



Your Question

Article: 00056

Question:


How do I do I Export Check Point Firewall-1 Log Files via Check Point SmartView Tracker (GUI) for Net Report?

Net Report Answer

Introduction

This Article explains how to:

- Launch Check Point SmartView Tracker (please see Section 1.0).
- Select Elapsed and Bytes Fields (please see Section 1.1).
- Ensure Resolve IP and Resolve Services Buttons are not selected (see Section 1.2).
- Export your Log File via Check Point SmartView Tracker (please see Section 1.3).
- Purge your Log File via Check Point SmartView Tracker (please see Section 1.4).

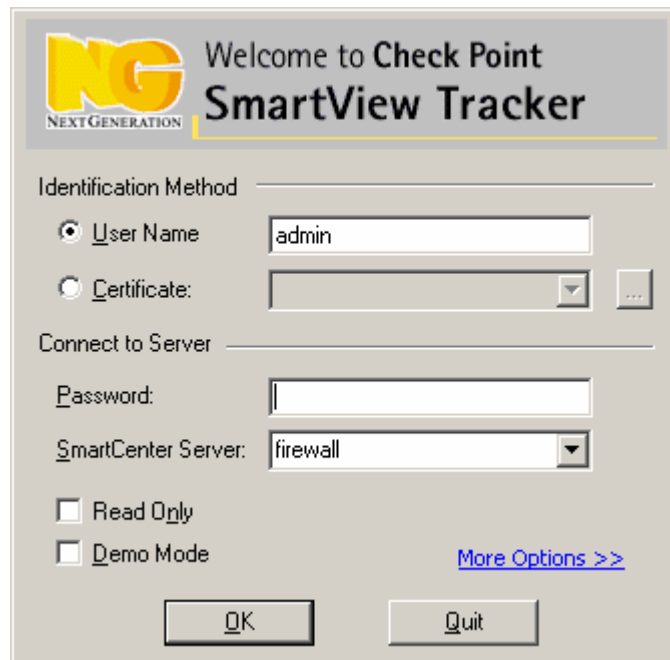
 **Note:** please note that instructions regarding switching, exporting and archiving your log files via command lines for Net Report (i.e. fw logswitch and fw logexport commands) instead of the Check Point GUI can be found in Net Report Knowledge Base Article 00055 <http://www.netreport.fr/us/OurDocuments/NRFAQs.htm>

1.0 Launching Check Point SmartView Tracker

To launch Check Point SmartView Tracker, please follow the steps below:

Steps

1. Open **Check Point SmartView Tracker**. The **Welcome to Check Point SmartView Tracker** dialog box appears.



Identification Method

User Name: admin

Certificate: [dropdown] [...]

Connect to Server

Password: [text box]

SmartCenter Server: firewall [dropdown]

Read Only

Demo Mode

[More Options >>](#)

