

<u>Overview</u>

This document outlines the installation, configuration, and upgrade procedures for the SonicWall Aventail Advanced Reporting 7.2.16 product. Aventail Advanced Reporting (AAR) is built on the Sawmill Professional universal log file analysis and reporting product from Flowerfire (http://www.sawmill.net).

Access log files from the SonicWall Aventail appliances are loaded onto the AAR Server for processing and analysis. The two log files used, extraweb_access.log and extranet_access.log provide detailed information about connection activity for both the Web Proxy and Network Tunnel services. This data includes session start and stop times, username and realm information, internal resources accessed, bytes transferred, and in the case of web access, explicit HTTP GET and POST details.

System level performance data, such as uptime, CPU utilization, maximum number of users, etc., is not provided in the access logs and therefore is not reported in the AAR product. AAR is focused on user access and auditing reports only. Other methods, such as SNMP, are available for system level reporting and analysis.

Server Requirements

Aventail Advanced Reporting runs on Windows NT/2000/XP/2003 and most versions of Linux. Basic system requirements are as follows:

- Memory: a minimum of 256 MB of RAM, with 1 GB preferred
- Disk: 500 MB of disk space for an average database
- Processor: 1.8 GHz Pentium 4 or greater

Additional sizing details can be found in the Sawmill FAQ

Aventail Advanced Reporting works with Safari, Mozilla, and Internet Explorer 5.5 or above. Other browsers may not be supported. Versions of Internet Explorer before 5.5 are not supported. The ability for the browser to run JavaScript must be enabled.

Licensing and Activation

Aventail Advanced Reporting is available as a free download from the SonicWall Support site (<u>http://www.mysonicwall.com</u>) for 15 days. If you have purchased AAR from your SonicWall reseller, you will be sent an activation code via email. Log into MySonicWall and register AAR as a new product with the activation code that you received:



Activating Aventail Advanced Reporting

- 1. Go to https://www.mysonicwall.com/ and log in with your username and password
- 2. Click on My Products on the Navigation menu
- 3. Under the Add New Product enter the activation code for Aventail Advanced Reporting in the Serial Number box and select Register
- 4. Aventail Advanced Reporting will now show up under the My Products tab in your mysonicwall account.

Retrieving your Aventail Advanced Reporting license

- 1. Click on Aventail Advanced Reporting under the My Products tab in your mysonicwall account
- 2. The license will be located under the Status button. It will appear to be a string of letters and numbers (Example: pro-7profile-psep-aar7hf8e-3cb6)

Obtaining Installation Files

Before installing Aventail Advanced Reporting, you must obtain the setup file and copy it to the file system of your local computer. The file is delivered as a tar archive for Linux and a setup executable program for Windows and is available in both 32-bit and 64-bit versions.

To obtain the AAR installation file:

- 1. Log in to the SonicWall Support site at http://www.mysonicwall.com
- 2. Under the Downloads section, select 'Free Downloads'
- 3. On the Software Type pull down menu, select 'Aventail Advanced Reporting'
- 4. Select the appropriate aar7.2.16 installation package for your operating system

<u>Upgrading</u>

Before upgrading, back up your existing LogAnalysisInfo folder located in the AAR installation directory. This folder contains all the existing Profile and customization settings.

It is also important to stop the current Aventail Advanced Reporting service that is running on your AAR server. Do this from the Windows Administrative Tools-Services Panel or from the Linux command line. Failure to perform this step may result in an unsuccessful upgrade.

Once the AAR Service is stopped, the new aar7.2.16 installation package can be installed over the old version following the steps below. All settings, profiles, and reports will be migrated to the new release and preserved.



Installation

Install the Aventail Advanced Reporting executable files as follows:

Linux

Copy the installation tar file to directory where you want to install Aventail Advanced Reporting.

From the command line, untar the installation file using the following command:

tar -xvf aar7.2.16_x86_linux-es4.tar

This will result in a directory called /aar being created containing the Aventail Advanced Reporting executable program called aar7.2.16

Aventail Advanced Reporting requires the libcrypto.so.4 library to run so this package may have to be installed on your Linux server. If you have a later version libcrypto library installed on your system, a link can be defined for AAR to use:

cd /usr/lib # In -s libcrypto.so.0.9.7 libcrypto.so.4

Windows

Execute the file aar7.2.16_x86_windows.exe.

