Overview

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 (http://www.mysonicwall.com) 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

Upgrading

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

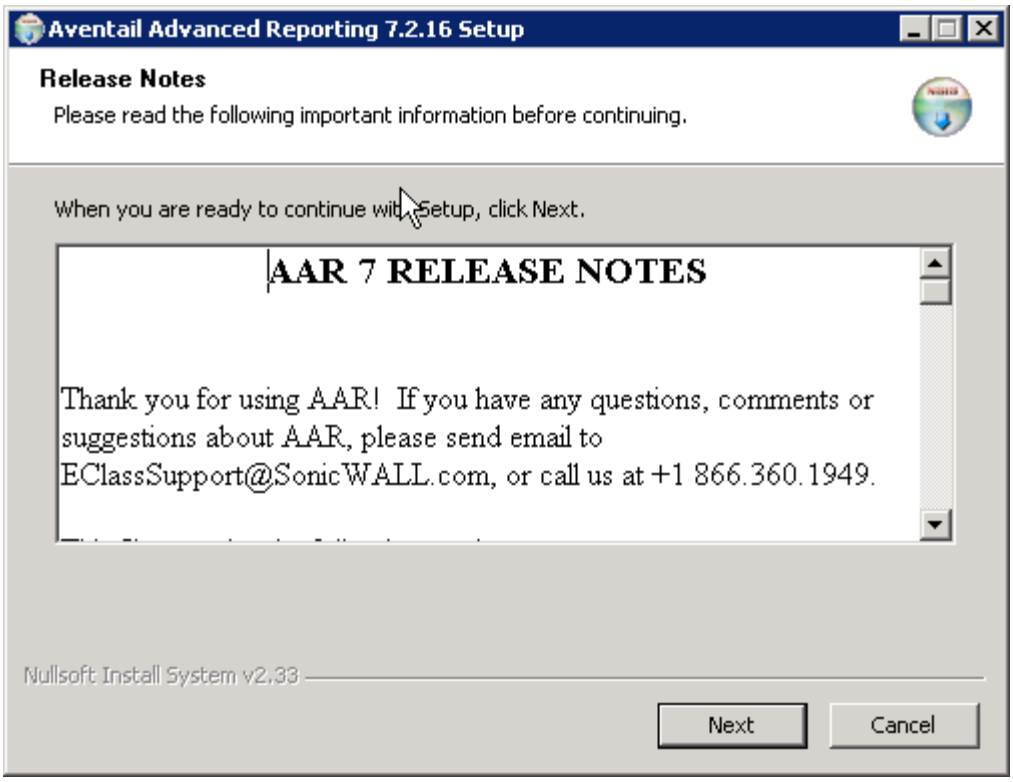
Aventail Advanced Reporting requires the libcrypto.so.4 library to run so this package may have to be installed on your Linux server. If you have a later version libcrypto library installed on your system, a link can be defined for AAR to use:

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

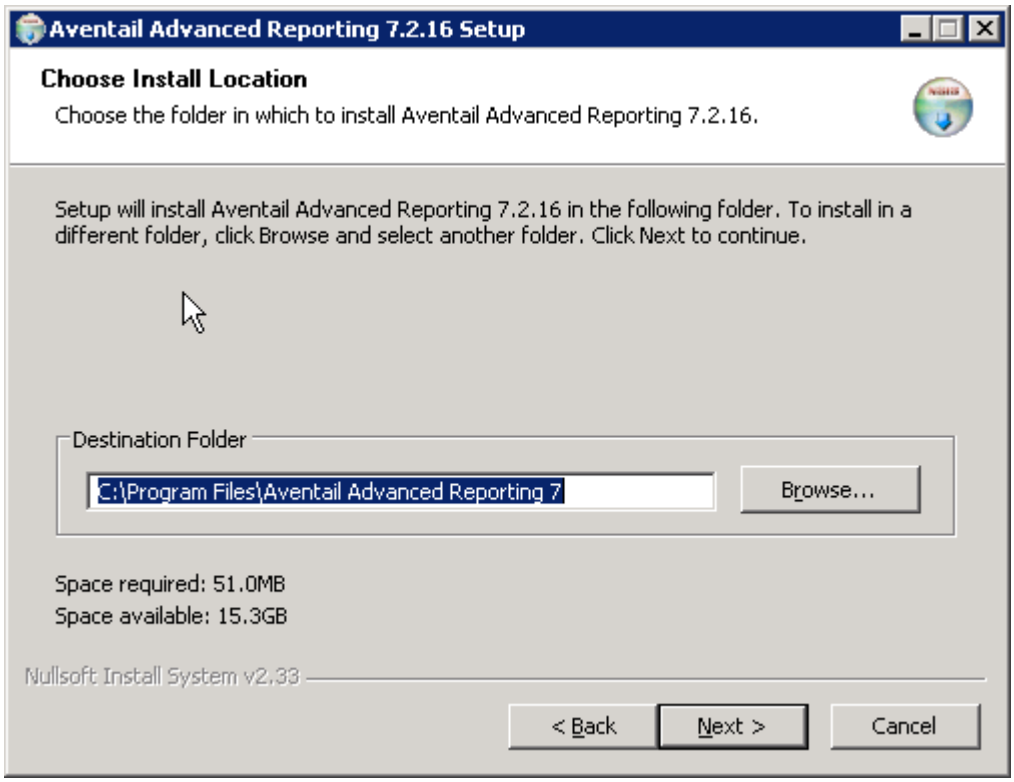
Windows

Execute the file aar7.2.16_x86_windows.exe.

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

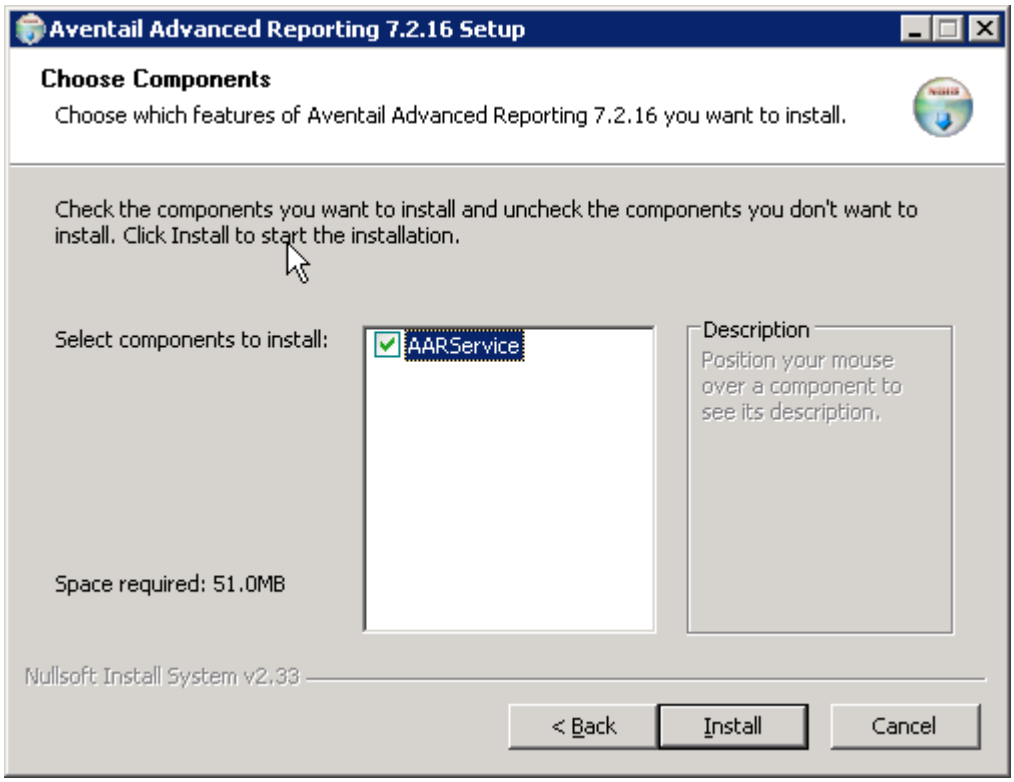


Choose a location to install AAR or leave the default location, then select Next:

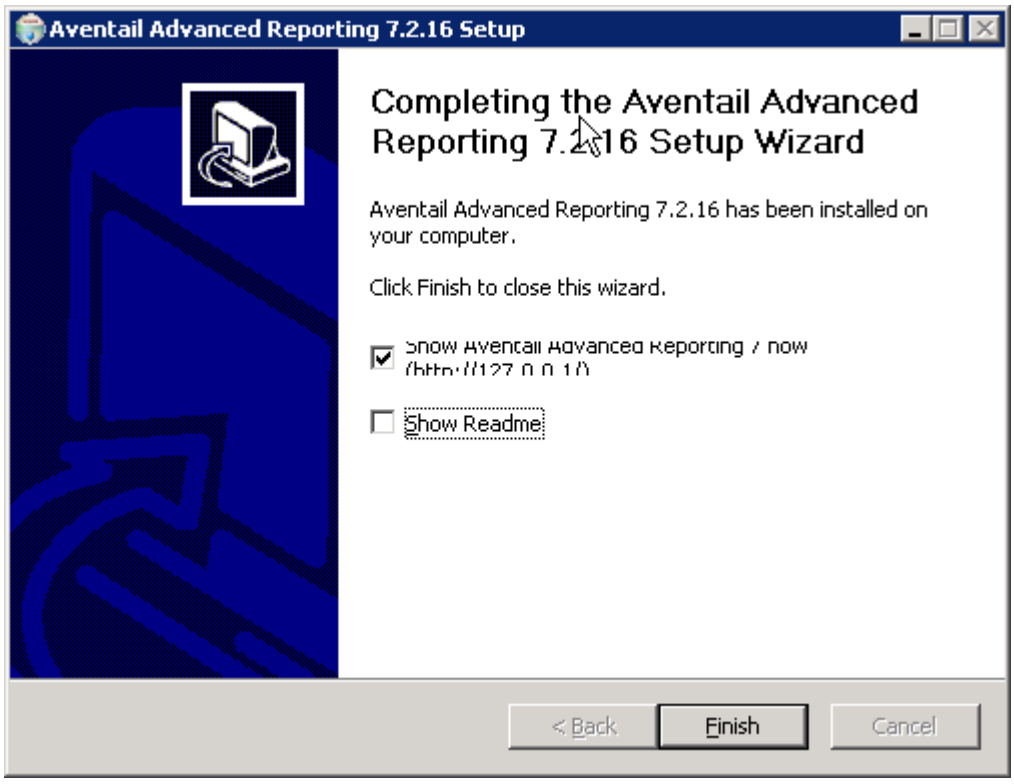


Choose, the AAR Components to install – leave the default setting for AARService:

Select Install to complete the installation.



Once complete, select Finish to access the AAR Console.



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.

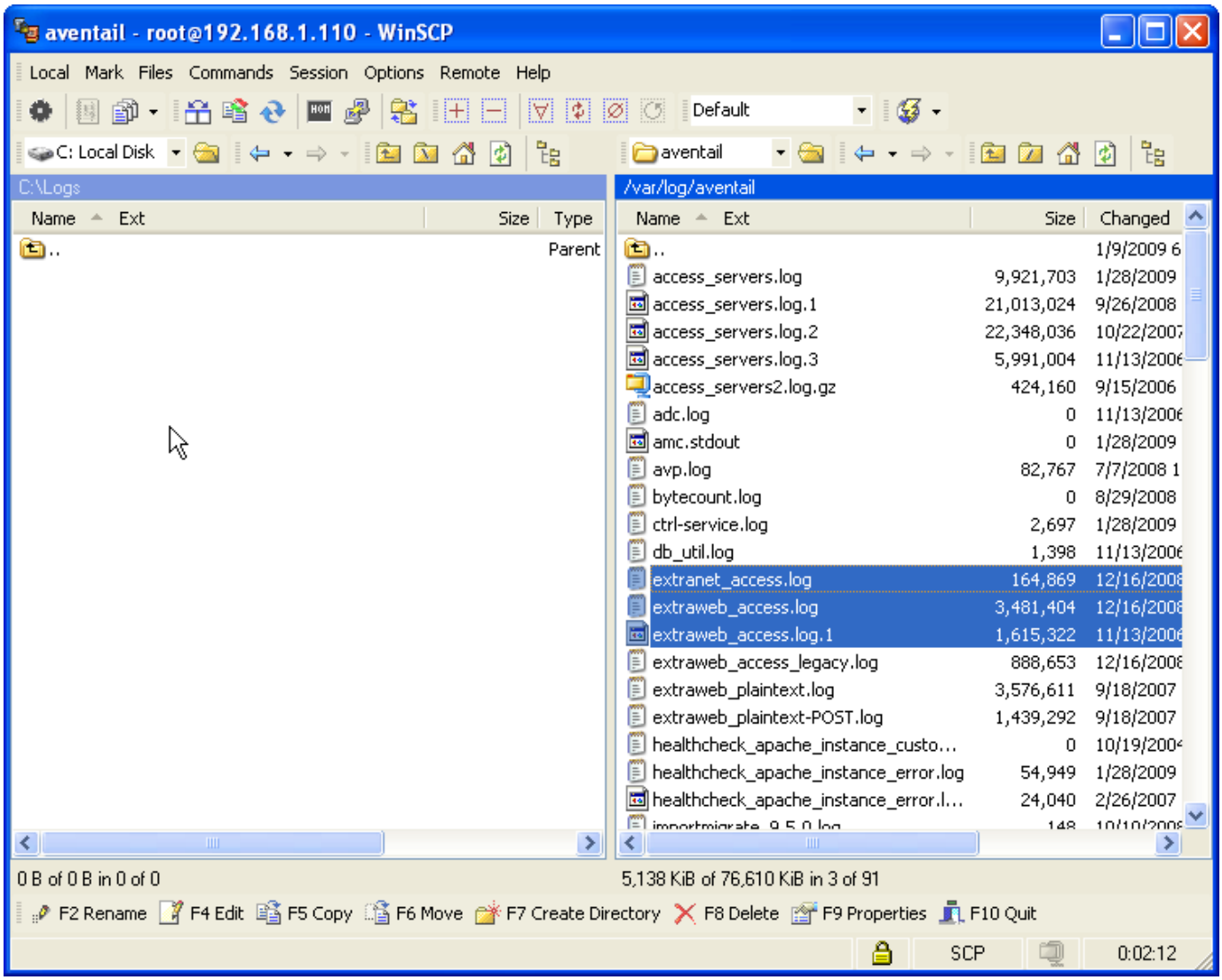
For a complete set of data, copy all of the files named extranet_access.log.* and extraweb_access.log.*

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

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:


aventail - root@192.168.1.110 - WinSCP
Local Mark Files Commands Session Options Remote Help
Default
C: Local Disk
aventail
C:\Logs
/var/log/aventail
Name Ext Size Type
Name Ext Size Changed
.. Parent
.. 1/9/2009 6
access_servers.log 9,921,703 1/28/2009
access_servers.log.1 21,013,024 9/26/2008
access_servers.log.2 22,348,036 10/22/2007
access_servers.log.3 5,991,004 11/13/2006
access_servers2.log.gz 424,160 9/15/2006
adc.log 0 11/13/2006
amc.stdout 0 1/28/2009
avp.log 82,767 7/7/2008 1
bytecount.log 0 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
healthcheck_apache_instance_error.l... 24,040 2/26/2007
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 F7 Create Directory F8 Delete F9 Properties F10 Quit
SCP
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.

