secure auditor

FREQUENTLY ASKED QUESTIONS

Note: Frequently asked questions are common problems which users encounter during Secure Auditor assessment. If you do not find answer(s) to your query in this document, then lookup the FAQ and KnowledgeBase section on Secure Bytes website.

Q1: Which operating systems are compatible with Secure Auditor?
Answer: Secure Auditor is compatible with Windows 2000 and above.

Q2: I have identified a windows based machine on my network through discovery; can I add that machine again for audit?
Answer: When you identified a machine through discovery process then that particular machine will be automatically added to audit machine window for authentication, when you choose windows from "Select an Application" tab. You do not need to add discovered machines instead you only need to provide their login credentials.

Q3: I am unable to connect with remote Oracle machine, why?
Answer: If you are unable to get connected with Oracle databases just check the default Oracle ports 1521 and 1526 to see if they are open or not. If following ports are closed then open them to resolve connectivity issue. If problem does not resolve then send an email to support@secure-bytes.com. Our technical representative will contact you shortly.

Q4: How can I get maximum vulnerabilities in my windows machine?
Answer: You can check your Windows machines for maximum vulnerabilities if you select SWA profile. By selecting the SWA profile within Profile Management you will be able to audit your machine against maximum number of vulnerabilities and will be able to identify largest number of security threats which can exploit to get control of your windows based machine.

Q5: Can I archive Secure Auditor reports for future purposes?
Answer: Yes, Reports provided by Secure Auditor are archived in multiple user friendly formats like PDF, MS Word, MS Excel, Rich Text format etc. Reports of Audits are saved in the database; so you can save them once you have closed the application.

Q6: Can I add vulnerabilities in Secure Auditor?
Answer: You can only work with vulnerabilities already embedded within Secure Auditor. It does not provide facility to add your own vulnerabilities for audit or enumeration but we are continuously upgrading Secure Auditor by adding new vulnerabilities as they are discovered by vendors, international bodies and other sources.

Q7: Does Secure Auditor support any command line options?
Answer: No, Secure Auditor does not support any command line options.

Q8: I have conduct discovery now what should I do?
Answer: Review the information assets produced after discovery, choose an audit profile and conducted audit.

Q9: Does Secure Auditor support the auditing of wireless networks?
Answer: Yes, Secure Auditor does support auditing of wireless networks.

Q10: How can I create my own profile according to my company policy?
Answer: Click on “Audit Profiles Manager”, and then go to “New Profile”, type the name for the new profile. You can check and uncheck the vulnerabilities you want your new profile to contain. An option for selecting all vulnerabilities is also present. After selecting vulnerabilities for your profile click on save button present on top of new profile screen and then click close. Your created profile will be shown in profile list of Profile Manager and you will be able to use it for multiple audits until you delete your profile.

Q11: What are different modules of Secure Auditor?
Answer: Secured Auditor consists of the following four modules:
- Secure ORA Auditor
- Secure SQL Auditor
- Secure Win Auditor
- Secure CISCO Auditor

Q12: Does Secure Auditor provide prove of existence of vulnerabilities?
Answer: One of the best features of Secure Auditor is the ability to provide exact specifications of identified threats. It is only possible because Secure Auditor does not work on guessing and false positive. Secure Auditor provides exact instance and location of vulnerability, along with overview, description and solution.

Q13: Why Secure Auditor does not offer fix it option?
Answer: Secure Auditor does not offer fix it option because many solutions if implemented might conflict with existing configurations. For instance some patches might impair the working of some existing applications. Hence Secure Auditor offers solution of identified vulnerabilities and recommends users to analyze their current environment before implementing any solution.

Q14: While I am trying to audit windows XP machine, trying to authentication to a machine getting an error (Invalid username & password) know provided the correct user name and password.
Answer: You may come up with this issue with your windows up machine due to default setting of simple file sharing. By default simple file sharing is disabled on windows XP. In order to enable the simple file sharing setting, select a folder on any drive go to -->tools -->folder options -->view -->look for (use simple file sharing (recommended)) unselect it. If problem persist then send your query at support@secure-bytes.com. Our technical support team will contact you shortly.

Q15: Do I need to deploy any agent on the host machine while installing Secure Auditor?
Answer: Secure Auditor is an agent less application. Only one instance of Secure Auditor is needed to be deployed on a host from where it will perform its functions throughout the network.