First the Readme file is displayed. After reading, select Next:

🕞 Aventail Advanced Reporting 7.2.16 Setup	
Release Notes Please read the following important information before continuing.	
When you are ready to continue wit Setup, click Next.	
AAR 7 RELEASE NOTES Thank you for using AAR! If you have any questions, comments or suggestions about AAR, please send email to EClassSupport@SonicWALL.com, or call us at +1 866.360.1949.	*
Nullsoft Install System v2,33	ancel



232-001694-00 REV A Aventail Advanced Reporting 7.2.16 Installation Guide

Choose a location to install AAR or leave the default location, then select Next:

🎲 Aventail Advanced Reporting 7.2.16 Setup
Choose Install Location Image: Choose the folder in which to install Aventail Advanced Reporting 7.2.16.
Setup will install Aventail Advanced Reporting 7.2.16 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.
ß
Destination Folder C:\Program Files\Aventail Advanced Reporting 7 Browse
Space required: 51.0MB Space available: 15.3GB
Nullsoft Install System v2,33



Choose, the AAR Components to install – leave the default setting for AARService:

Select Install to complete the installation.

🗊 Aventail Advanced Report	ing 7.2.16 Setup		
Choose Components Choose which features of Aventail Advanced Reporting 7.2.16 you want to install.			
Check the components you want to install and uncheck the components you don't want to install. Click Install to start the installation. \Box			
Select components to install:	AAR Service	Description Position your mouse over a component to see its description,	
Space required: 51.0MB			
Vullsoft Install System v2.33 ——			



Once complete, select Finish to access the AAR Console.

🌍 Aventail Advanced Report	ing 7.2.16 Setup 📃 🔲 🔀
	Completing the Aventail Advanced Reporting 7.2 316 Setup Wizard Aventail Advanced Reporting 7.2.16 has been installed on your computer. Click Finish to close this wizard. ✓ Snow Aventail Advanced Reporting / now (http://(127.0.0.10)
	< Back Einish Cancel

These steps will result in (by default) a directory created called C:\Program Files\Aventail Advanced Reporting 7 containing the Aventail Advanced Reporting files.

Aventail Advanced Reporting will be installed as a service that starts automatically.

An Aventail Advanced Reporting icon will also be created on the desktop to access the AAR Console.



Executing Aventail Advanced Reporting

Linux

On Linux, you can start using Aventail Advanced Reporting immediately by executing the file "aar7.2.16". Aventail Advanced Reporting will establish itself as a Web server on port 8987 (by default), and will print a message describing how to access it from your Web browser.

To have Aventail Advanced Reporting startup automatically with the system and run as a daemon, you can add or modify a system init script to automatically start Aventail Advanced Reporting at system startup.

Please note that the startup script location will vary depending on the Linux distribution that you are using and that this information will need to be gathered from the Linux distribution documentation.

Once you have accessed the Aventail Advanced Reporting web application, you can follow the steps below to collect Aventail access logs, perform the initial setup of Aventail Advanced Reporting, and configure Aventail Advanced Reporting.

Windows

On Windows, Aventail Advanced Reporting is installed as a service and is started by default. Follow the steps below to collect Aventail access logs, perform the initial setup of Aventail Advanced Reporting, and configure Aventail Advanced Reporting.

Collect Aventail access logs

Aventail Advanced Reporting relies on data from the SonicWALL Aventail appliance access log files. Since the SonicWALL Aventail appliances are hardened by default, the only way to copy the log files off the appliance is by using SSH (Secure Shell) and SCP (Secure Copy). For the initial configuration, the log files will be manually copied off the SonicWALL Aventail appliance and onto the local system. Examples will be given in a later section on how to automate the log collection task.

To enable SSH access to the SonicWALL Aventail appliance:

- 1. Log in to Aventail Management Console
- 2. From the main menu, select Services
- 3. In the Network Services area click the Configure link for SSH.
- 4. Enable **SSH** by checking the **Enable SSH** check box.
- 5. Add a host or network from which you want to allow SSH access, select **New**, type the IP address and subnet mask (make sure to allow the host or network that the AAR Server is on)



On the SonicWALL Aventail appliance, the access logs are located in the /var/log/aventail directory and are called extranet_access.log and extraweb_access.log. The extranet_access.log file is used for client/server connections or Network Tunnel access while the extraweb_access.log file is used to log web access only.

Log rotation is enabled by default so there may be several logs in the /var/log/aventail directory named extranet_access.log.n or extraweb_access.log.n where n is a number indicating that a file has been rolled over.

