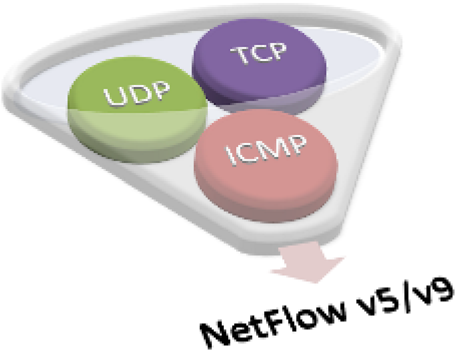
SoftPI – Software Projects & Innovations



fSonar 1.5

User guide

Version: 1.0
Date: October 2011

Contents

Introduction

The **fSonar** program is a network sensor of NetFlow. It scans the whole or a specified type of traffic passing through one or more network interfaces of computer running under Windows (Microsoft), and generates a flow of data in the format of the NetFlow version 5 or 9 on the network activity on these interfaces. NetFlow data is sent to a computer with a installed NetFlow collector (any manufacturer), with further analysis of network activity with the corresponding program.

Therefore you can use fSonar if:

- you want to monitor data traffic within your network and you do not have routes and switches that support protocols NetFlow (IPFIX or similar),
- necessary to control traffic on the Internet, but routers do not support the above-mentioned protocols,
- there is a need to control IP traffic versions 4 and 6 (IPv4 and IPv6),
- a network flow collector have an IP address has a network of IPv6,
- a network flow collector have an IP address of a network of IPv6.

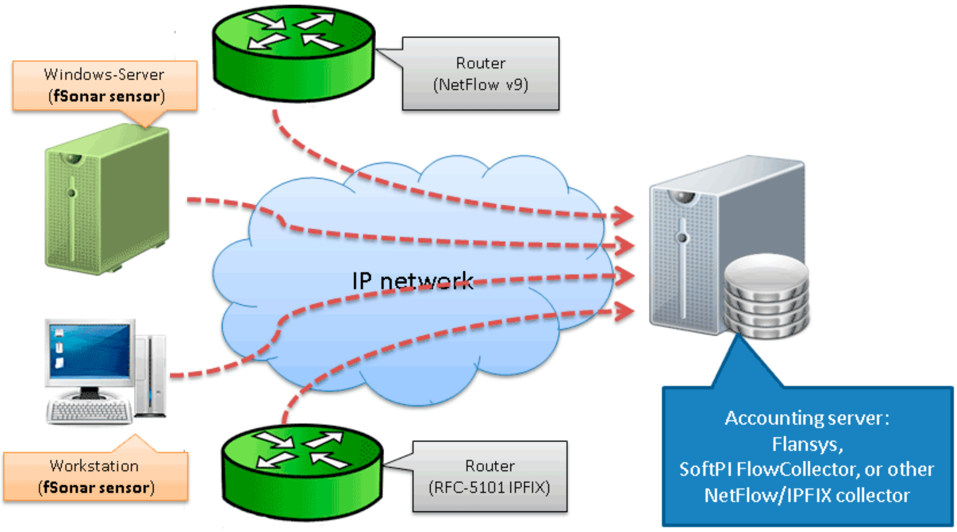


Figure 1

NetFlow is a network protocol developed by Cisco Systems for collecting IP traffic information and it is widely used in network devices like this company and other manufacturers. However, not all network devices support NetFlow. In addition, if, for example, a router supports NetFlow and network switches do not support NetFlow, it is not possible to obtain a complete picture of network activity within a LAN. These and other reasons make it necessary to install on computers (servers) NetFlow sensors.

fSonar program can be used in large networks for the analysis of incoming / outgoing network traffic, servers and ordinary PCs, and home users to analyze traffic of a home computer. Analysis of network traffic on home computers can be useful for identifying the network activity of malicious programs (trojans, viruses, etc), detection of applications generating the most network traffic, the hidden network activity of legitimate applications, and so on.

fSonar monitors network traffic as IP protocol version 4 (IPv4), and version 6 (IPv6), which facilitates the translation of the company's network to IPv6 or to control both types of protocols.

fSonar can generate information about MAC addresses, which allows to uniquely identify a network device generating traffic, if your network uses automatic IP assignment.

Based on data received from fSonar, you can find information about:

- Amount of traffic passing through the computer / user interface (including real-time);
- Load of a network device / interface (including real-time);
- The direction of traffic (country, city);
- Applications involved in the exchange of data (including real-time);
- The protocols used for data transmission;
- The activity of an IP address or address range in the interaction with the computer;
- As well as some other information.

Features and benefits

- fSonar works as a Windows service.
- fSonar supports NetFlow versions 5 and 9.