Q16: Can I run audit on multiple Windows machines?
Answer: Yes you can run audit on single or multiple Windows machines in a single audit session. The procedure is simple. You either need to discover or add multiple Windows machines you wish to audit and then start an audit with Secure Win Auditor. You can select number of Windows machines you wish to audit, but audit will not be conducted simultaneously. Secure Auditor will audit multiple Windows machines one by one in a single session.

Q17: Why can't we scan .0 and .255 addresses?
Answer: By default, IP Address 0 is used for network address and IP Address 255 is used for broadcast addresses therefore Secure Auditor will not scan them.

Q18: Can I run audit on multiple Oracle databases?
Answer: Yes you can run audit on single or multiple Oracle databases in a single audit session. The procedure is simple. You either need to discover or add multiple Oracle databases you wish to audit and then start an audit with Secure Ora Auditor. You can select number of Oracle databases you wish to audit, but audit will not be conducted simultaneously. Secure Auditor will audit multiple Oracle databases one by one in a single session.

Q19: What are the Secure Auditor Version 2.0 evaluation limitations?
Answer: Secure Auditor is a suite of software specifically designed to facilitate multiple security concerns of an organization. Its evaluation version is having limited functionality. In the evaluation version you cannot access, view or print reports of the Audit, discovery or utilities. You cannot schedule an audit with Secure Auditor evaluation version.

Q20: When I am trying to conduct audit on windows system, getting an error The RPC server is unavailable. (Exception from HRESULT: 0x800706BA)
Answer: For a Windows system audit if you get an error message regarding RPC server unavailability then Please check whether the firewall on the target machine is on or not. If it is turned on then turn it off and try again to conduct audit on your Windows system. If problem persist then send your query at support@secure-bytes.com. Our technical support team will contact you shortly. Our general suggestion to you before conducting audit is to either turn off firewall on target machine or open port number 135, 139, and 445.

Q21: Can I get the number of software installed on a range of scanned Windows based machine?
Answer: Definitely yes! You can get all software installed on a range of scanned windows based machine with the help of Windows software inventory viewer which is embedded in Secure Win Auditor.

Q22: My Scheduled Scan with Secure Auditor doesn't seem to work?
Answer: If your scheduled scan with Secure Auditor doesn’t seem to work then most probably the machine you wish to audit was not up at the time of scan.

Q23: Do I need to deploy any agent on the machine while running Secure Auditor?
Answer: Secure Auditor is an agent less application, it needs to be deployed on one host and it can scan the entire network. So while conducting audits on any machine you only need to get connected with remote machine and do not need to deploy any agent on them.

Q24: Does Secure Cisco Auditor audit firewalls?
Answer: Yes, Secure CISCO Auditor audits firewalls as well as Cisco routers and Switches.

Q25: Does Secure Auditor scan machines running UNIX?
Answer: Secure Auditor does not scan UNIX Operating systems, but it does scan Oracle database servers running on UNIX OS.

Q26: Troubleshooting errors during installation?
Answer: For troubleshooting errors you should be able to open the log file in notepad. Secure Auditor logs can be find in following directory C:\Program Files\Secure Bytes\Secure Auditor 2.0\Error_Logs. If you are still having the same problem then please email the log file to support@secure-bytes.com for further investigation. Kindly email the screen shot of the error along with your email as attachment.

Q27: I am unable to audit MSSQL database server on my network.
Answer: If you are having trouble in auditing MSSQL database server on your network then make sure that firewall is not blocking Secure Auditor to audit MSSQL database server on your network. Also check that you are using correct MSSQL authentication information and provided correct password.

Q28: Why the installation of Secure Auditor fails to complete?
Answer: If you encountered with an installation issue of this sort kindly make sure that you are login with Administrators privileges and then install the software. If you are reinstalling Secure Auditor make sure that you have uninstalled the previous version of the same software completely from your system. Also remove the Secure Bytes folder from program file and restart the system. After completing defined steps kindly start installation of Secure Auditor again on your system.

Q29: I am unable to Audit Oracle database server on my network.
Answer: It is possible Remote login is disabled on Oracle database in order to enable Remote login as Sysdba to Oracle database server do the following steps.
Step 1:
Log on the database machine and create a password file:
For Unix (Shell):orapwd file=$ORACLE_HOME/dbs/orapw password=*password_for_sys*
For Windows (Command Prompt):
orapwdfile=%ORACLE_HOME%\database\PWD*sid_name*.orapassword=*password_or_sys*
Step 2:
Add the following line to init*service_name*.ora in UNIX, or init.ora in Windows:
REMOTE_LOGIN_PASSWORDFILE=EXCLUSIVE
Change it to SHARED

Step 3:
Restart the Database and Test the Remote Login. Connect sys/password_for_sys@tns_name_of_db as Sysdba.