For a complete set of data, copy all of the files named extranet_access.log.* and extraweb_access.log.*

To copy the logs off the appliance using Windows, the most popular client is called WinSCP and can be downloaded from: <u>http://winscp.sourceforge.net/eng</u>

For Linux, SCP is typically available on Linux boxes from the command line. As an example, run the following on the Linux-based Aventail Advanced Reporting host computer to copy files from your Aventail appliance to a local directory called /logs on the Aventail Advanced Reporting host:

scp root@aventailappliance:/var/log/aventail/extra*.log /logs

In this example, WinSCP is used to copy the log files from the appliance to the local AAR server C:\Logs directory:



SonicWall Aventail

😼 aventail - root@192.168.1.110 - WinSCP				
Local Mark Files Commands Session Options Rei	mote Help			
I 🏟 🔢 🗊 🔹 🕋 📽 😵 🔛 I 🗄	- 🛛 🔹	🧭 🕜 🛛 Default 🔹 🍕 🗸		
🖙 C: Local Disk 🔻 🥱 🖕 🗸 🔿 🗸 🕅 🕅	3 🔂 🎭	🍙 aventail 🔹 🐜 🦕 🛶 🚽	🖻 🗖 🖪	
	Size Type		Size	
	Dize Type Dizet		5/20	1/0/2009.6
	Farenc	E	0 021 702	1/28/2009 0
		access_servers.log 1	21 012 024	0/26/2009
		access_servers.log.2	22 249 024	5/20/2000
		access_servers.log.3	5 001 004	11/13/2006
			424 160	9/15/2006
			121,100	11/13/2006
Ν		ame.stdout	0	1/28/2009
r\			82.767	7/7/2008 1
		bytecount.log	02,101	8/29/2008
		Ctrl-service.log	2.697	1/28/2009
		🗐 db util.log	1,398	11/13/2006
		extranet access.log	164,869	12/16/2008
		extraweb_access.log	3,481,404	12/16/2008
		extraweb_access.log.1	1,615,322	11/13/2006
		extraweb_access_legacy.log	888,653	12/16/2008
		extraweb_plaintext.log	3,576,611	9/18/2007
		🗊 extraweb_plaintext-POST.log	1,439,292	9/18/2007
		🗊 healthcheck_apache_instance_custo	0	10/19/2004
		🗐 healthcheck_apache_instance_error.log	54,949	1/28/2009
		istance_error.l	24,040	2/26/2007 🔜
		🗐 importmiarate 9.5.0 log	148	10/10/2008
			J	
0 B of 0 B in 0 of 0 5,138 KiB of 76,610 KiB in 3 of 91				
📲 🧬 F2 Rename 📑 F4 Edit 📑 F5 Copy 📑 F6 Move	澘 F7 Create Dii	'ectory 🗙 F8 Delete 😁 F9 Properties 👖	=10 Quit	
		🔒 sc	Р 🛄	0:02:12



Version 10.x Log Format Configuration

For Version 10.x there was a change to the extranet_access.log file. In order for Aventail Advanced Reporting to recognize the log, a new configuration file must be loaded on the AAR Server.

Go to the Knowledge Portal section of MySonicWall and search for Knowledgebase article number 6009. From this article, you will be able to download a new aventail_client_server_access.cfg file with instructions on where to copy the file on your AAR Server.

Initial Setup of Aventail Advanced Reporting

After Aventail Advanced Reporting has been installed it runs as a local web application on port 8987. It can be accessed using a web browser with the URL <u>http://localhost:8987/</u> or <u>http://127.0.0.1:8987</u>

On Windows, the desktop icon can also be opened to access the AAR web application.

When accessed for the first time, a Setup wizard will be displayed:



Select Next:





Read and accept the license agreement, then select Next

🥭 Aventail Advanced Reporting Setup-License Agreement - Windows Internet Explorer	
🔆 🔄 👻 http://127.0.0.1:8987/?dp+templates.setup	X Live Search
<u>Eile E</u> dit <u>Vi</u> ew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp	
😪 🍄 🔯 Aventail Advanced Reporting Setup-License Agreement	🐴 🔹 🗟 👻 🖶 🔹 🔂 <u>P</u> age 🔹 🎯 T <u>o</u> ols 🔹 🎽
Aventail 🕼	<u> </u>
Aventail Advanced Reporting Setup	
License Agreement	
Please read the following license agreement carefully.	
FLOWERFIRE END USER LICENSE AGREEMENT FOR SAWMILL THIS IS A LEGAL AGREEMENT BETWEEN YOU EITHER AN INDIVIDUAL OR AN ENTITY ("LICENSEE") AND FLOWERFIRE, INC. ("FLOWERFIRE"). BY INSTALLING OR USING THE LICENSED PRODUCT LICENSEE AGREES TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS FLOWERFIRE END USER LICENSE AGREEMENT FOR SAWMILL ("AGREEMENT"). IF LICENSEE DOES NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT DO NOT CONTINUE THE INSTALLATION PROCESS, INTERDITED CORE FOR ALL DOUGNIL CONCENTIONS OF THIS AGREEMENT DO NOT CONTINUE THE INSTALLATION PROCESS,	
I do not accept the terms in the license agreement Next Done	▼ Internet 100% ▼



Enter in the license key obtained from your MySonicWall account in the appropriate field. If not, you can use Aventail Advanced Reporting free for 15 days.