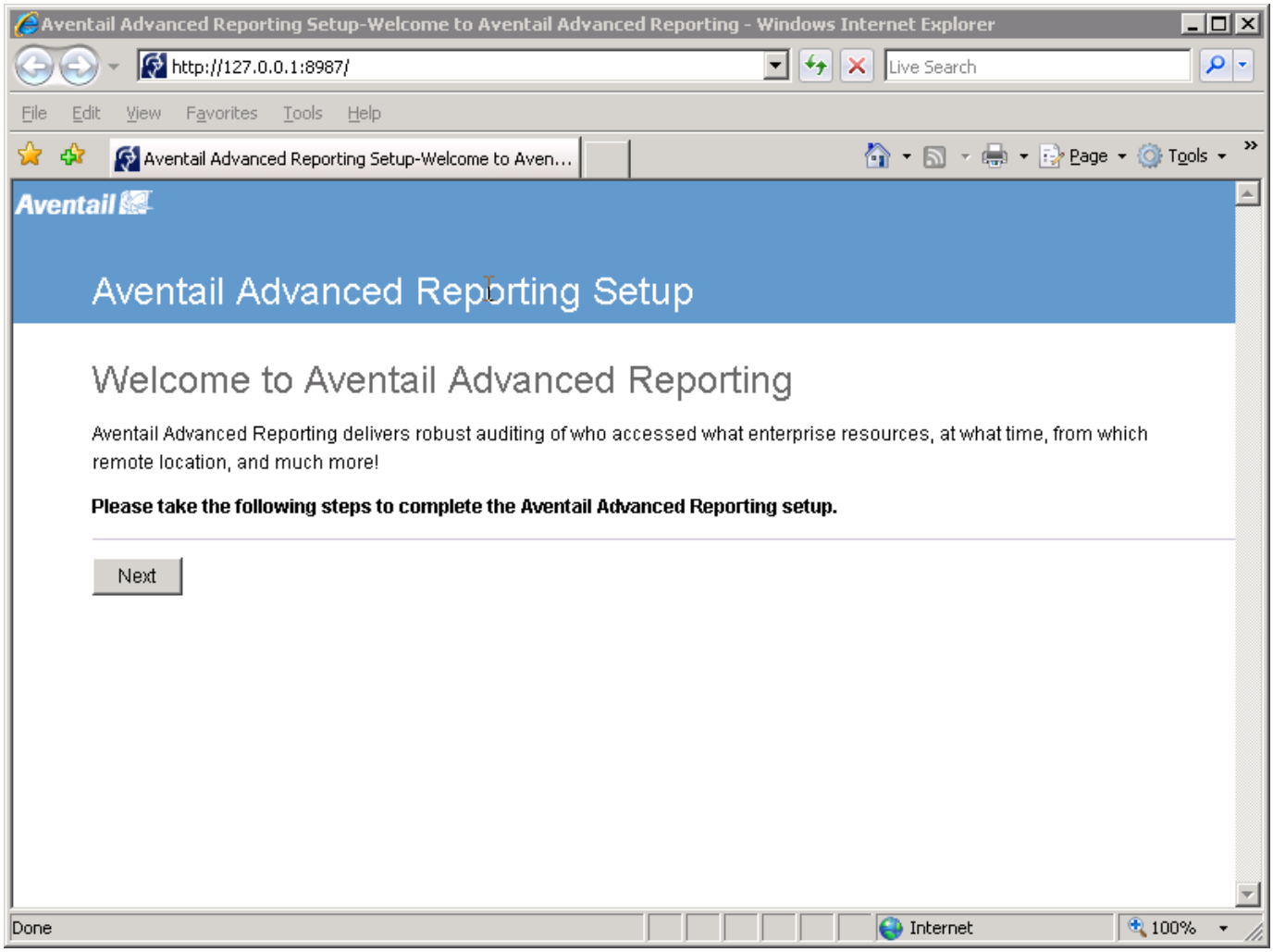
Initial Setup of Aventail Advanced Reporting

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 http://localhost:8987/ or http://127.0.0.1:8987

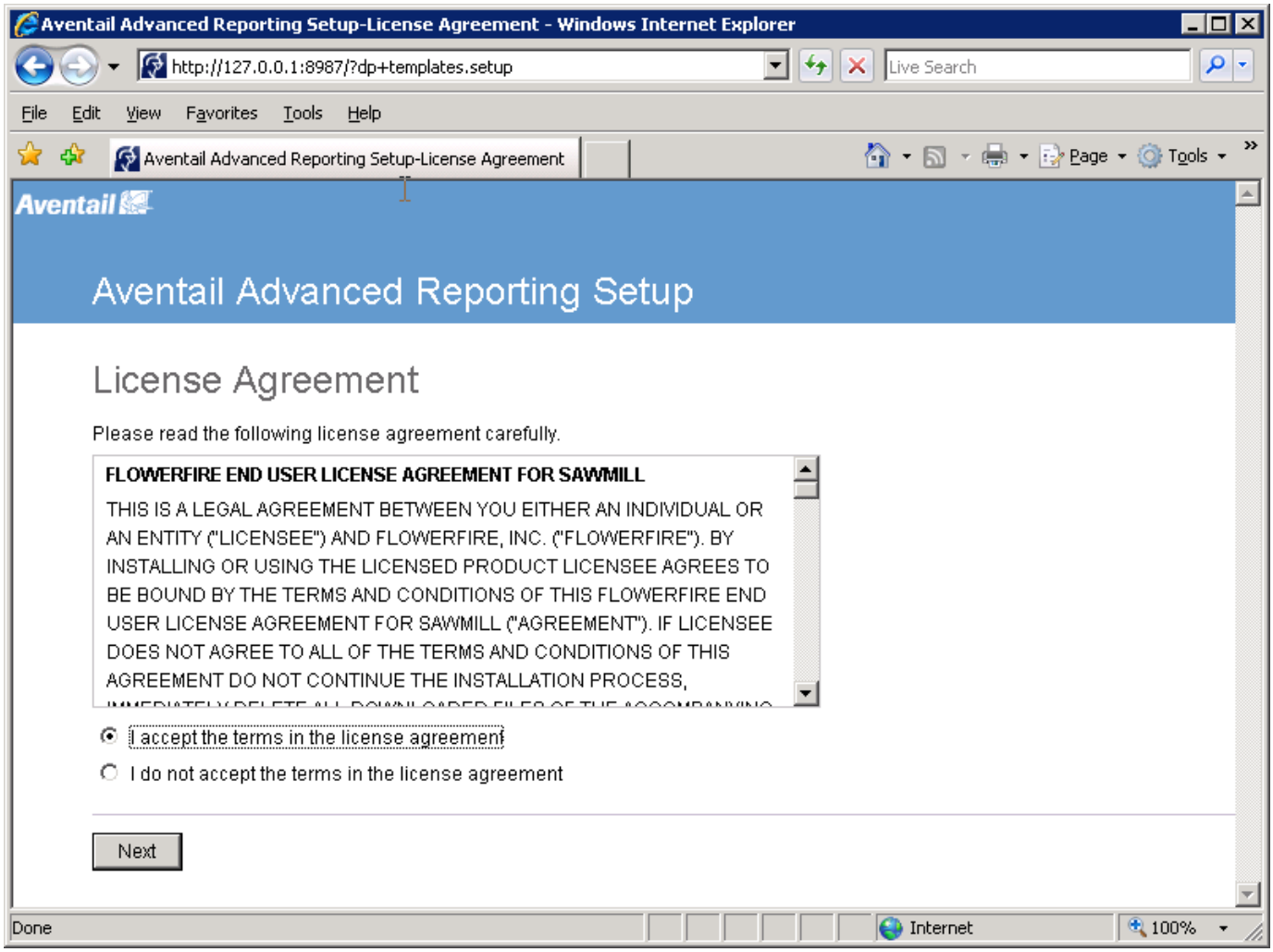
On Windows, the desktop icon can also be opened to access the AAR web application.

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

Select Next:

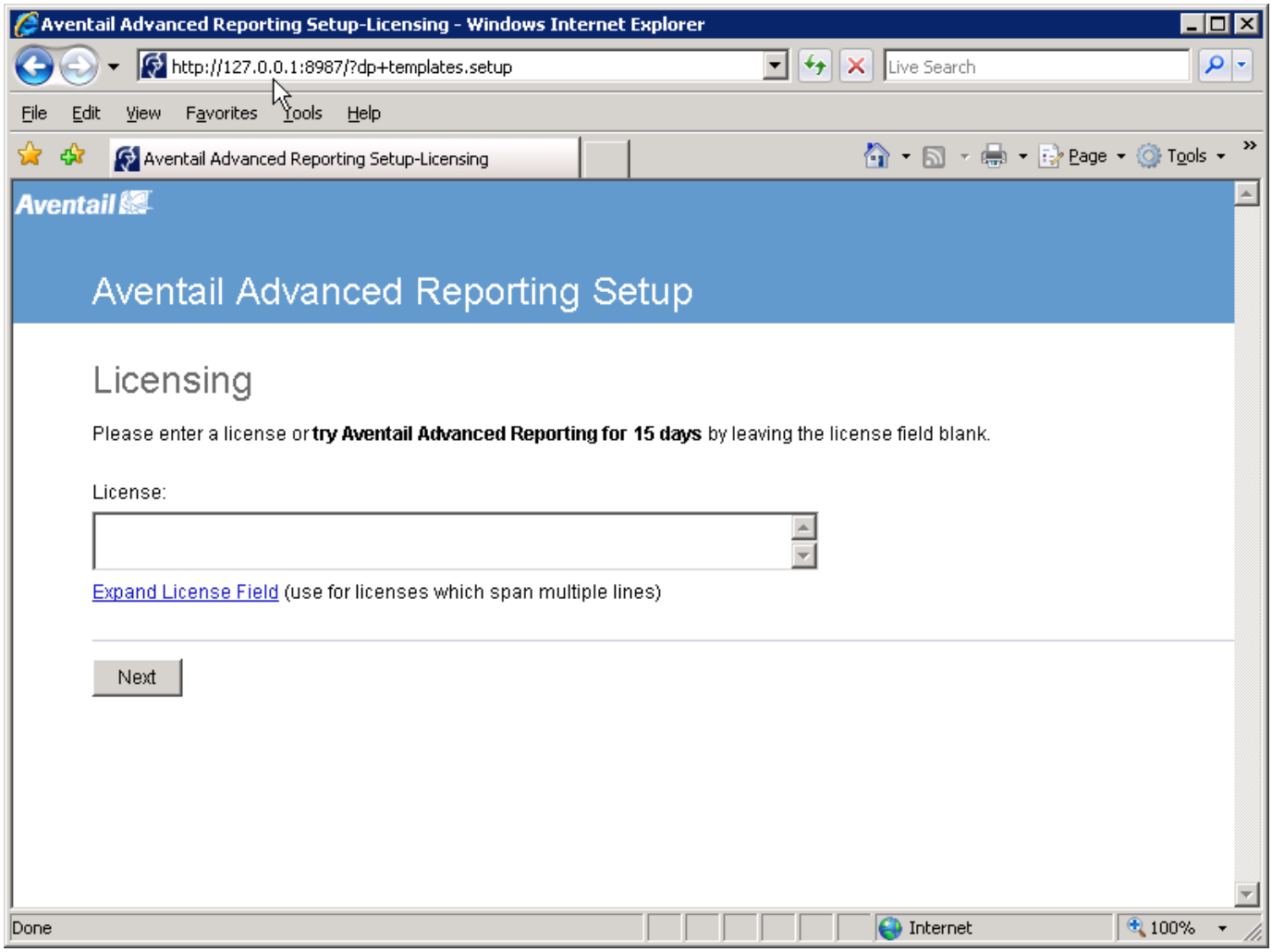

Aventail Advanced Reporting Setup-Welcome to Aventail Advanced Reporting - Windows Internet Explorer
http://127.0.0.1:8987/
Live Search
File Edit View Favorites Tools Help
Aventail Advanced Reporting Setup-Welcome to Aven...
Page Tools
Aventail
Aventail Advanced Reporting Setup
Welcome to Aventail Advanced Reporting
Aventail Advanced Reporting delivers robust auditing of who accessed what enterprise resources, at what time, from which remote location, and much more!
Please take the following steps to complete the Aventail Advanced Reporting setup.
Next
Done
Internet
100%