Q30: In discovery report under high vulnerability heading there is an entry about Patch missing, but does not identify the missing patch number.
Answer: In discovery process Secure Auditor does not show the detail information. It provides this information in audit. So if you want to see missing patch number you just need to conduct an audit on selected machine which will provide your desired information.

Q31: Secure Auditor send an error message and closed its application, Why?
Answer: If you encountered this problem then most probably your license file may be got corrupted. For new license file you may contact with sales department at sales@securebytes. com or if you are using trial version than you can download new version of Secure Auditor.

Q32: I am unable to discover SQL Database Server on my network.
Answer: Make sure that TCP/IP is enabled to match the server. It is recommended that you set TCP/IP above named pipes. If you are using MDAC (Drive={SQL Server} or SQLOLEDB.x) in your client application, you will want to run the cliconfg.exe program to enable TCP/IP and named pipes and to set the order so that TCP/IP is above named pipes. Make sure the "Hide server" checkbox in TCP/IP properties of Server in SQL Server Network Utility is not check because if it checked SQL Server will hide server and not send any announcements. MS SQL Server announces itself over network via UDP port1434. Tools like osql, isql, isqlw, ODBC Data Source Administrator, SQL-DMO powered programs send UDP packets to this port for discovery of SQL Server on host.

Q33: How do I get Secure Auditor auto update functionality to work through my web proxy?
Answer: You don't need to do anything if web proxy information is correctly configure in the internet properties option and http is enable out going on Web proxy then Secure Auditor update function will automatically start working.

Q34: I am running a non-English version of Windows 2000. Can I install Secure Auditor on my operating system?
Answer: No currently we do not support non-English version of Windows. End user must have English version of Windows in order to install and work with Secure Auditor.

Q35: During installation, setup fails with the message that I do not have administrative rights?
Answer: Before installing Secure Auditor make sure that you are login with Administrator privileges and then try to install the software on your system. If you are reinstalling Secure Auditor make sure that you uninstall the software completely from your system. Kindly remove the Secure Bytes folder from program file and then restart the system. Then try to install software again on your system.

Q36: How much performance overhead does Secure Auditor add to an audited server?

Answer: On different systems Secure Auditor performs different check so the performance overheads Secure Auditor add to an audited server really depends on what a user is checking for example while it is checking windows system, Secure Auditor can take some performance hit but on other applications like Oracle databases, MSSQL databases and Cisco routers user will not face any performance overhead.

Q37: Secure Auditor is showing error message that Router does not exist, why?

Answer: Secure Auditor show defined message that the "Router does not exist" when Cisco Router in question may not be accessible. This sort of error is shown when user has selected the wrong port for audit or a firewall in blocking Secure Auditor.

Q38: Do I have to reinstall Secure Auditor when moving to the paid version?

Answer: Yes, you need to reinstall a new instance if you want to move from a trail version to paid version of Secure Auditor.

Q39: Does Secure Cisco Auditor audit Cisco switches?

Answer: Yes, Secure CISCO Auditor does audit Cisco switches.

Q40: Can Secure Auditor run an audit on a machine across the network?

Answer: Yes Secure Auditor is a network based tool and it can run audit on any machines across the network. From a single machine Secure Auditor can audit Windows machines, Oracle databases, MSSQL databases and Cisco Routers across the network with ease of use and without deploying any agent.

Q41: What software components does Secure Auditor install and where?

Answer: By default Secure Auditor installs instant of MSDE on the system at C:\Program Files\Microsoft SQL Server\MSSQL$SADATABASE and it also installed runtime version Crystal reports on the system at c:\Program Files\Business Objects.

Q42: What to do after conducting discovery?

Answer: When you complete discovery process on your network than you will get enumeration results from your network. It provides a brief overview regarding possible and most visible exploitable system information on your network which could be used for simulating an attack on the network. After discovery you can save your session and view discovery report which could be archived in multiple formats for comparative and competency analyses. You can also conduct audit or select Profile manager to customized audit profile for an audit.

Q43: Can I run audit on multiple Oracle databases?

Answer: Definitely, you can run audit on single or multiple Oracle databases running on single or multiple machines. You can conduct audit on multiple Oracle databases in one instance or audit where you need to add multiple Oracle databases one by one or provide credentials of already discovered Oracle databases. You can add multiple Oracle databases deployed and running on Window, Solaris or any other platform.