Select Next:

CAventail Advanced Reporting Setup-Licensing - Windows Internet Ex	plorer	
• Maintenant State	🔽 🗲 🗙 🛛 Live Search	P -
Eile Edit View Favorites Yools Help		
😪 🎄 🙀 Aventail Advanced Reporting Setup-Licensing	🏠 🔹 🔝 👻 🖶 😦 Page 🗉	• 🔘 T <u>o</u> ols • »
Aventail 🐻		<u> </u>
Aventail Advanced Reporting Set	up	
Licensing		
Please enter a license or try Aventail Advanced Reporting for 15	5 days by leaving the license field blank.	
Lirense.		
	Y	
Expand License Field (use for licenses which span multiple lines	3)	
bloot		
Done	Internet	🔍 100% 🔻 🏿



Enter in a username and password for the Aventail Advanced Reporting Administrator account. Then select Next:

🤗 Aventail Advanced Reporting Setup-Administrative User - Windows Internet Explorer	
😋 🕙 👻 http://127.0.0.1:8987/?dp+templates.setup 💽 🛃 🗙 Live Search	n
Eile Edit View Pavorites Iools Help	
😪 🍄 🔯 Aventail Advanced Reporting Setup-Administrative User 🛛 🖄 🔹 🖾 🗠	\blacksquare • \blacksquare Page • \textcircled{O} Tools • $\overset{\circ}{}$
Aventail 💷	<u> </u>
Aventail Advanced Reporting Setup	
Administrative User	
Please choose an administrative username and password. Note, you will need to enter this username and password whenever you access Aventail Advanced	Reporting in the future.
Username: admin	
Password:	
Re-type password:	
Next	
	v
Done	. 🛛 🔍 100% 👻 🎢



If you would like to allow Aventail Advanced Reporting to send information about the devices you are analyzing to the development team, check the box and then select Next:

🤌 Aventail Advanced Reporting Satup-Automated Feedback Agent - Windows Internet Explorer
🕞 🕤 👻 http://127.0.0.1:8987/?dp+templates.setup
<u> E</u> ile <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp
😭 🍄 🔯 Aventail Advanced Reporting Setup-Automated Feed 👌 🔹 🗟 🔹 🤤 Page 🔹 🎯 Tools 🔹
Aventail 🐖
Aventail Advanced Reporting Setup
Automated Feedback Agent
Please help us to improve Aventail Advanced Reporting by automatically sending us the types of devices you analyze.
Aventail Advanced Reporting will not send your log data or any other personal information; it will only send non-specific demographic information: log formats autodetected, log formats selected, platform, success/failure of first database build, license type (not key), and database type.
Uncheck this option if you do not want Aventail Advanced Reporting to send any information.
 Yes, I agree to allow Aventail Advanced Reporting to send information about the types of devices I analyze (via port 80) to the Aventail Advanced Reporting development team.
Done



Please make sure that any Antivirus scans on the system do not include the Aventail Advanced Reporting directory then click Next:

🔗 Aventail Advanced Reporting Setup-Antivirus Warning - Windows Internet Explorer 📃	X
🕞 🕞 👻 http://127.0.0.1:8987/?dp+templates.setup 💽 🚱 🗙 Live Search 🔎	•
Eile Edit View Favorites Iou's Help	
😪 🍄 🔯 Aventail Advanced Reporting Setup-Antivirus Warning 🏠 🔹 🔝 🔹 🎰 🖓 Page 🔹 🍥 Tools 🔹	»
Aventail 🕮	
Aventail Advanced Reporting Setup	
Antivirus vvarning	
Please disable any active antivirus scanning of Aventail Advanced Reporting's installation directory	
Active-scanning antivirus software (and automatic disk defragmentation software), which runs continually and monitors all files on the disk, can interfere with Aventail Advanced Reporting's operation. This software may incorrectly conclude that Aventail Advanced Reporting's database files contain viruses (they don't), causing it to modify or delete the files, resulting in database corruption. This can cause log processing and report generation to fail. This type of software also slows Aventail Advanced Reporting down considerably, making it as much as 20 times slower in extreme cases.	
So, you must disable scanning of the directory where Aventail Advanced Reporting is installed, in order for Aventail Advanced Reporting to operate properly. It is not necessary to disable the active-scanning software entirely; you can just configure it so it does not scan Aventail Advanced Reporting's files (most antivirus products can be configured to exclude certain directories for their scanning).	
Once you have disabled scanning of Aventail Advanced Reporting's directory, click Next. You can also proceed without disabling scanning, but you may experience the problems described above.	_
Next	-
Done	-//