  - NetFlow version 9 contains a large set of fields. But not all of these fields are available for computers running Windows. Of those fields that are available, the user of fSonar can choose only necessary fields for him at the moment, which will reduce the load on the CPU for data processing and reduce costs of network traffic in NetFlow data transfer.
- You can configure fSonar to get NetFlow data from a specific network interface as well as to collect information only on incoming or outgoing traffic. In addition you can configure the program to monitor a network traffic:

  - on specific IP address;
  - on specific range of IP addresses;
  - on specific IP port;
  - excluding from monitoring specific IP ports or addresses;

  and etc.
- fSonar 1.5 not only allows you to select the necessary fields for export, and save them as a template that can be used later on the same computer or for quick installation on other computers.
- fSonar 1.5 can work in networks with IPv4 and IPv6.
- The program does not consume significant system resources, even at high load of network interfaces.

System requirements

Minimum hardware requirements for a computer:

- Processor: Pentium III (x86 or x64) 1 GHz or more;
- RAM: 256 MB or more;
- Network card.

Software requirements for a computer:

- Operating System: Windows 2000/XP/2003/Vista/7 (x86 or x64);
- Net Framework 3.5. If computer where you install fSonar has an Internet connection and does not contain .Net Framework 3.5, then .Net Framework 3.5 is downloaded and installed automatically. If the computer at the time of installation of the system will not have a connection to the Internet, then to work the system, you must download and install .Net Framework 3.5.

Monitored parameters

The fSonar program depending on configured version of NetFlow protocol allows to monitor a various set of network parameters.
When using NetFlow version 5, you can collect the following parameters:

- Source IP address;
- Destination IP address;
- IP address of next hop router;
- SNMP index of input interface;
- SNMP index of output interface;
- Packets in the flow;
- Total number of Layer 3 bytes in the packets of the flow;
- SysUptime at start of flow;
- SysUptime at the time the last packet of the flow was received;
- TCP/UDP source port number or equivalent;
- TCP/UDP destination port number or equivalent;
- Cumulative OR of TCP flags;
- IP protocol type (for example, TCP = 6; UDP = 17);
- IP type of service (ToS).

When using NetFlow version 9, you can collect the following parameters:

- Incoming counter with length N x 8 bits for number of bytes associated with an IP Flow;
- Incoming counter with length N x 8 bits for the number of packets associated with an IP Flow;
- Number of flows that were aggregated; default for N is 4;
- IP protocol;
- Type of Service byte setting when entering incoming interface;
- Cumulative of all the TCP flags seen for this flow;
- TCP/UDP source port number e.g. FTP, Telnet, or equivalent;
- IPv4 source address;
- The number of contiguous bits in the source address subnet mask i.e. the submask in slash notation;
- Input interface index;
- TCP/UDP destination port number e.g. FTP, Telnet, or equivalent;
- IPv4 destination address;

- The number of contiguous bits in the destination address subnet mask i.e. the submask in slash notation;
- Output interface index; default for N is 2 but higher values could be used;
- IPv4 address of next-hop router;
- System uptime at which the last packet of this flow was switched;
- System uptime at which the first packet of this flow was switched;
- Outgoing counter with length N x 8 bits for the number of bytes associated with an IP Flow;
- Outgoing counter with length N x 8 bits for the number of packets associated with an IP Flow;
- Minimum IP packet length on incoming packets of the flow;
- Maximum IP packet length on incoming packets of the flow;
- IPv6 Source Address;
- IPv6 Destination Address;
- Length of the IPv6 source mask in contiguous bits;
- Length of the IPv6 destination mask in contiguous bits;
- IPv6 flow label as per RFC 2460 definition;
- Internet Control Message Protocol (ICMP) packet type;
- Internet Group Management Protocol (IGMP) packet type;
- When using sampled NetFlow, the rate at which packets are sampled;
- The type of algorithm used for sampled NetFlow;
- Timeout value (in seconds) for active flow entries in the NetFlow cache;
- Timeout value (in seconds) for inactive flow entries in the NetFlow cache;
- IPv4 source address prefix;
- IPv4 destination address prefix;
- Minimum TTL on incoming packets of the flow;
- Maximum TTL on incoming packets of the flow;
- The IP v4 identification field;
- Type of Service (ToS) byte setting when exiting outgoing interface;
- Incoming source MAC address;
- Outgoing destination MAC address;
- Incoming destination MAC address;
- Outgoing source MAC address;
- Internet Protocol Version Set to 4 for IPv4, set to 6 for IPv6;
- Flow direction: 0 - ingress flow, 1 - egress flow;
- IPv6 address of the next-hop router;
- Bit-encoded field identifying IPv6 option headers found in the flow;

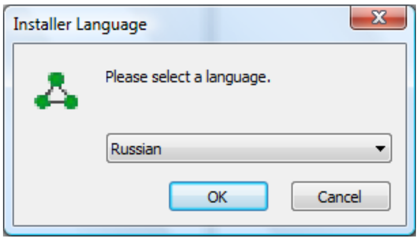
- The fragment offset value from fragmented IP packets.

Installation

Before installing, make sure that you have installed .NET Framework 3.5. If it is not and the computer at the time of installation does not have access to the Internet, you must download .NET Framework 3.5 and install on your computer. If at the time of installation, the computer has access to the Internet, .NET Framework 3.5 will be downloaded and installed automatically.