Q44: Can Windows Event Log Viewer work if DCOM is disabled on remote systems?
Answer: NO, Windows Event Log Viewer require DCOM in order to work properly, so please make sure that DCOM is enable on your remote windows machine or Oracle database before using their respective event log viewers.

Q45: Question: Can I simultaneously run discovery on Windows, Oracle, MSSQL Server and Cisco router?
Answer: Yes, Discovery process could be conducted simultaneously on single or multiple machines and applications. You can also conduct discovery of the Windows network in single session. Secure Auditor will display results regarding all discovered applications in a form of single report.

Q46: Can I run audit on multiple Cisco Routers?
Answer: Definitely, you can run audit on single or multiple Cisco Routers (only if you have license for all those IP's) due to the fact that Secure Auditor license is IP bounded. You can conduct audit on multiple Cisco Routers in one instance where you need to add multiple Cisco Routers one by one or provide credentials of already discovered Cisco Routers. You can add multiple Cisco Routers and do not conduct audit on switches or firewalls.

Q47: Do I need any additional software installed in order to run Secure Auditor?
Answer: Yes! Secure Auditor requires Windows Installer 3.1 and Dot Net Framework 2.0 as a pre-requisite before installing Secure Auditor. You need to install both the software before start installing Secure Auditor. You can download .Net framework from the location prescribed in installation guide or you can also download Secure Auditor from installation CD.

Q48: Can Secure Auditor be used with high transaction volume servers?
Answer: Yes it will work fine but it is recommended to run any Security Assessment Tool during slow transaction time.

Q49: Can I run an audit on Windows, Oracle, MSSQL Server and Cisco Router in a single audit session?
Answer: No, you cannot run an audit on Oracle, Windows, MSSQL or Cisco Router in a single audit session. You need to create separate audit sessions to conduct audit on separate applications. Because before conducting an audit you first need to select an application which could be Cisco, Oracle, Windows or MSSQL. There is no option to select all applications during single audit session. Because when a user selects one application for audit he will able to view its related utilities which are embedded into the software.

Q50: Does Secure Auditor audits Oracle Database on other operating systems?
Answer: Yes. It has the ability to audit Oracle on Linux as well as Sun Solaris machines but it cannot run from a Linux or Sun Solaris platform. In other words Secure Auditor can only be installed on Windows Machines but it can audit Oracle databases deployed and running on Linux and Sun Solaris or any other platform. It is due to the fact that Oracle databases are audited via Oracle's listener capability hence Oracle can be deployed on

any operating system in order to be scanned by Secure Auditor

Q51. On a machine where windows vista is installed, I logged on windows vista machine with a User account which belongs to Domain Administrators Group. I run secure auditor on my local machine and tried to Audit the Local Machine then a message appeared that "You are currently login as Domain user this user doesn't have enough rights to perform full audit, therefore you may not be able to view all vulnerabilities on the system, to perform full audit please login again on the system with a administrative privilege user, or run the software with Run as Administrator.Do you still like to continue (Yes/ No) ' what is the solution.
Answer: The Problem is due to the User Account Control (UAC) which is enabled on local machines in windows vista, windows 7 and windows 2008 Servers. This problem does not exist in XP and previous versions of window because User Account Control (UAC) was introduced in windows vista. Solution of this problem is that you right click on Secure Auditor icon, select (Run as Administrator) option that will work fine.

Note: User Account Control (UAC) is a technology and security infrastructure introduced with Microsoft's Windows Vista and Windows Server 2008 operating system. It aims to improve the security of Microsoft Windows by limiting application software to standard user privileges until an administrator authorizes an increase or elevation. In this way, only applications trusted by the user may receive administrative privileges, and malware should be kept from compromising the operating system. In other words, a user account may have administrator privileges assigned to it, but applications that the user runs do not inherit those privileges unless they are approved beforehand or the user explicitly authorizes it.

Q52. I am unable to connect to the SQL database for audit, All my credentials are correct. I receive an error "Data source should be on the same machine".

Answer:
This problem should be solved if the 'Data Source' field is filled in the following manner : [IP-Address]\[InstanceName]

Make sure that if you enter ServerName instead of IP-Address in the 'Host Name / IP' field, then the 'Data Source' field should be entered in the following format instead : [Server-Name]\[InstanceName]

Also Note that if the 'SQL Server Browser' service is running on the Server [which has the SQL Instance], then the above format will be automatically inserted in the 'Data Source' drop down field by our appliciation.