Select Finish to complete the Initial setup:

🤗 Aventail Advanced Reporting Setup-Complete Setup - Windows Internet Explorer	
	₽ •
<u>File Edit View Favorites Iools Help</u>	
😪 🎄 🜠 Aventail Advanced Reporting Setup-Complete Setup	age \star \bigcirc Tools \star »
Aventail 🐻	<u> </u>
Aventail Advanced Reporting Setup	
Complete Setup	
You are almost done, please click on the Finish button to complete the setup.	
Thank you for choosing Aventail Advanced Reporting.	
Finish	
	T
Done	🔍 100% 🔹 🎢



Configuring Aventail Advanced Reporting

After you complete the initial setup, you will be presented with the Aventail Advanced Reporting login menu. Enter in the name and password of the Administrator account that you defined during the initial setup:





After logging in, you will be presented with the Profile page to create a new Profile. A Profile is a log data source that will be used as input into the AAR system.

From the Profiles Page, select 'Start here' to launch the new profile wizard:

🖉 Aventail Advanced Reporting A	dmin - Windows Internet Explorer		IX
😋 🕤 👻 🥳 http://127.0.0.1:89	987/?dp+templates.admin.index	💽 🗲 🗙 Live Search 🖉	
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	: <u>H</u> elp		
🚖 🔅 👰 Aventail Advanced Rep	orting Admin	🟠 🔹 🔝 👻 🆶 🔹 📴 Page 🔹 🎯 T <u>o</u> ols 🔹	, »
Aventail 🐖 Professional		Logged in as 'admin' Logout Help Abo	ut
Admin			
• Profiles			
Scheduler	Profiles	Create New Profile	
Preferences	No profiles exist.		
Tasks			
Licensing	» Start here		
Support	to create a new profile and view reports.		
	© 2000 Flowerfire		
	© 2009 Flowenine		
			-
http://127.0.0.1:8987/?dp+templates.a	dmin.profiles.profiles_view	😜 Internet 🔍 100% 🔻	• //



Select Browse to browse the local hard drive and navigate to the folder where the Aventail access logs are stored:

🌽 Aventail Adv	anced Reporting - Windows Internet Explorer					_	
Nttp://127.0.0	8987/?dp+templates.admin.new_profile_wizard.in	idex					<u> </u>
New Pro	file Wizard		Back		Next	Cancel	
Log sou	rce						
Please spec	ify where you would like Aventail Advanced Rep	porting to g	get your log	g data fror	n. <u>More inform</u>	<u>iation</u>	
Log source: Pathname:	e.g.: C:\logs\access.log, C:\logs*.log, \\ho	st\share\	dir\ex*.lo	9	Browse	1	
	Process subfolders (local folders only)					1	
	Pattern is a regular expression						
	Show Matching Files						
							v
Done				😜 Intern	iet	🔍 100%	• //



Select a file (extranet_access.log) and then click OK:

Browse folders and files - Windows Ir	iternet Exp	lorer	
Mttp://127.0.0.1:8987/?dp+templates.sha	red.file_man	ager.index+volatile.pathnam	e_field_id+local_pathnam
OK Cancel Sho	w Root	Show Drive: 💌	Network Shares
Use arrows to expand, click on folder	or file nam	ne to select it.	<u> </u>
🖙 🖼 C:\Documents and Setting	js∖Admini	strator\Desktop\Log	s\
extranet_access.log	Оb		
extranet_access.log.1	1 K		
extranet_access.log.2	4 K		
extranet_access.log.3	48 K		
extranet_access.log.4	4 K		
extranet_access.log.5	7 K		
extranet_access.log.6	3 K		
extraweb_access.log	80 K		
extraweb_access.log.1	584 K		
extraweb_access.log.2	410 K		
extraweb_access.log.3	13 K		
extraweb_access.log.4	282 b		
extraweb_access.log.5	232 K		
extraweb_access.log.6	221 K		
extraweb_access.log.7	204 K		
extraweb_access.log.8	1 M		<u> </u>
		Internet	🔍 100% 🔻 //.



Modify the pathname so all extranet_access.log files in the Logs directory are retrieved. Change extranet_access.log to extranet_access*.* and check the box to Process subfolders (local folder only).