OK Quit

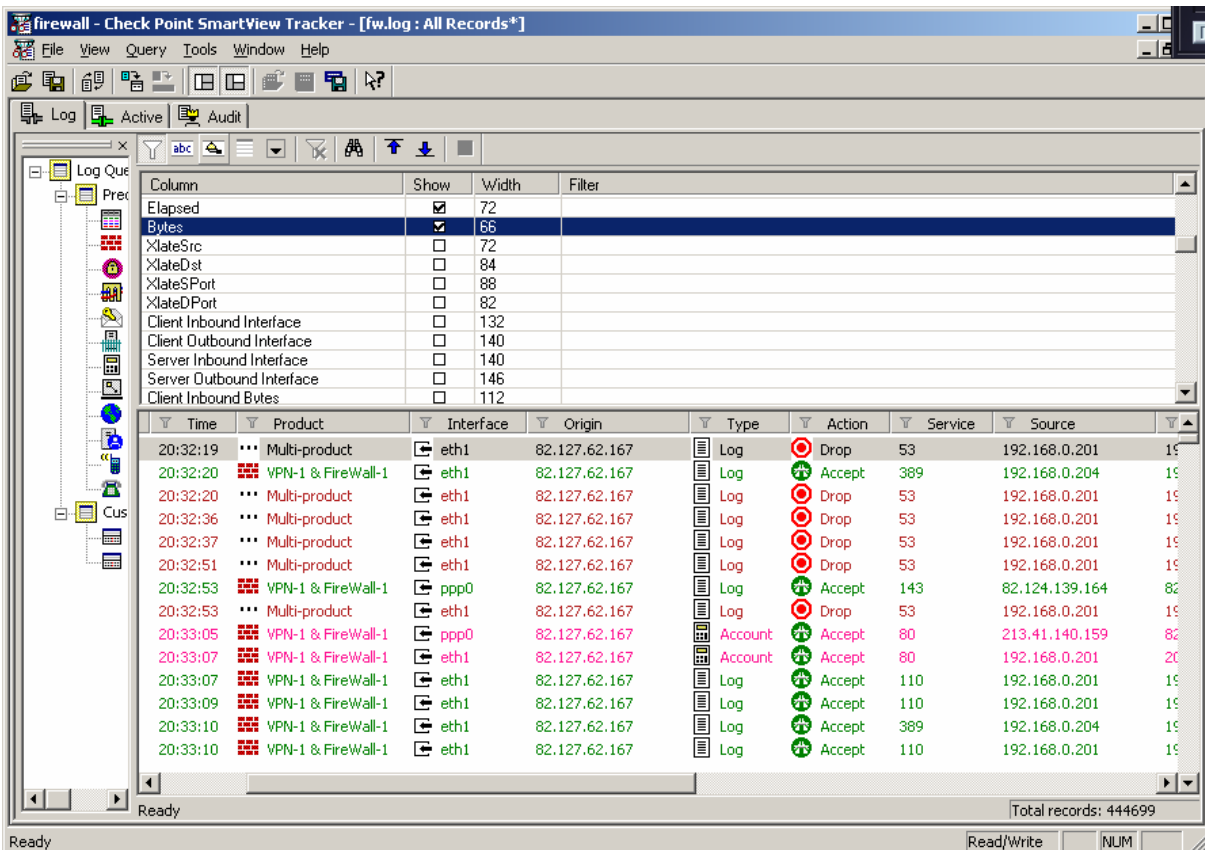
2. Select the **User Name** option button.
3. Enter your **User Name** in the **User Name** field.
4. Enter your **Password** in the **Password** field.
5. Click **OK**. The **Check Point SmartView Tracker** interface appears.

1.1 Selecting Elapsed and Bytes Fields

To select the Elapsed and Bytes Fields (amongst others), please follow the steps below:

Steps

1. Select **View > Query Property**. The Fields table appears in the central pane.
2. Select Fields by selecting the check box in the Show column adjacent to the field you want. In this example the **Elapsed** and **Bytes** fields are selected.
3. Select the:
 - **Elapsed** field **Show** check box in the **Show** column.
 - **Bytes** field **Show** check box in the **Show** column.



The screenshot shows the 'firewall - Check Point SmartView Tracker' interface. The 'Fields' table is visible, with the 'Show' column checked for 'Elapsed' and 'Bytes'. Below the table, a list of log records is displayed.

Column	Show	Width	Filter
Elapsed	<input checked="" type="checkbox"/>	72	
Bytes	<input checked="" type="checkbox"/>	66	
XlateSrc	<input type="checkbox"/>	72	
XlateDst	<input type="checkbox"/>	84	
XlateSPort	<input type="checkbox"/>	88	
XlateDPort	<input type="checkbox"/>	82	
Client Inbound Interface	<input type="checkbox"/>	132	
Client Outbound Interface	<input type="checkbox"/>	140	
Server Inbound Interface	<input type="checkbox"/>	140	
Server Outbound Interface	<input type="checkbox"/>	146	
Client Inbound Bytes	<input type="checkbox"/>	112	