Read and accept the license agreement, then select Next

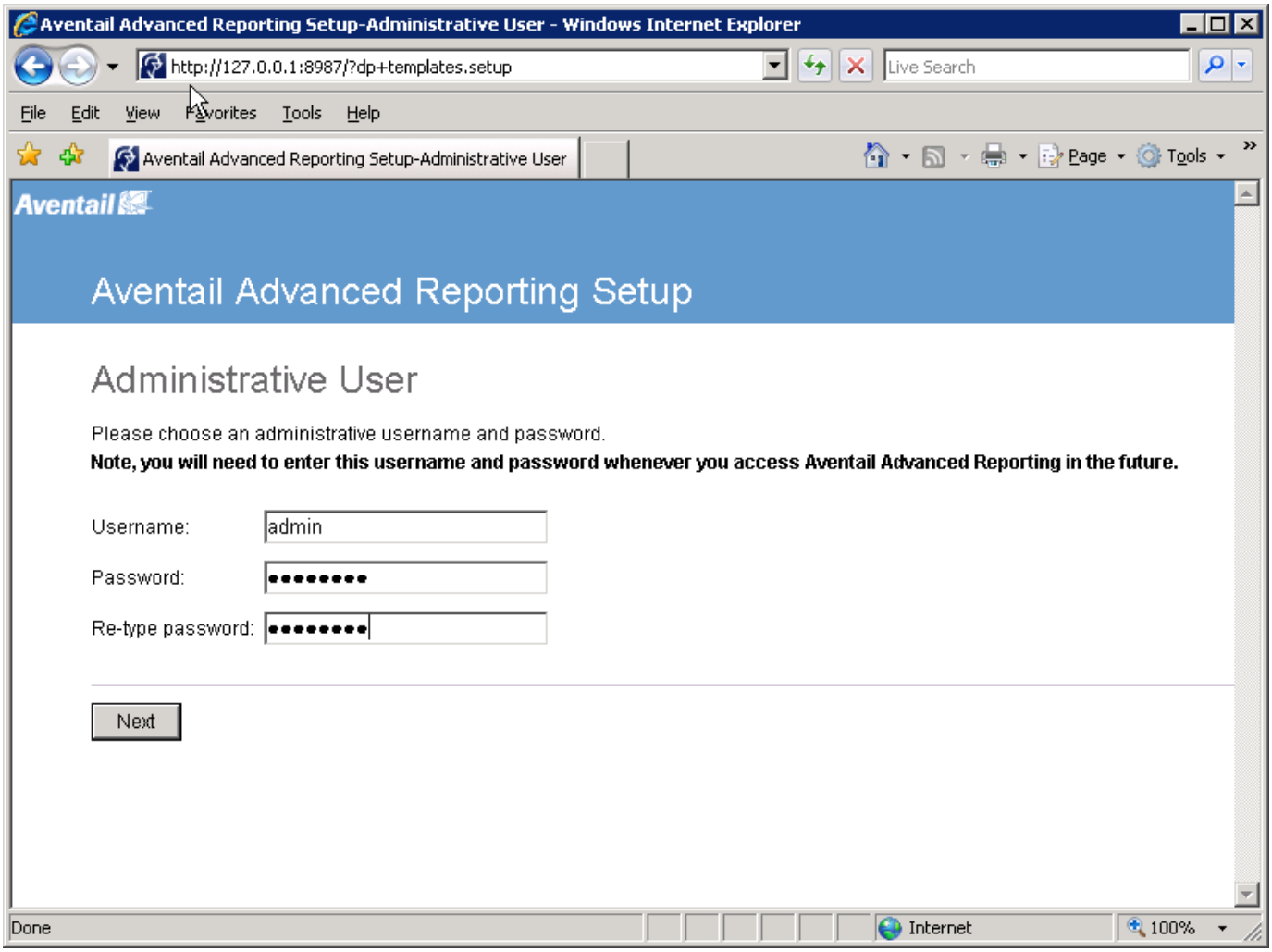


Enter in the license key obtained from your MySonicWall account in the appropriate field. If not, you can use Aventail Advanced Reporting free for 15 days.

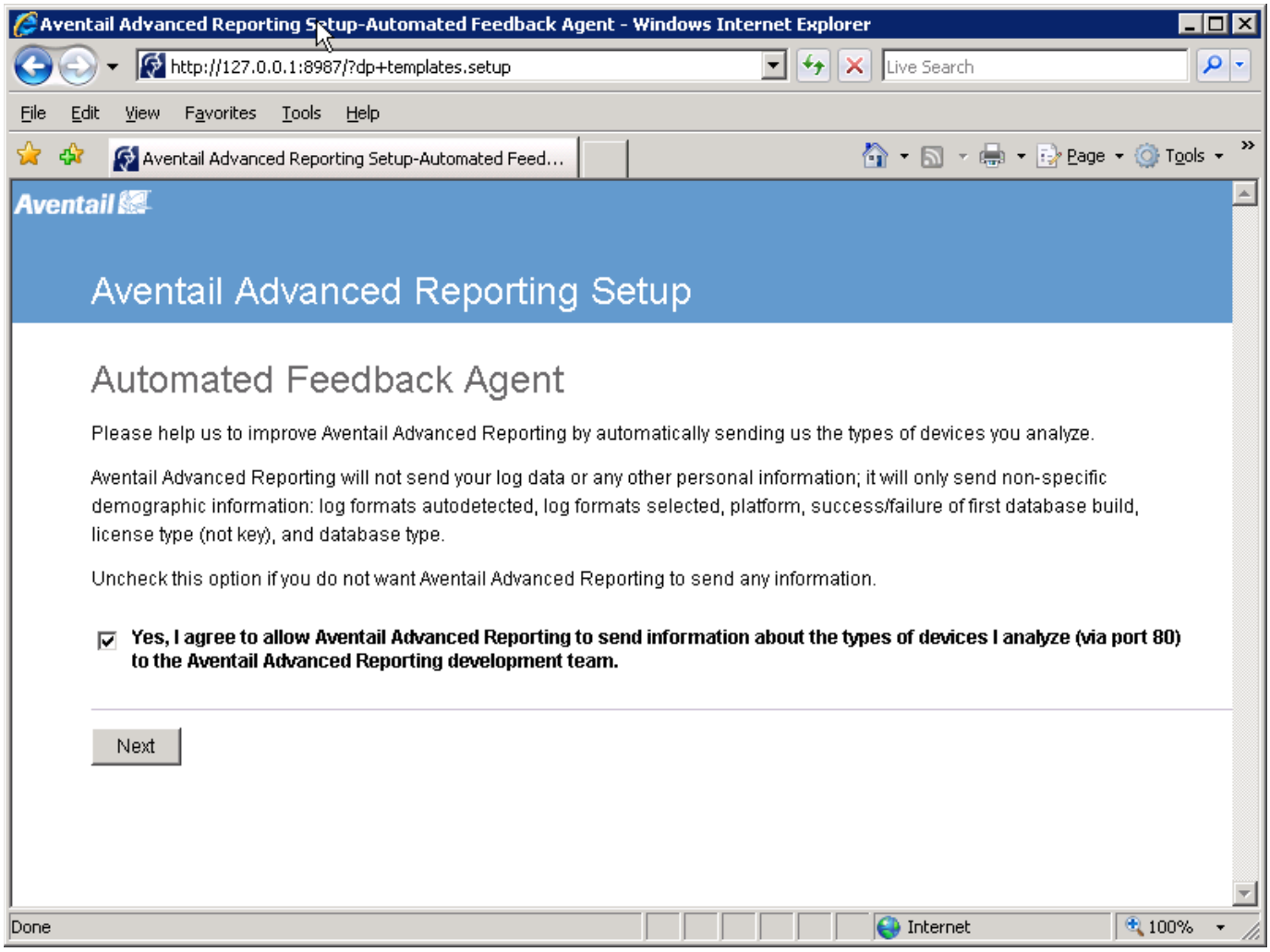
Select Next:



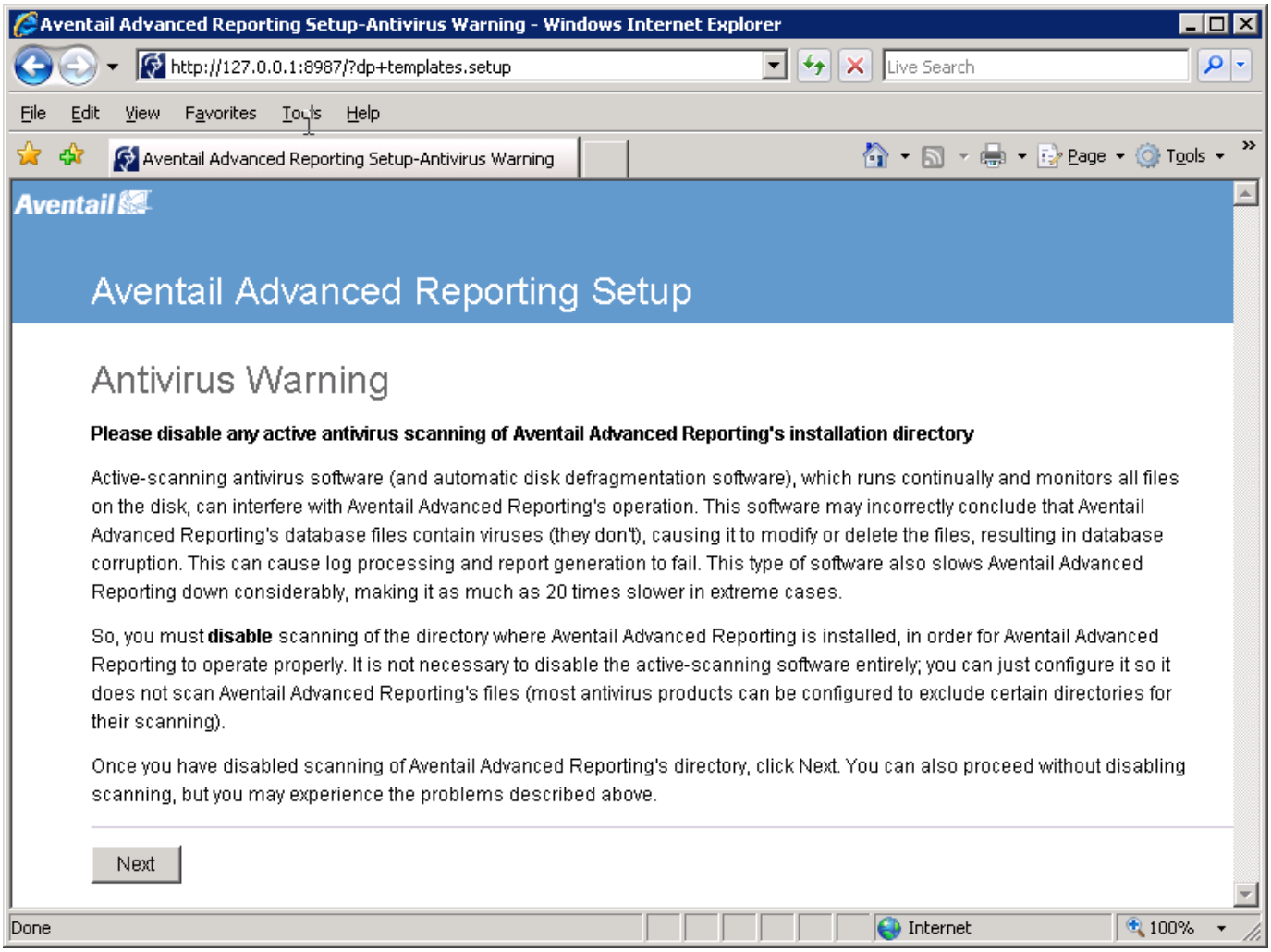
Enter in a username and password for the Aventail Advanced Reporting Administrator account. Then select Next:



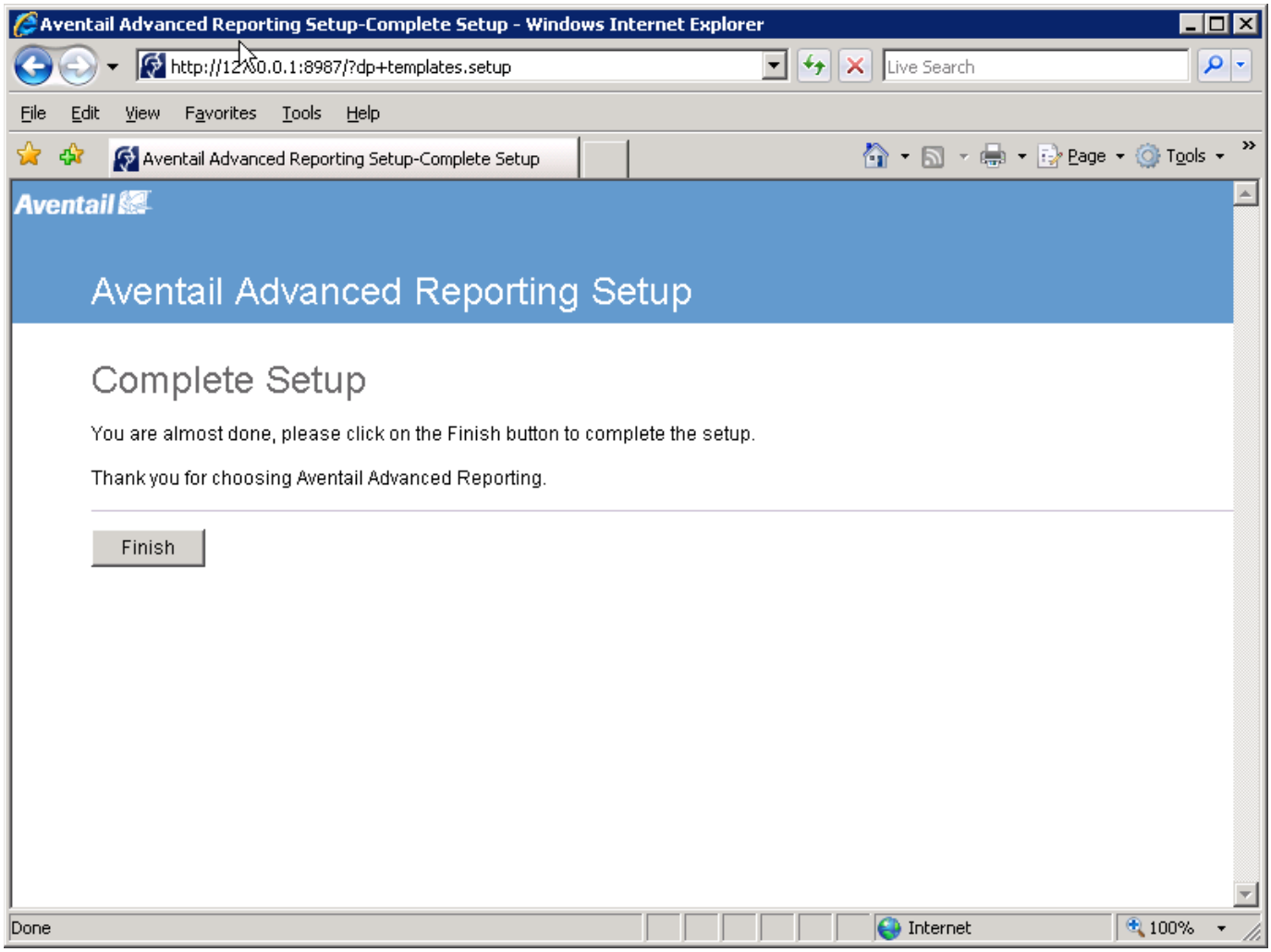
If you would like to allow Aventail Advanced Reporting to send information about the devices you are analyzing to the development team, check the box and then select Next:



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

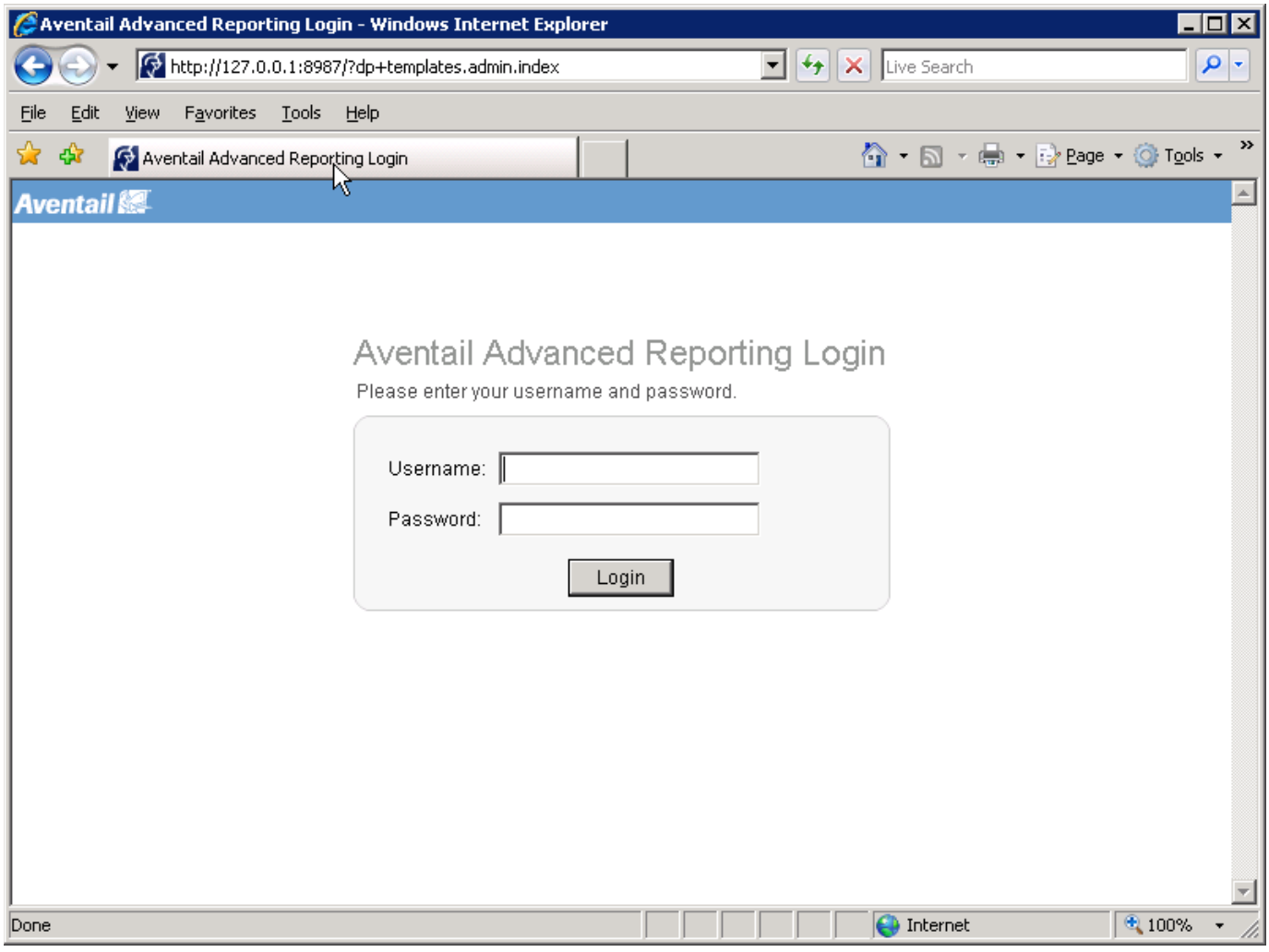


Select Finish to complete the Initial setup:



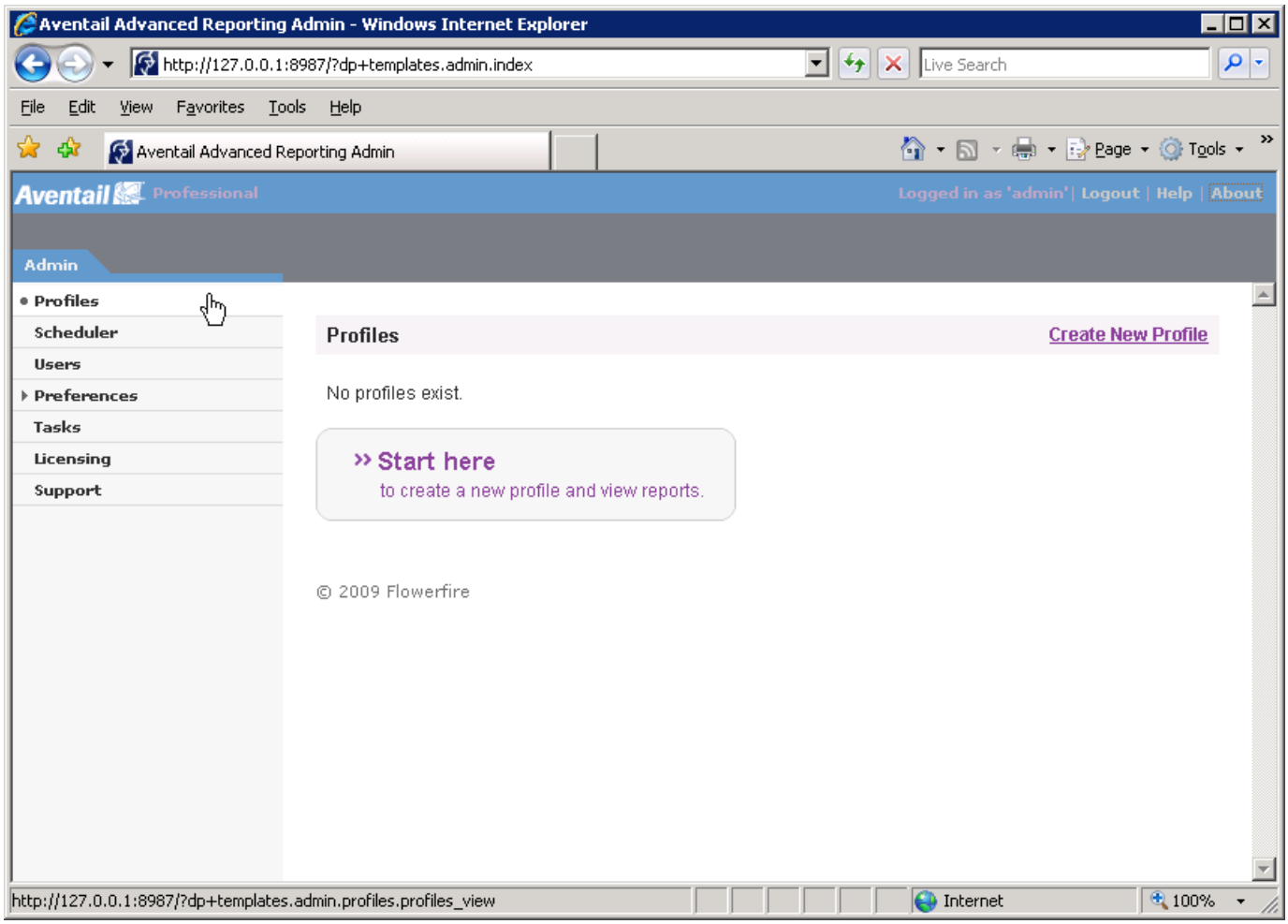
Configuring Aventail Advanced Reporting

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:

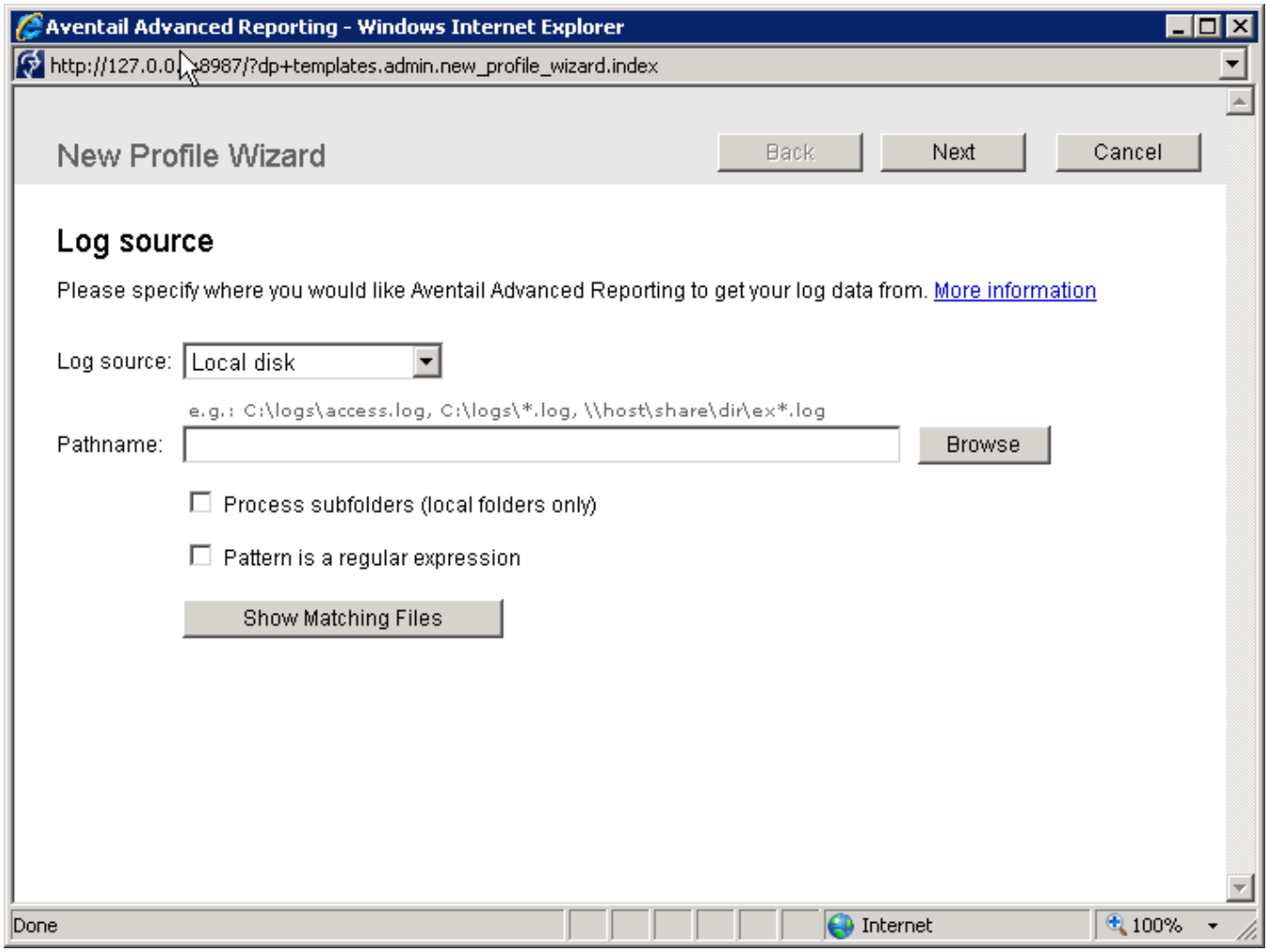


After logging in, you will be presented with the Profile page to create a new Profile. A Profile is a log data source that will be used as input into the AAR system.

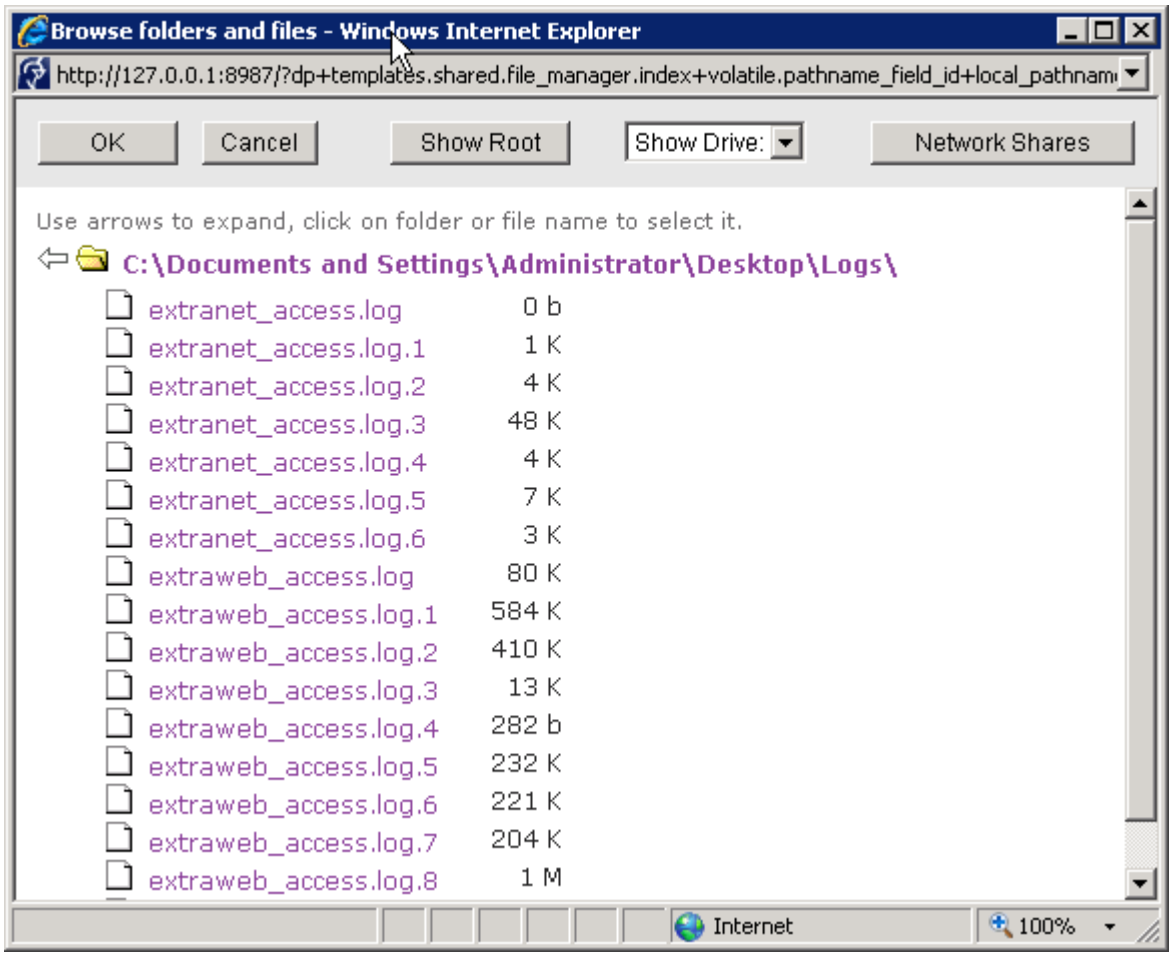
From the Profiles Page, select 'Start here' to launch the new profile wizard:



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

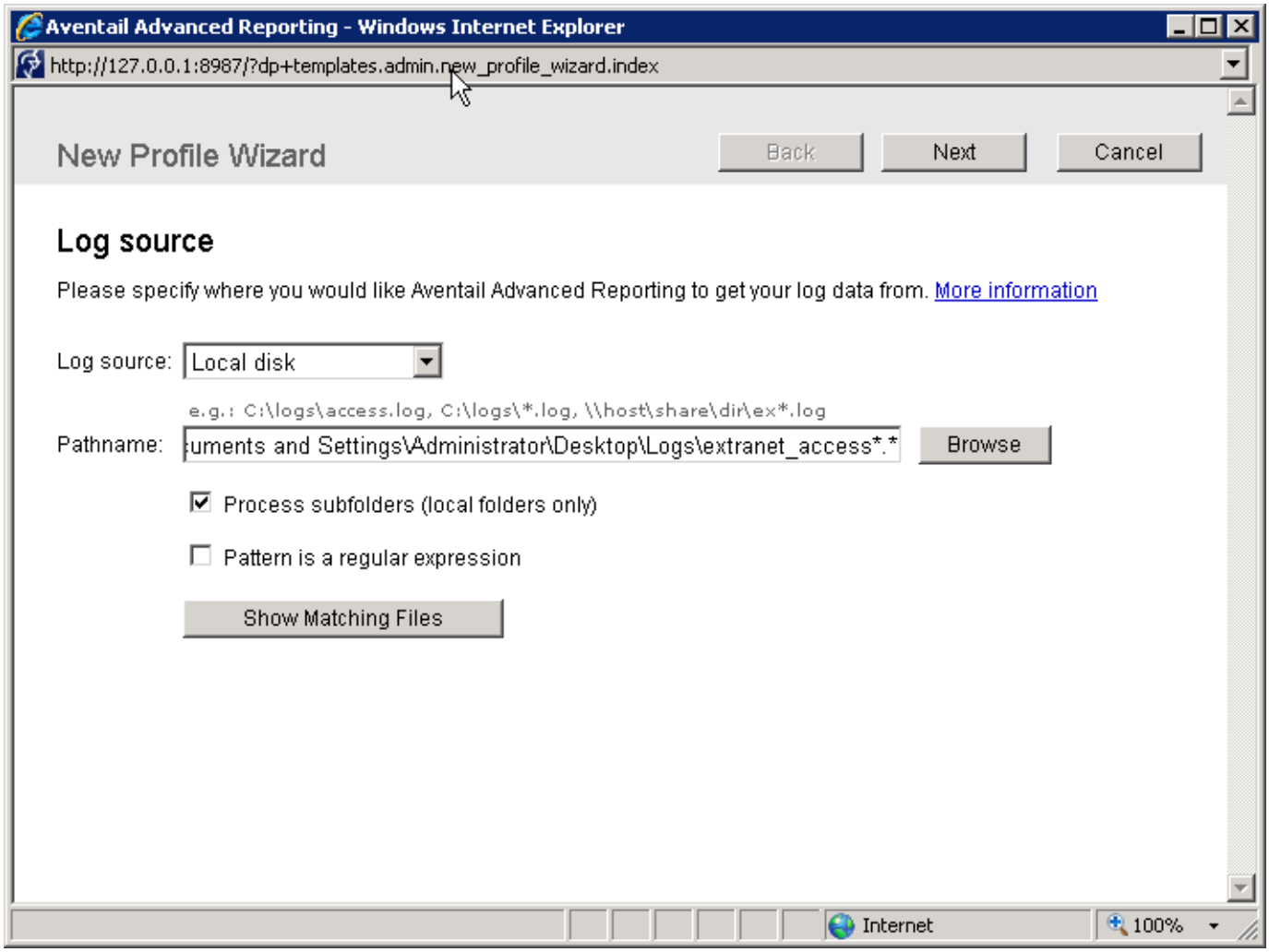


Select a file (extranet_access.log) and then click OK:



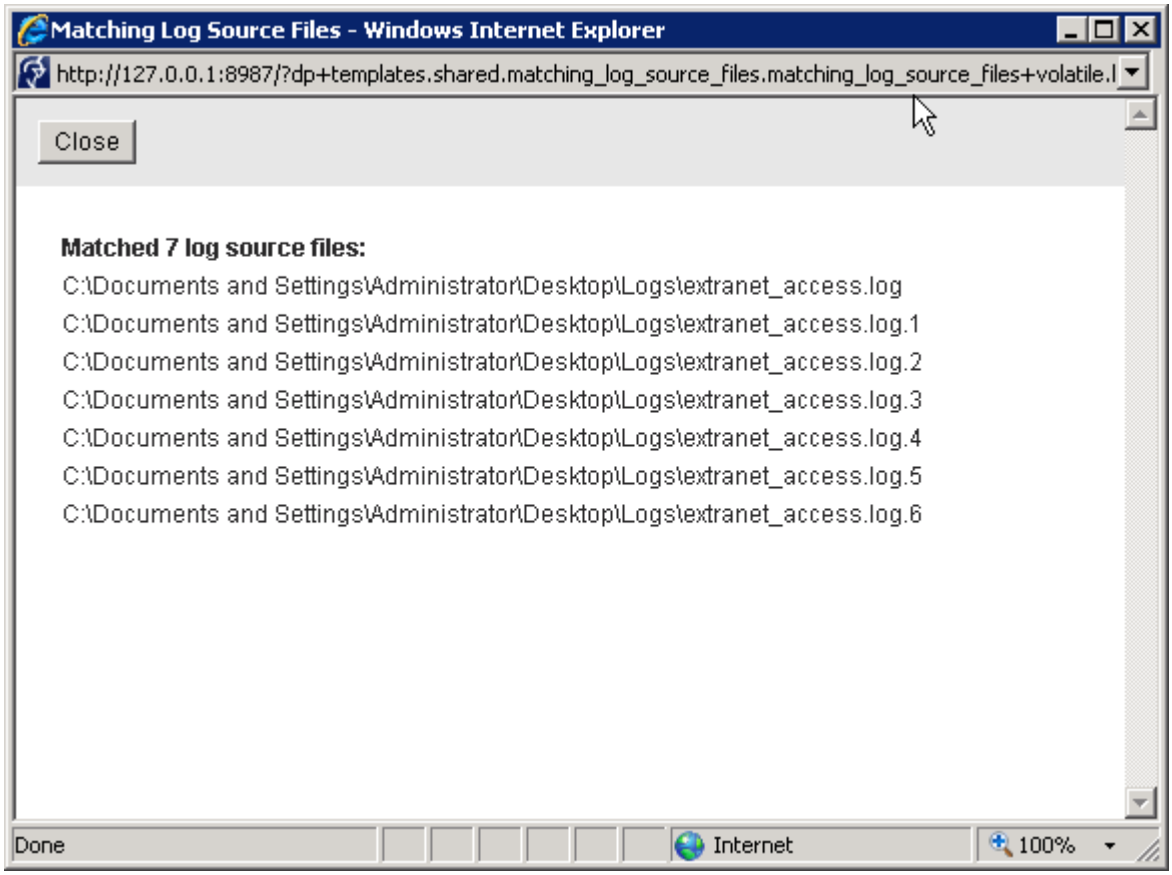
Modify the pathname so all extranet_access.log files in the Logs directory are retrieved. Change extranet_access.log to extranet_access*.* and check the box to Process subfolders (local folder only).

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



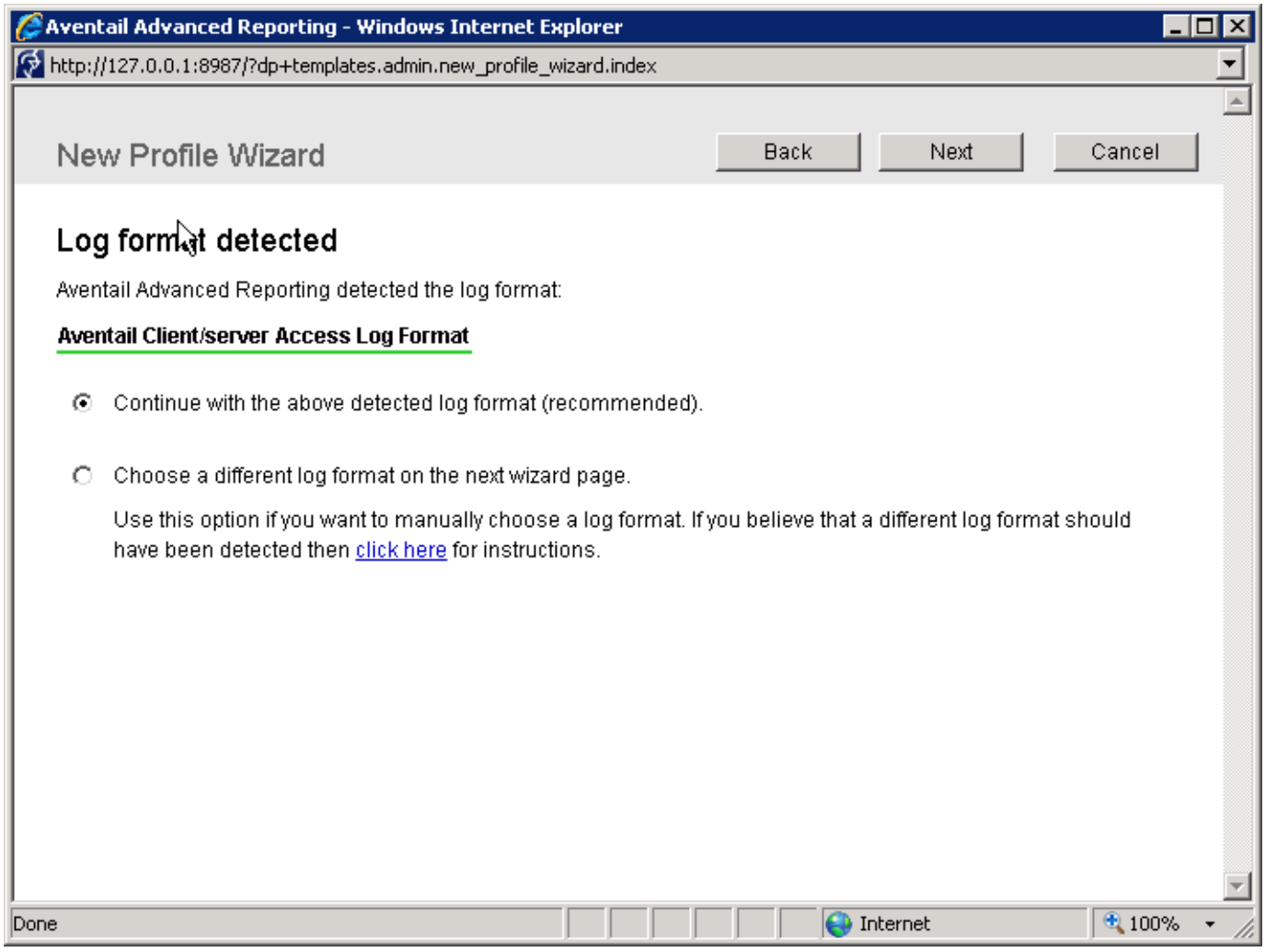
:

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.

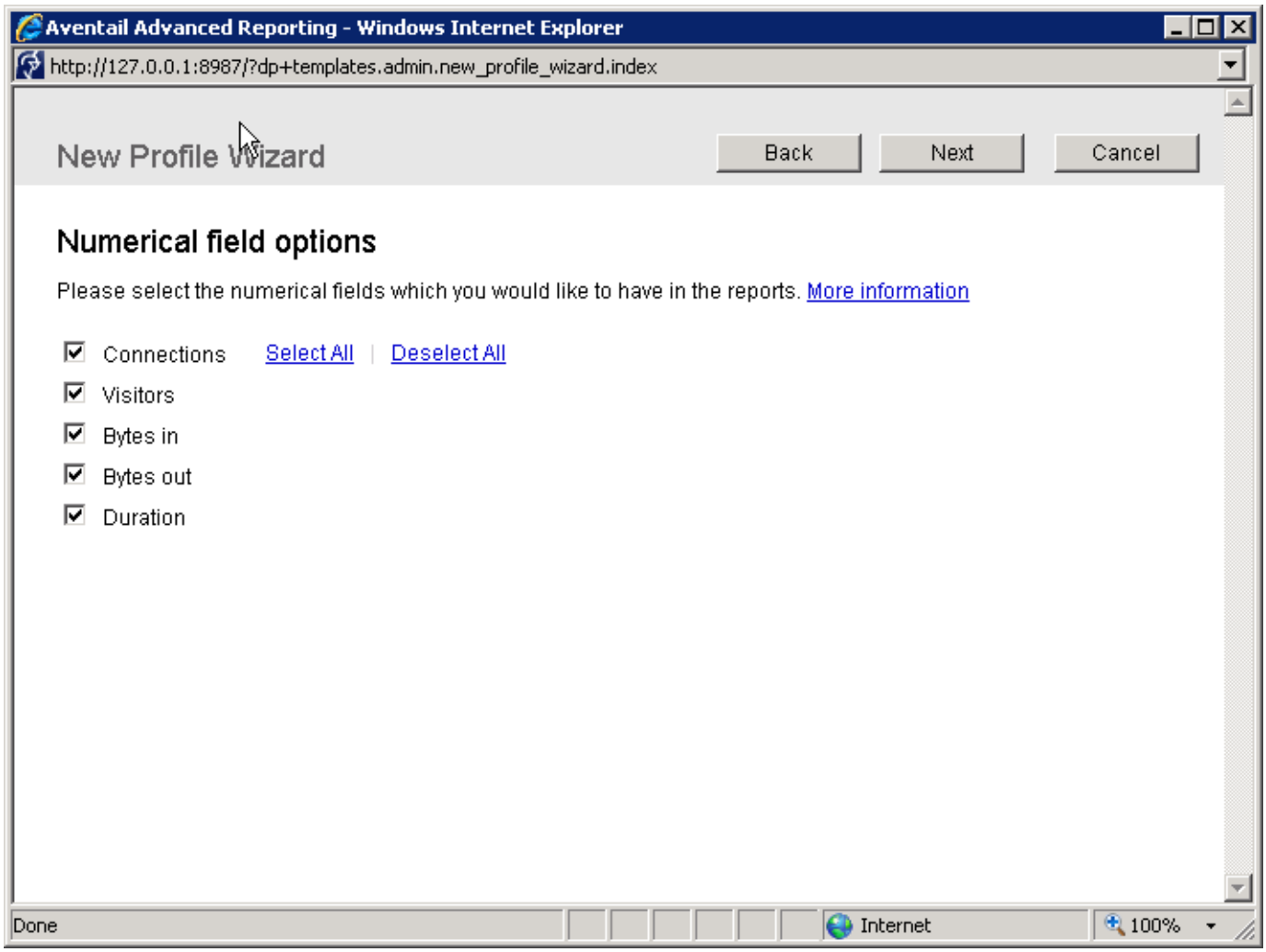


AAR will then automatically detect the log file format. Leave the default of Aventail Client/server Access Log Format and select Next:

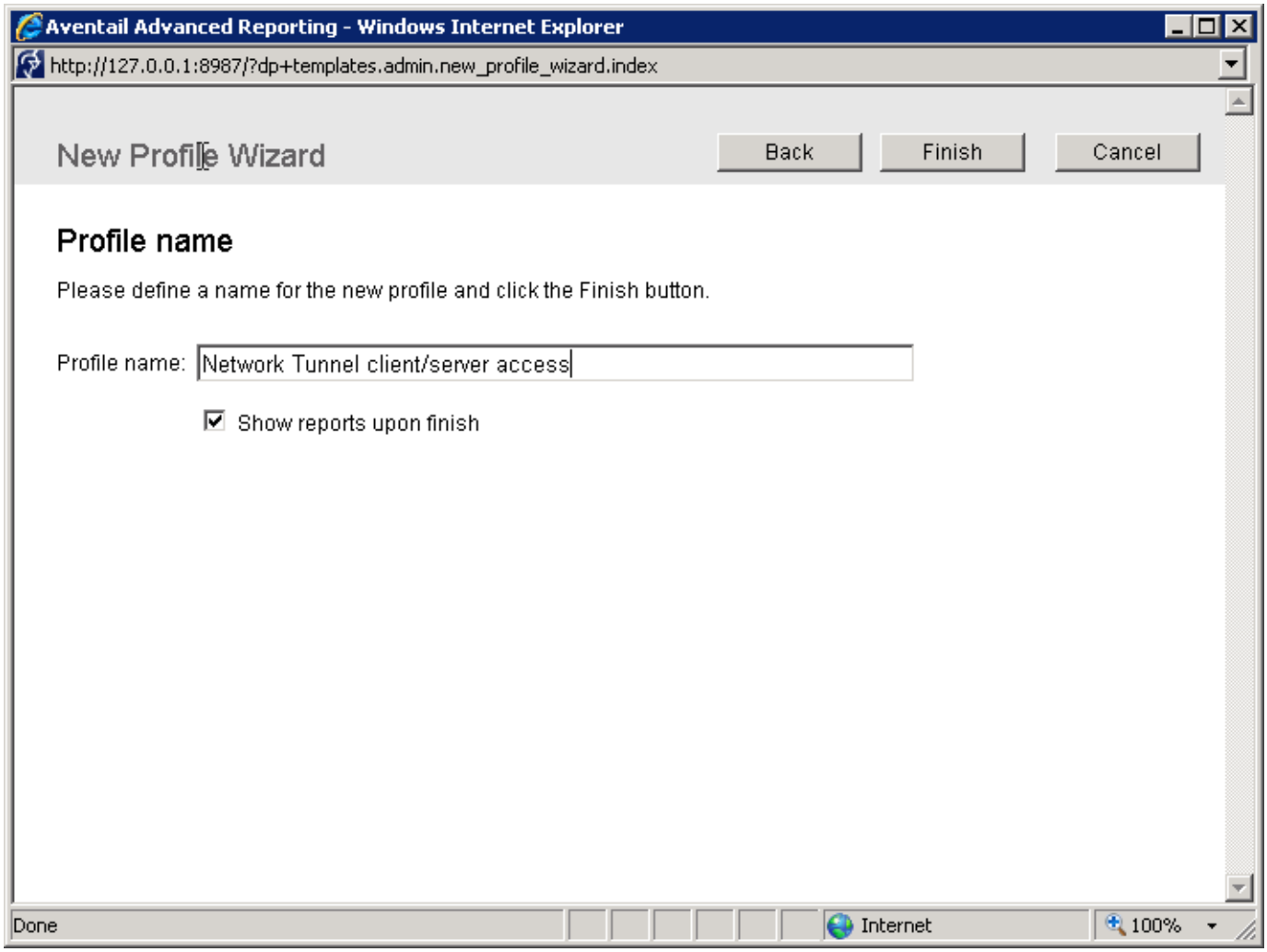
Note: If you are running 10.x firmware on the Aventail appliance, you must load a new AAR configuration file to recognize this log. Please see the step above on page 10 for more details.



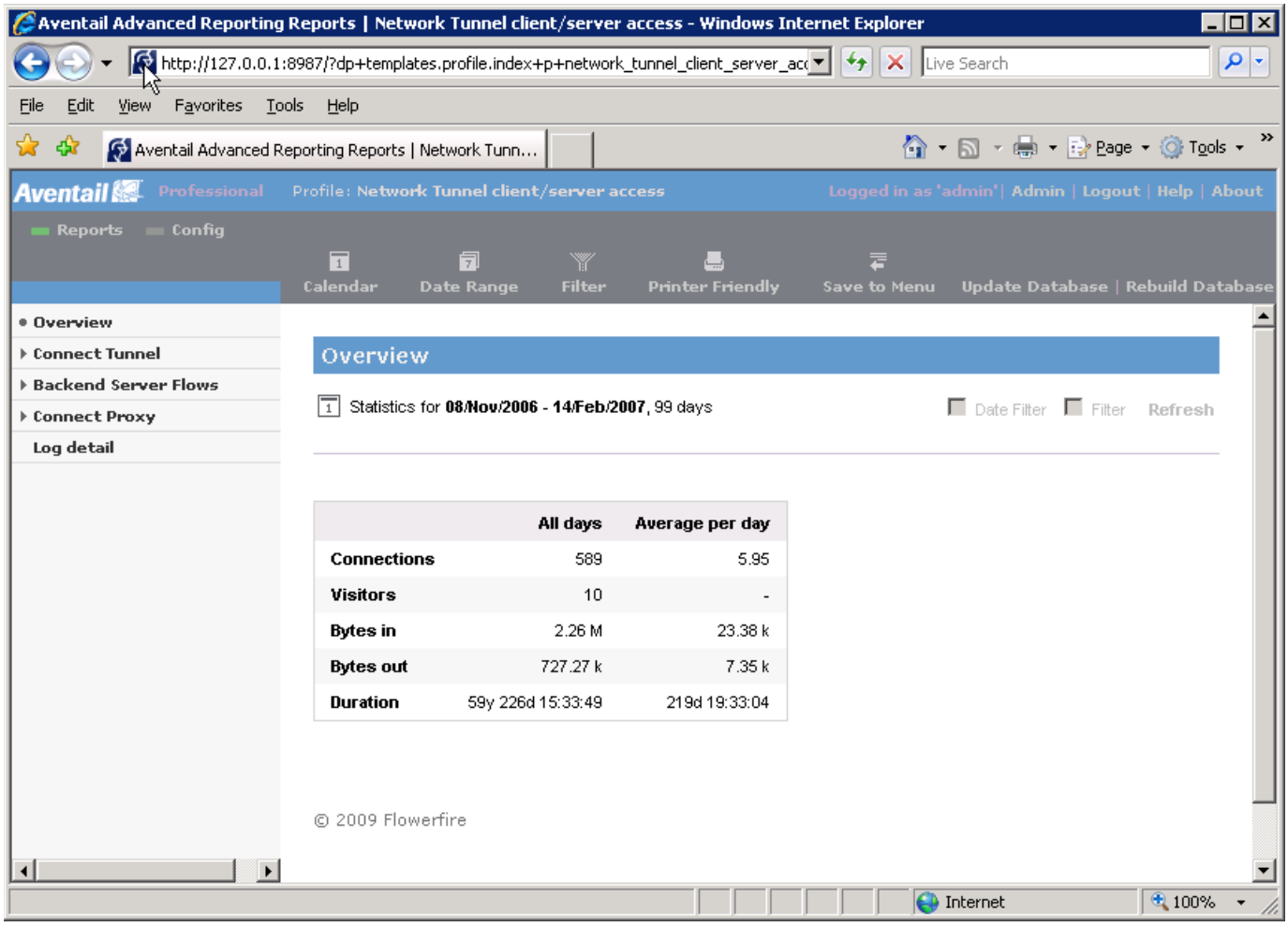
Leave all the defaults for Numerical field options and select Next:



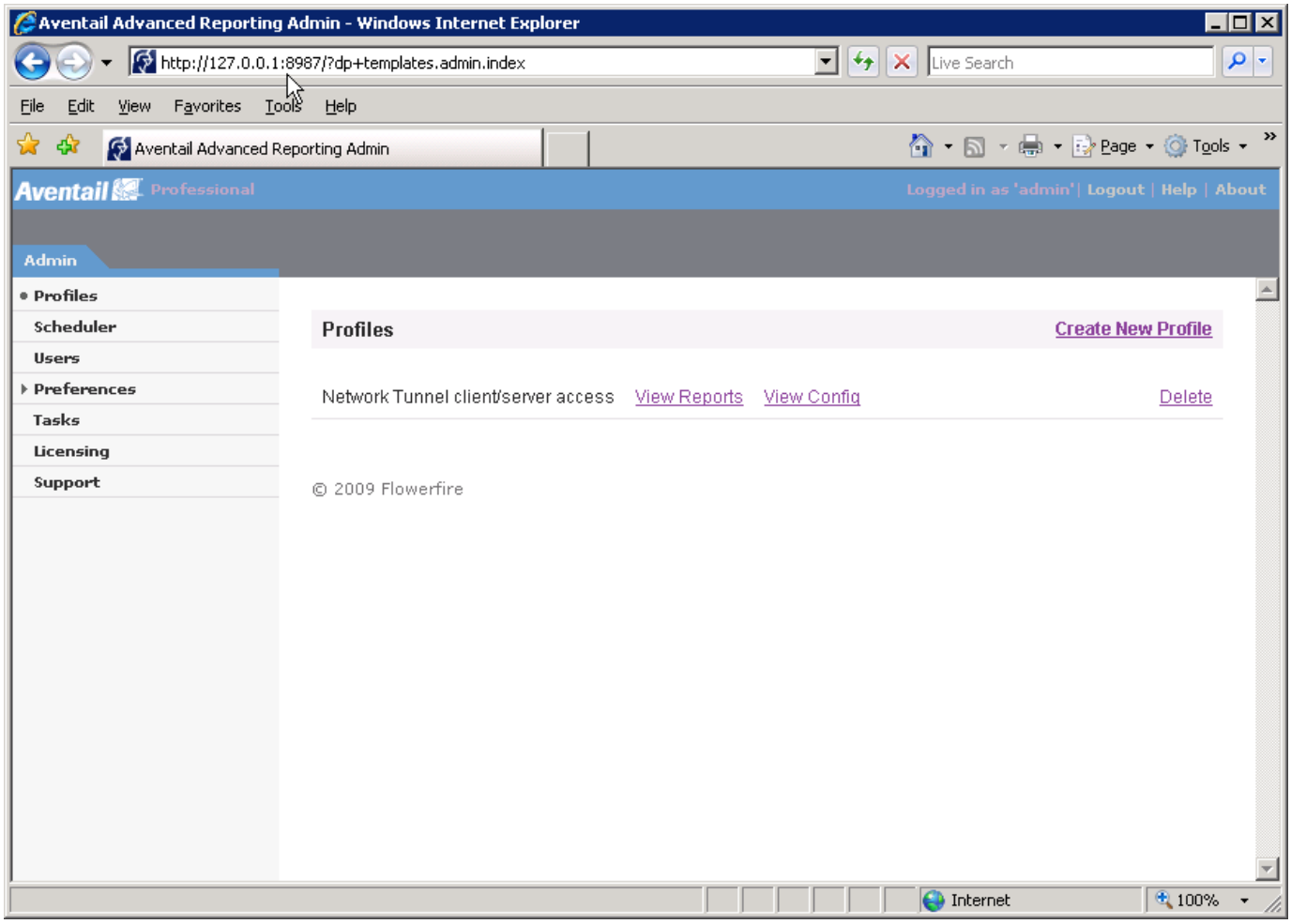
Change the Profile name to reflect the type of reports that will be displayed (e.g. Network Tunnel client/server access):