Then select 'Show Matching Files' to make sure that all the extranet_access.log files are retrieved:

🥭 Aventail Advanced Reporting - Windows Internet Explorer			_ [×
🛃 http://127.0.0.1:8987/?dp+templates.admin.new_profile_wizard.index				•
				A
New Profile Wizard	Back	Next	Cancel	
Log source				
Please specify where you would like Aventail Advanced Reporting t	o get your log data 1	from. <u>More inform</u>	nation	
Log source: Local disk				
e.g.: C:\logs\access.log, C:\logs*.log, \\host\shar	e\dir\ex*.log	+ Drawaa	1	
Painname. juments and Settingsvadministrator/Desktop/Logs	extranet_access".	Browse]	
Process subfolders (local folders only)				
Pattern is a regular expression				
Show Matching Files				
Show Matching Thes				
	Int	ternet	a 100%	• //



If all the correct log files are retrieved, then Close the Matching Log Source Files and select Next to go to the next step. Otherwise, go back and modify the Pathname field until the correct logs are retrieved.

:

Atching Log Source Files - Windows Internet Explorer		
http://127.0.0.1:8987/?dp+templates.shared.matching_log_source_files.matching_log_source	_files+volatil	e.I 💌
Close		<u> </u>
Matched 7 log source files:		
C:\Documents and Settings\Administrator\Desktop\Logs\extranet_access.log		
C:\Documents and Settings\Administrator\Desktop\Logs\extranet_access.log.1		
C:\Documents and Settings\Administrator\Desktop\Logs\extranet_access.log.2		
C:\Documents and Settings\Administrator\Desktop\Logs\extranet_access.log.3		
C:\Documents and Settings\Administrator\Desktop\Logs\extranet_access.log.4		
C:\Documents and Settings\Administrator\Desktop\Logs\extranet_access.log.5		
C:\Documents and Settings\Administrator\Desktop\Logs\extranet_access.log.6		
<u> </u>		-
Done Solution Solutio	🔍 100%	• //



AAR will then automatically detect the log file format. Leave the default of Aventail Client/server Access Log Format and select Next:

Note: If you are running 10.x firmware on the Aventail appliance, you must load a new AAR configuration file to recognize this log. Please see the step above on page 10 for more details.

Ø Aven	ail Advanced Reporting - Windows Internet Explorer				
👰 http:/	/127.0.0.1:8987/?dp+templates.admin.new_profile_wizard.index				•
					<u> </u>
Ne	w Profile Wizard	Back	Next	Cancel	
Log	format detected				
Aven	tail Advanced Reporting detected the log format:				
Aver	tail Client/server Access Log Format				
o	Continue with the above detected log format (recommended).				
0	Choose a different log format on the next wizard page.				
	Use this option if you want to manually choose a log format. If have been detected then <u>click here</u> for instructions.	/ou believe that	a different log form	at should	
					_
Done			Internet	🔍 100%	• //.



Leave all the defaults for Numerical field options and select Next:

Ø Aver	ntail Advanced F	Reporting - W	indows Internet Ex	plorer			_	
👰 http:	//127.0.0.1:8987	/?dp+templates	.admin.new_profile_w	izard.index				•
Ne	ew Profile √	vizard			Back	Next	Cancel	
Nu	umerical fiel	ld options						
Plea	ase select the n	umerical field:	s which you would l	ike to have in th	e reports. <u>More ir</u>	nformation		
	Connections	Select All	Deselect All					
	Visitors							
	Bytes in							
	Bytes out							
	Duration							
								-
Done						nternet	🔍 100%	•



Change the Profile name to reflect the type of reports that will be displayed (e.g. Network Tunnel client/server access):

🥖 Aventail Advanced Reporting - Windows Internet Explorer			_ _ ×
http://127.0.0.1:8987/?dp+templates.admin.new_profile_wizard.index			<u> </u>
			<u> </u>
New Profile Wizard	Back	Finish	Cancel
Profile name			
Please define a name for the new profile and click the Finish button			
Profile name: Network Tunnel client/server access			
✓ Show reports upon finish			
			=
Done	In 😜 In	ternet	100% • //



Then select Finish to build the database and display the reports. When the database build is complete, the Reports page will be shown starting with the Overview page:





Now that the Network Tunnel client/server Profile is complete, you must add a new Profile for the Web access logs. From the Overview menu select 'Admin' in the upper right corner of the page and then select Profile:

Sector 2 Aventail Advanced Reporting Ac	lmin - Windows Internet Explorer				-	
	37/?dp+templates.admin.index		• +,	X Live Search		P -
File Edit View Favorites Tools	Help					
🙀 🎄 🥳 Aventail Advanced Repo	orting Admin			🟠 • 🔊 - 🖨	▼ 📝 Page ▼ 🍥 Tool:	s •
Aventail 🕵 Professional	1			Logged in as 'adı	min' Logout Help A	bout
Admin						
• Profiles						<u> </u>
Scheduler	Profiles				Create New Profile	
Users						
Preferences	Network Tunnel client/server access	View Reports	<u>View Confiq</u>		<u>Delete</u>	
licensing						
Support	© 2000 Elawarfira					
	© 2009 Flowernire					
						~
				😽 Internet	100%	• //