Time	Product	Interface	Origin	Type	Action	Service	Source
20:32:19	Multi-product	eth1	82.127.62.167	Log	Drop	53	192.168.0.201
20:32:20	VPN-1 & FireWall-1	eth1	82.127.62.167	Log	Accept	389	192.168.0.204
20:32:20	Multi-product	eth1	82.127.62.167	Log	Drop	53	192.168.0.201
20:32:36	Multi-product	eth1	82.127.62.167	Log	Drop	53	192.168.0.201
20:32:37	Multi-product	eth1	82.127.62.167	Log	Drop	53	192.168.0.201
20:32:51	Multi-product	eth1	82.127.62.167	Log	Drop	53	192.168.0.201
20:32:53	VPN-1 & FireWall-1	ppp0	82.127.62.167	Log	Accept	143	82.124.139.164
20:32:53	Multi-product	eth1	82.127.62.167	Log	Drop	53	192.168.0.201
20:33:05	VPN-1 & FireWall-1	ppp0	82.127.62.167	Account	Accept	80	213.41.140.159
20:33:07	VPN-1 & FireWall-1	eth1	82.127.62.167	Account	Accept	80	192.168.0.201
20:33:07	VPN-1 & FireWall-1	eth1	82.127.62.167	Log	Accept	110	192.168.0.201
20:33:09	VPN-1 & FireWall-1	eth1	82.127.62.167	Log	Accept	110	192.168.0.201
20:33:10	VPN-1 & FireWall-1	eth1	82.127.62.167	Log	Accept	389	192.168.0.204
20:33:10	VPN-1 & FireWall-1	eth1	82.127.62.167	Log	Accept	110	192.168.0.201

1.2 Ensuring the Resolve IP and Resolve Services Buttons Are Not Selected

To export log files for Net Report, you must ensure that you have not selected the **Resolve IP** and **Resolve Services** buttons in the toolbar at the top of the SmartView Tracker Pane central pane. To do so, please follow the steps below:

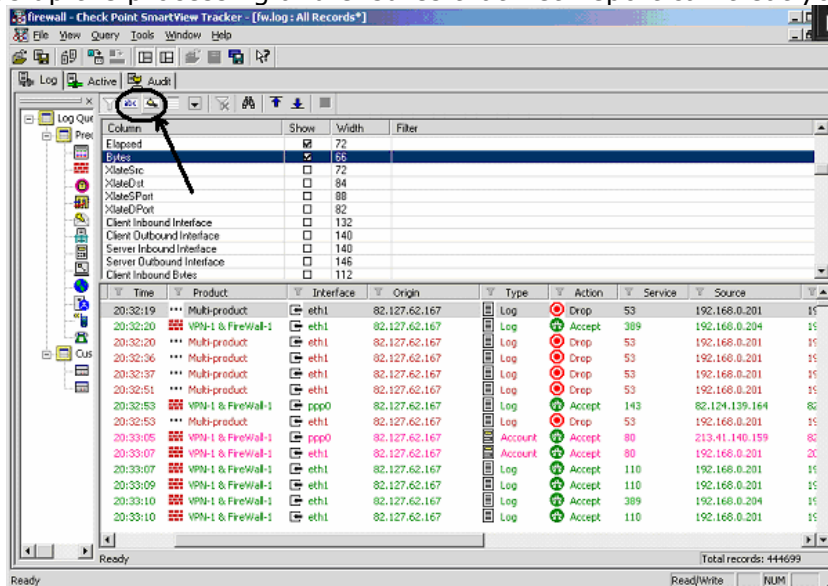
Steps

1. Ensure that the following buttons have not been selected (i.e. pressed):

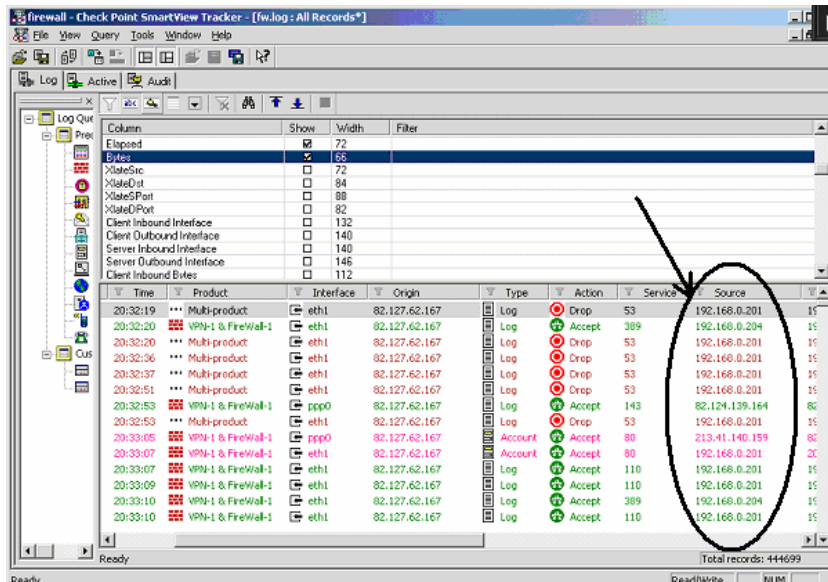
 **Resolve IP**

 **Resolve Services**

This ensures that no DNS resolution of the IP addresses in the Log File is performed (this option significantly speeds up the processing and ensures that Net Report can treat your log files).