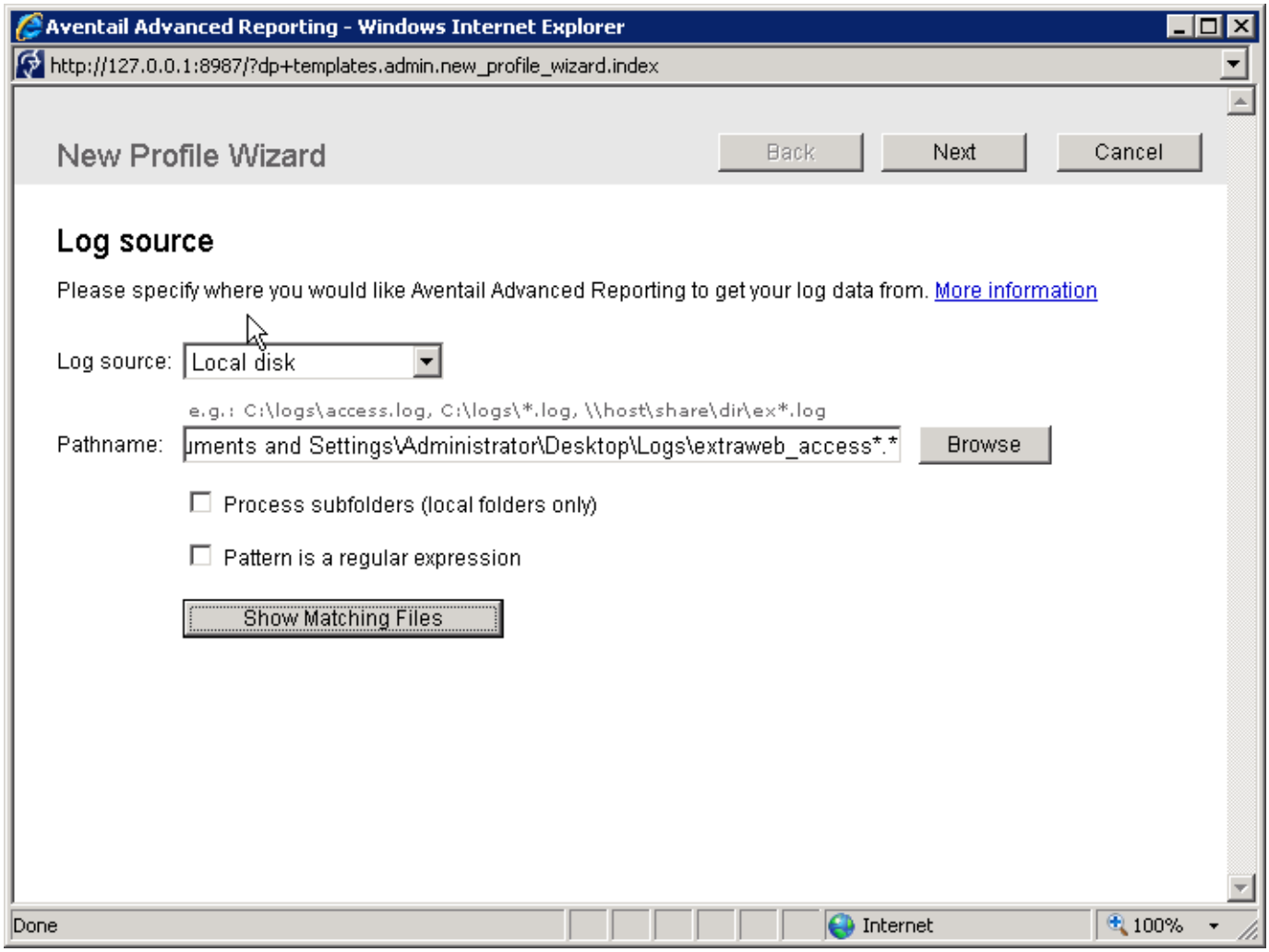
Then select Finish to build the database and display the reports. When the database build is complete, the Reports page will be shown starting with the Overview page:



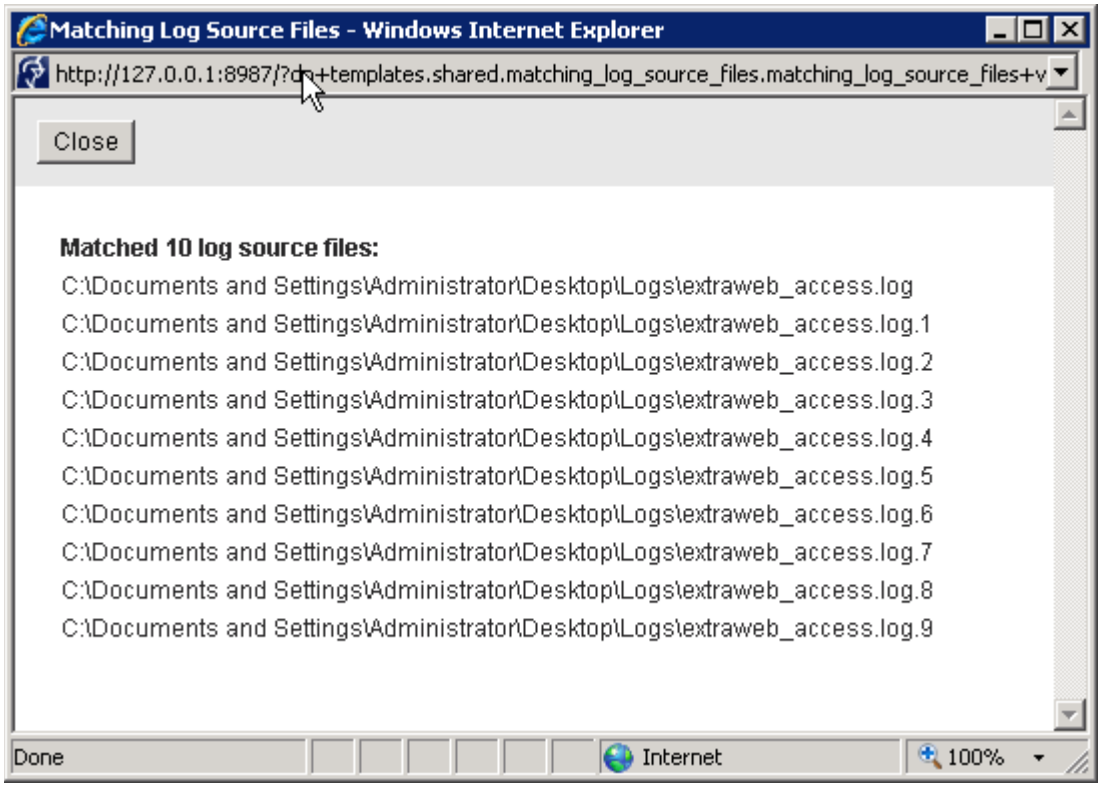
Now that the Network Tunnel client/server Profile is complete, you must add a new Profile for the Web access logs. From the Overview menu select 'Admin' in the upper right corner of the page and then select Profile:



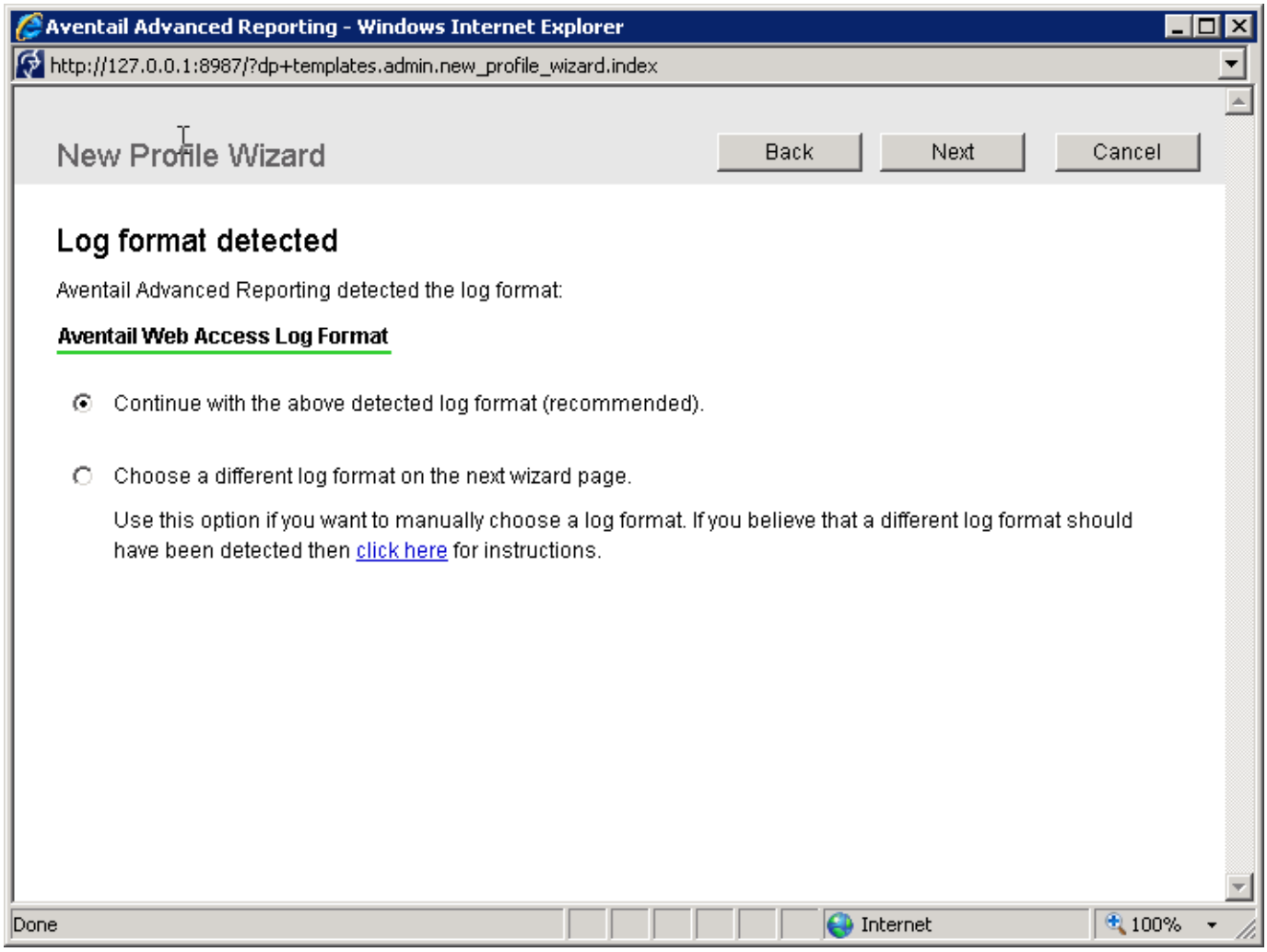
From the Profile menu, select ‘Create new profile’ to begin the process again except this time the log file names will be extraweb_access*.* as show below:



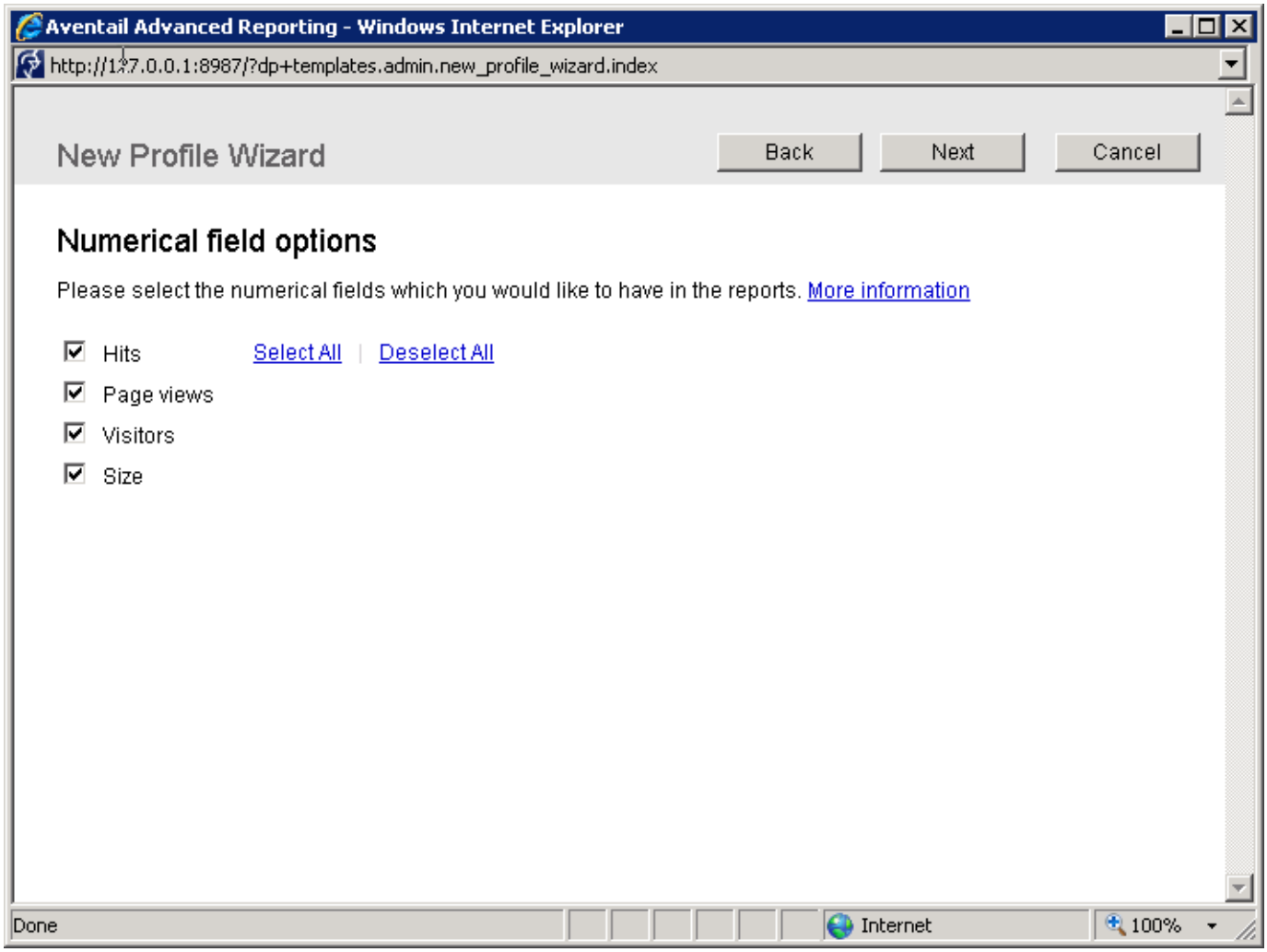
Check the matched log file to make sure the Pathname is correct and all the files are retrieved:



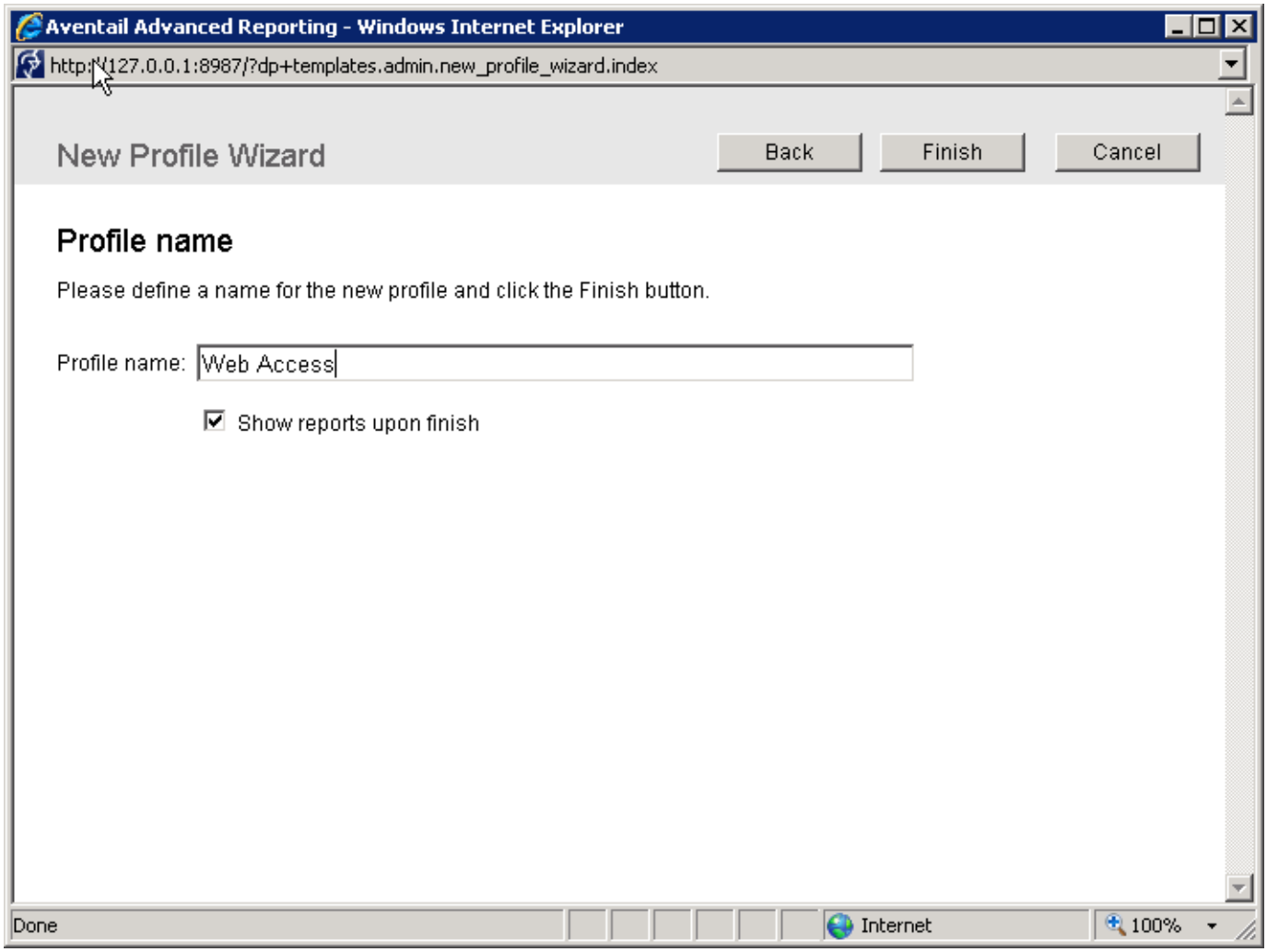
Leave the default Log format of Aventail Web Access Log Format:



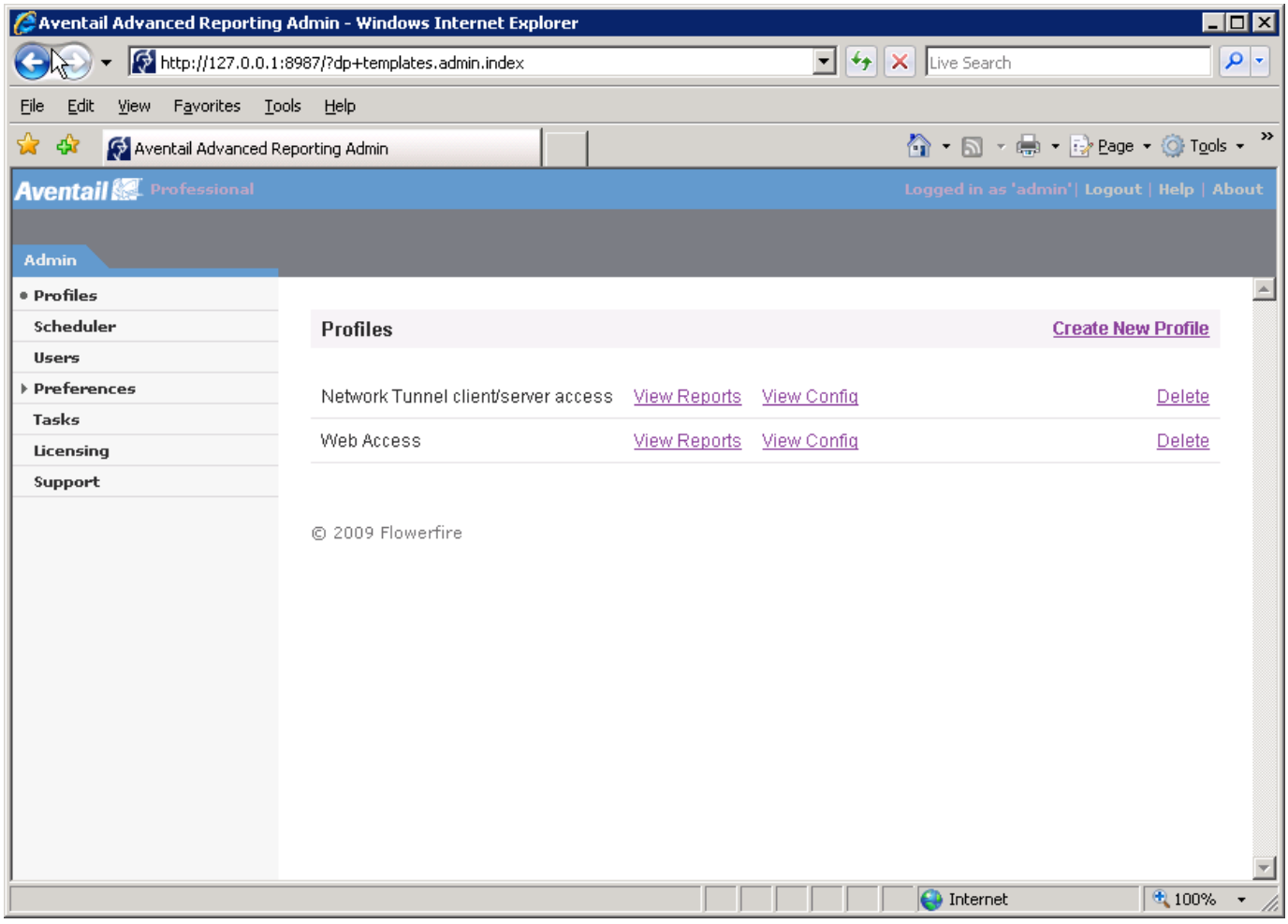
Leave the default Numerical field options:



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



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



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 http://www.mysonicwall.com 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.

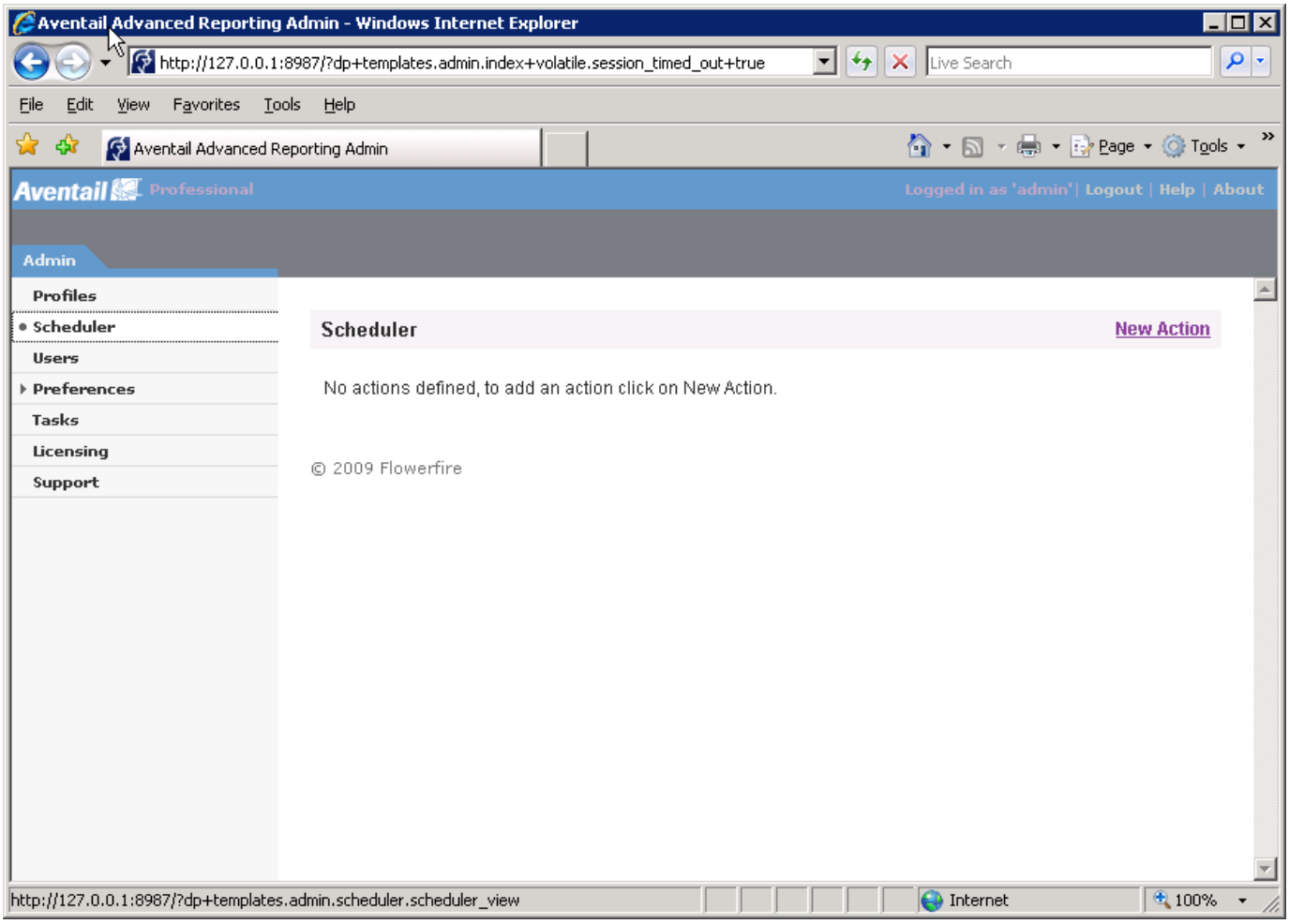
The log retrieval will now happen automatically each day.

Automated Database Build

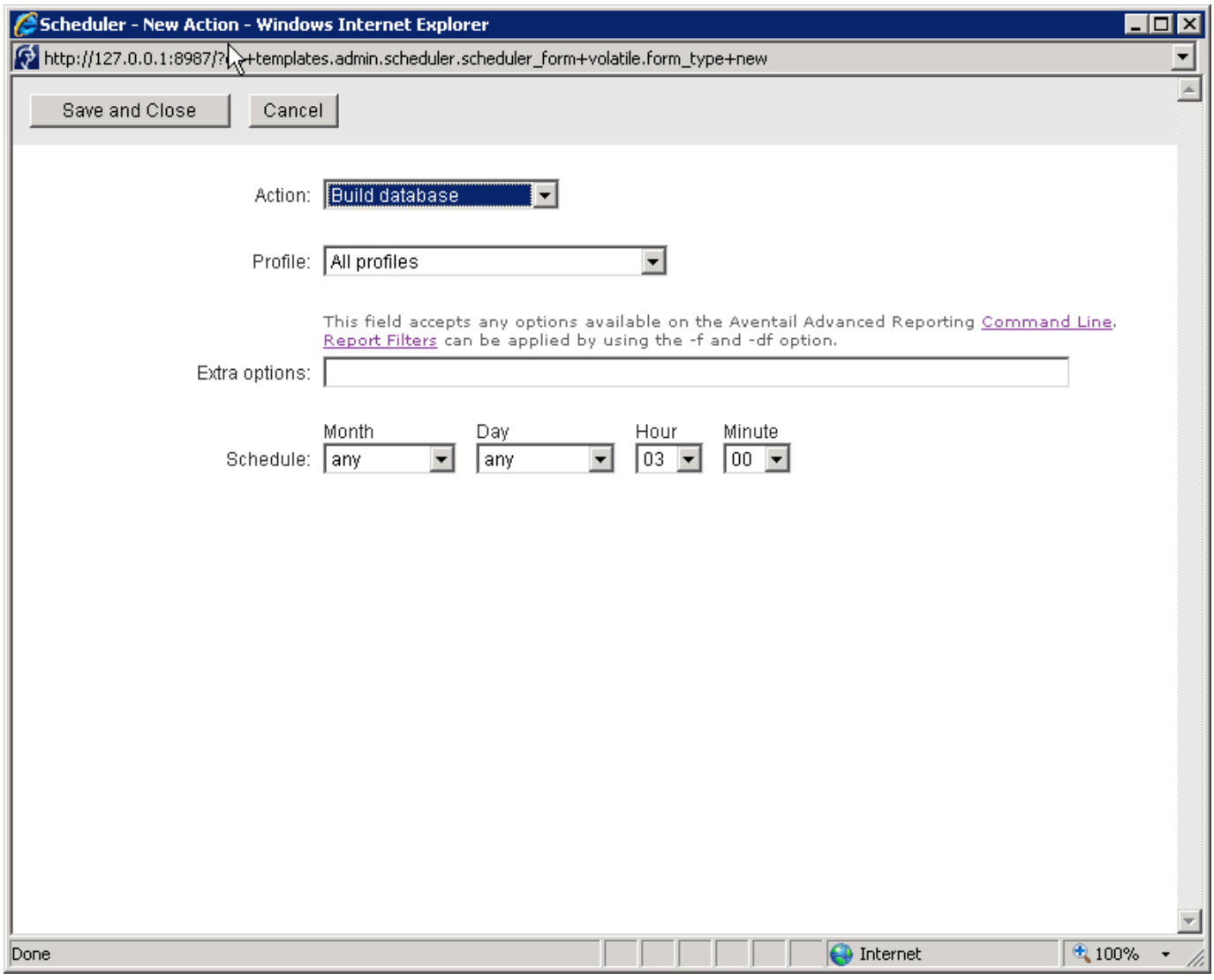
Once the log files are copied to the AAR Server, they must be loaded into the database for subsequent analysis and reporting. AAR has an internal scheduler system to allow a scheduled build of the database after the log files have been copied.

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:



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 http://www.mysonicwall.com covering additional topics on customization, reporting, and operation.