summary of installation instructions for Safend Auditor. For complete step-by-step instructions, please refer to the user manual provided together with the installation files.

Important note: All Safend products are architected with powerful anti-tampering capabilities. Please follow closely the installation instructions and product documentation, paying especially close attention to the instructions regarding the importance of saving the uninstall password. Without the uninstall password there is no way to uninstall the product.

1. Ensure the person you are doing the Safend Auditor audit with has:
    - Network administrator permissions
    - One client machine with network access to all the computers to be audited
2. Ensure the system requirements above are met
3. If a firewall is in place, ensure all relevant ports are open to enable the audit.
    Note: If Active Directory is deployed, the required ports are typically open by default.
4. Have the required installation files available:
    - CD-ROM: Can be left behind with customer or download from www.safend.com
    - USB Disk-on-Key: Can be left behind with customer. Can also be part of the audit – it will show up on the audit!
    - Download: Not recommended, as this will take time.
5. Locate the 'Safend Auditor.msi' file and double click it to install the Safend Auditor on the local computer. Click the Next button in the Welcome screen.
6. The License Agreement screen is displayed. Check the license agreement check box and click the 'Next' button.
7. The Destination Folder screen is displayed. Click the 'Change' button in order to change the destination. Click the 'Next' button to continue. The Ready to Install' screen is displayed.
8. Check or uncheck the 'create desktop icon' checkbox and click 'Install' to begin the installation. A progress bar is displayed until the installation process is completed, at which point the InstallShield Wizard Completed screen is displayed.
9. Check or uncheck the 'Launch Safend Auditor' checkbox and then click the 'Finish' button to complete the installation.
10. The Auditor installation is valid for five (5) runs before registration. After five (5) 5 runs, a registration key will be required. While not registered, a message notifying how much time before the evaluation period is over will be displayed. To start the audit, click "Remind me later"

11. Upon completion of the installation, you will find Safend within the Start > All Programs menu. Access the program and important product documentation within the Safend menu.

If you encounter any problems or have any questions, please contact support@safend.com , or call (215) 496-9646.

SAFEND AUDITOR SUMMARY

- ✓ **Non-intrusive, clientless and very easy to use**
- ✓ **Reliable, precise and simple device discovery**
- ✓ **Comprehensive report of devices currently or previously connected to any endpoint**
- ✓ **Immediate report on-screen or report exported to MS Excel or XML**
- ✓ **Easy to use user interface**
- ✓ **Fully compatible with Microsoft Active Directory and other domain management software**
- ✓ **Can audit only selected PCs, groups or the entire enterprise**
- ✓ **Provides discovery only – is a perfect complement to Safend Protector which gives comprehensive control**