2. Ensure that the IP Addresses appear in the central pane table. For example in the Source column.



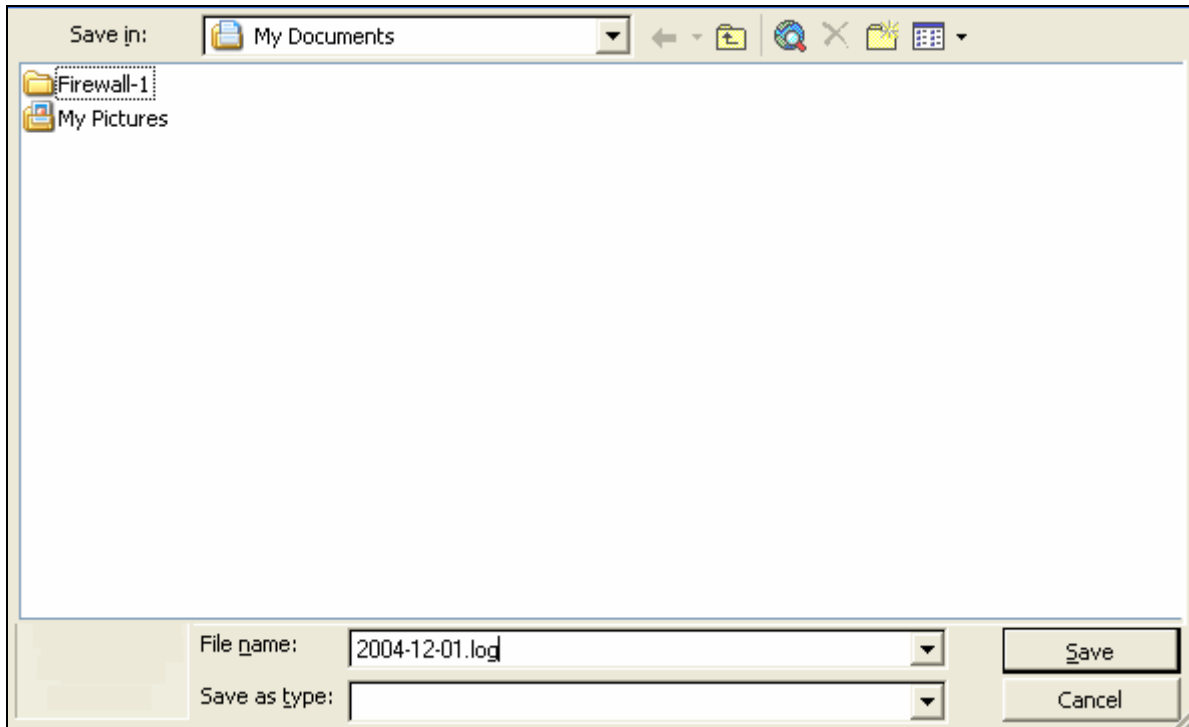
Warning: you must ensure that the IP Addresses are not resolved. This ensures that no DNS Resolution of IP addresses is carried out in the Log File. Net Report needs the IP addresses in order to process the Log File. If DNS resolution is performed, Net Report will be unable to correctly process the Log File.