From the Profile menu, select 'Create new profile' to begin the process again except this time the log file names will be extraweb_access*.* as show below:

🧭 Aventail Advanced Reporting - Windows Internet Explorer			
Main http://127.0.0.1:8987/?dp+templates.admin.new_profile_wizard.index			-
New Profile Wizard	Back	Next	Cancel
Log source			
Please specify where you would like Aventail Advanced Reporting to) get your log data fror	n. <u>More informatic</u>	<u>on</u>
Log source: Local disk			
e.g.: C:\logs\access.log, C:\logs*.log, \\host\shar Pathname: uments and Settings\Administrator\Desktop\Logs\a	//dir/ex*.log xtraweb_access*.*	Browse	
Process subfolders (local folders only)			
Pattern is a regular expression			
Show Matching Files			
Done	Interr	net	🔍 100% 👻 🎢



Check the matched log file to make sure the Pathname is correct and all the files are retrieved:

🥖 Matching Log Source Files - Windows Internet Explorer
http://127.0.0.1:8987/?do+templates.shared.matching_log_source_files.matching_log_source_files+v
Matched 10 log source files:
C:\Documents and Settings\Administrator\Desktop\Logs\extraweb_access.log
C:\Documents and Settings\Administrator\Desktop\Logs\extraweb_access.log.1
C:\Documents and Settings\Administrator\Desktop\Logs\extraweb_access.log.2
C:\Documents and Settings\Administrator\Desktop\Logs\extraweb_access.log.3
C:\Documents and Settings\Administrator\Desktop\Logs\extraweb_access.log.4
C:\Documents and Settings\Administrator\Desktop\Logs\extraweb_access.log.5
C:\Documents and Settings\Administrator\Desktop\Logs\extraweb_access.log.6
C:\Documents and Settings\Administrator\Desktop\Logs\extraweb_access.log.7
C:\Documents and Settings\Administrator\Desktop\Logs\extraweb_access.log.8
C:\Documents and Settings\Administrator\Desktop\Logs\extraweb_access.log.9
·
Done



Leave the default Log format of Aventail Web Access Log Format:

🏉 Avent	ail Advanced Reporting - Windows Internet Explorer			
👰 http://	/127.0.0.1:8987/?dp+templates.admin.new_profile_wizard.index			•
	r			<u>~</u>
Nev	v Profile Wizard	Back	Next	Cancel
Log	format detected			
Aven	tail Advanced Reporting detected the log format:			
Aver	tail Web Access Log Format			
~	Continue with the above detected law formet (recommended)			
Ū	Continue with the above detected log format (recommended)			
0	Choose a different log format on the next wizard page.			
	Use this option if you want to manually choose a log format. I	fyou believe that :	a different log forr	nat should
	have been detected then <u>click here</u> for instructions.			
				-
Done		()	internet	🔍 100% 👻 🂋



Leave the default Numerical field options:

Aventail Advanced	J Reporting - Windows Internet Ex 37/2dp+templates.admin.new_profile_w	plorer vizard.index				
	······································					
New Profile	Wizard		Back	Next	Cancel	
Numerical fi	eld options					
Please select the	numerical fields which you would I	ike to have in the	e reports. <u>More ir</u>	nformation		
I Hits	Select All Deselect All					
🗹 Page views						
✓ Visitors						
Size						
						-
Done				nternet	🔍 100%	•



Change the Profile name to reflect the type of reports that will be displayed (e.g. Web Access):

Sector Aventail Advanced Reporting - Windows Internet	Explore						
http://127.0.0.1:8987/?dp+templates.admin.new_profile	e_wizard.ir	ndex					_
New Profile Wizard			B	ack	Finish	Cancel	
Profile name							
Please define a name for the new profile and click	the Finis	sh button					
Profile name: Web Access							
Show reports upon finish							
							~
Done				II 😜 Ir	nternet	🔍 100%	• //



When complete, there should be two Profile Definitions to generate reports from:

Saventail Advanced Reporting A	dmin - Windows Internet Explorer				_ [X
	987/?dp+templates.admin.index		• 4	X Live Search		- C
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools	; <u>H</u> elp					
🔆 🎄 🚮 Aventail Advanced Rep	orting Admin			🐴 • 🗟 - 🖶	⋆ → Page ⋆ → Tools	• »
Aventail 🕵 Professional	- 1 1			Logged in as 'adr	nin' Logout Help Ab	out
Aventantes						
Admin						
• Profiles						
Scheduler	Profiles				Create New Profile	
Users						
Preferences	Network Tunnel client/server access	View Reports	<u>View Confiq</u>		<u>Delete</u>	
licensing	Web Access	View Reports	<u>View Confiq</u>		Delete	
Support						
	© 2009 Flowertire					
						_
				Nernet 😌	🔍 100%	• //



Customization

Automated Log File Retrieval

There are two methods of automatically retrieving the SonicWALL Aventail access log files from the Aventail appliance to the AAR server.