1.3 Exporting your Log File via Check Point SmartView Tracker

To export your Log File, please follow the steps below:

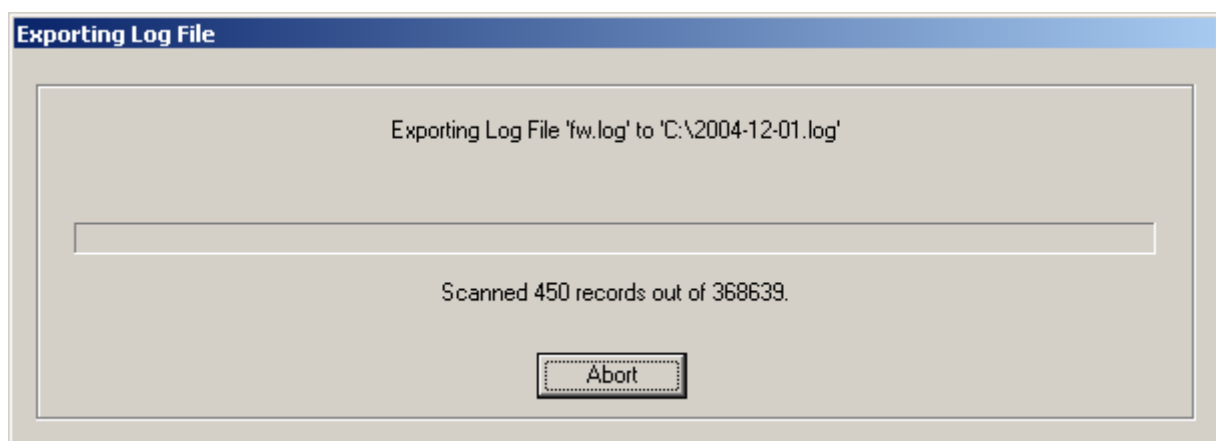
Steps

1. Select **File > Export**.



2. Enter the File name you want for the exported file in the **File name** field.

3. Click **Save**.

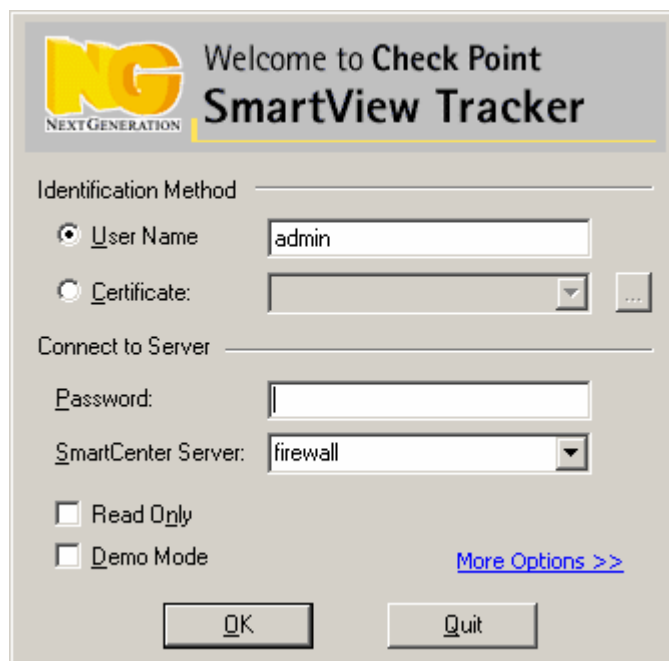


1.4 Purging your Log Files

To purge your log files, please follow the steps below:

Steps

1. Open **Check Point SmartView Tracker**. The **Welcome to Check Point SmartView Tracker** dialog box appears.

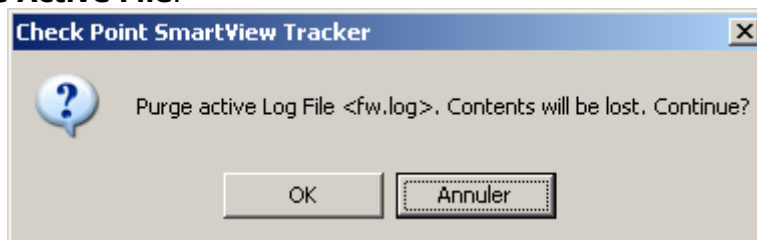


2. Select the **User Name** option button.

3. Enter your **User Name** in the **User Name** field and **Password** in the **Password** field.

4. Click **OK**. The Check Point SmartView Tracker interface appears.

5. Click **File > Purge Active File**.



6. The **Purge active Log File <fw.log>** message appears.

7. Click **OK** to continue. Your log file will be purged.

Further Information

Please see our Net Report Knowledge Base at:

http://www.netreport.fr/us/support/sup_knowledgebase.asp