1) Automatically push the logs from the Aventail appliance to the AAR Server:

A script is available on the SonicWALL Support Knowledge Portal which is located at <u>http://www.mysonicwall.com</u> to automate transfers of the Aventail access logs from the Aventail appliance to the AAR Server using SCP. For more information, please refer to Knowledge Base article #2455.

2) Automatically pull the logs from the Aventail appliance to a Windows AAR Server.

This retrieval method utilizes the pscp application which is a command line tool that is run automatically using the Windows Task Scheduler. The pscp application is a subset of PuTTy, the open source SSH client that can be downloaded from:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Open up Notepad and create the following file:

@echo off pscp -unsafe -pw aventail root@192.168.1.5:/var/log/aventail/extra*_access.log* c:\aventail_logs

This command uses two optional parameters. The –unsafe option allows for the use of wild cards when retrieving files. This allows all Aventail access logs to be retrieved with a single command. The –pw option includes the root password to the Aventail appliance to automatically establish the pscp session without further prompting. If this parameter is omitted, the administrator will be prompted to enter the root password. The –pw option is required for automated log retrieval.

Substitute your root password to the appliance following the -pw command and enter your appliance's IP address of the appliance after the @ sign

Save the file as Aventail_log_retrieval.bat extension into the same directory where the Aventail access logs are stored on the AAR Server (e.g. C:\Logs).

From the Windows Start menu, select Control Panel -> Scheduled Tasks -> Add Scheduled Task. This will bring up the Windows Scheduled Task Wizard. Click Next from the Wizard interface to select the task to be automated.



Click the Browse button and navigate to the C:\Logs folder. Highlight the Aventail_log_retrieval.bat file and click the Open button to select this task.

On the next screen, click the Daily radio button and then click Next to continue.

Select the Start Time for the task, click the every day radio button and select the start date. By default, the Scheduled Task Wizard uses the current system date of the AAR server. Click the Next button to continue.

Enter the username and password that will be used to run this task. Click Next to continue.

Click the Finish button to complete adding the task.

The log retrieval will now happen automatically each day.



Automated Database Build

Once the log files are copied to the AAR Server, they must be loaded into the database for subsequent analysis and reporting. AAR has an internal scheduler system to allow a scheduled build of the database after the log files have been copied.

To access the scheduler, from the main AAR page select Admin and then select Scheduler from the menu on the left side of the page:

Select New Action:





Select Build Database from the Action field, which Profile you want to build, and the time schedule:

Scheduler - New Action - Windows Internet Explorer	
Save and Close Cancel	<u> </u>
Action: Build database	
Profile: All profiles	
This field accepts any options available on the Aventail Advanced Reporting <u>Command</u> <u>Report Filters</u> can be applied by using the -f and -df option. Extra options:	<u> Line</u> .
Month Day Hour Minute Schedule: any 🔽 any 🔽 03 🔽 00 🔽	
	▼



Multiple Aventail Appliances

Since the log files on Aventail appliances all have the same names and are not unique, separate subdirectories must be created in the log file storage directory on the AAR server. For example, under the C:\Logs directory, there would be a separate directory for each appliance:

C:/Logs/node1 C:/Logs/node2 C:/Logs/node3

Copying the log files in their own directories will ensure that none of the files are overwritten. Aventail Advanced Reporting automatically collates the log files from the various appliances thereby providing a single view.

If you would like separate views of each appliance, then create a profile for each appliance and log file directory combination.

Every Aventail appliance has two sets of access logs, one for Tunnel client/server access auditing, extranet_access.log, and one for Web traffic auditing, extraweb_access.log. Therefore, a single appliance will require two Profiles. Due to licensing limitations, a single AAR server can support a maximum of five Profiles.

If there is a requirement to analyze and report on logs from more then two Aventail appliances, the Sawmill package can be purchased directly from Flowerfire with no limits on the number of Profiles or log sources.

Additional Customization

Numerous Knowledge Base articles are available on the SonicWALL Support Knowledge Portal which is located at <u>http://www.mysonicwall.com</u> covering additional topics on customization, reporting, and operation.