To install fSonar, run **sonarsetup.exe**. The latest version of the installation file you can download from the site: http://www.softpiua.com/

After begin of installation the window appears as shown in Figure 2.



Installer Language

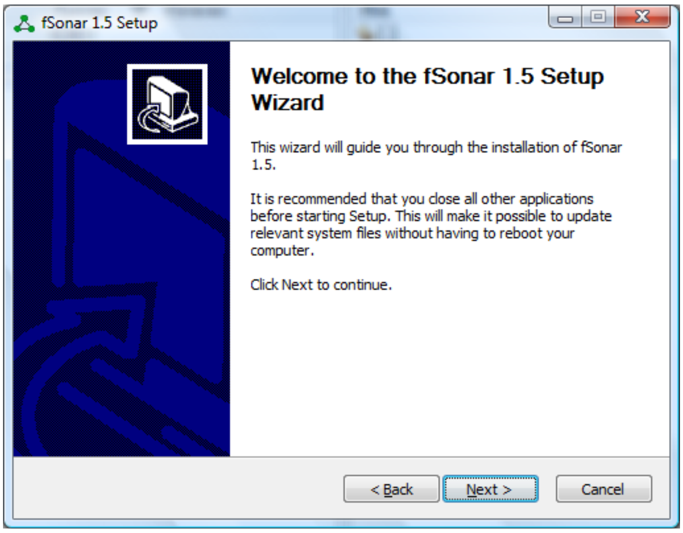
Please select a language.

Russian

Figure 2

Select the required languages. Now two languages are supported: English and Russian.

Click **OK**. The window appears as shown in Figure 3.



fSonar 1.5 Setup

Welcome to the fSonar 1.5 Setup Wizard

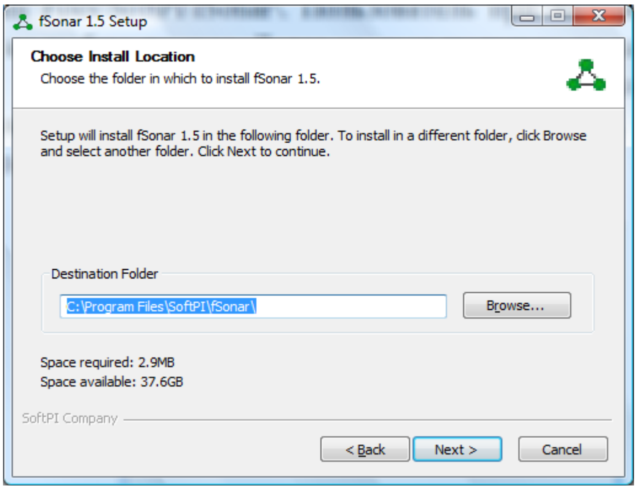
This wizard will guide you through the installation of fSonar 1.5.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

Figure 3

Click **Next.** The window appears as shown if Figure 3. Enter the required folder to install the program. By default, the folder is used: **....\Program Files\SoftPI\fSonar\**


fSonar 1.5 Setup

Choose Install Location

Choose the folder in which to install fSonar 1.5.

Setup will install fSonar 1.5 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder

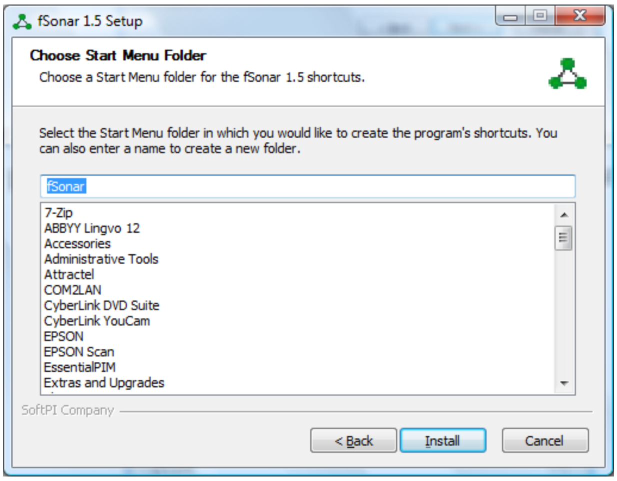
C:\Program Files\SoftPI\fSonar\

Space required: 2.9MB
Space available: 37.6GB

SoftPI Company

Figure 4

Click **Next**. The window appears as shown if Figure 5. This window allows to change the program name that is used in the **Start** menu. By default name: **fSonar**.


fSonar 1.5 Setup

Choose Start Menu Folder

Choose a Start Menu folder for the fSonar 1.5 shortcuts.

Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.

fSonar

- 7-Zip
- ABBYY Lingvo 12
- Accessories
- Administrative Tools
- Attractel
- COM2LAN
- CyberLink DVD Suite
- CyberLink YouCam
- EPSON
- EPSON Scan
- EssentialPIM
- Extras and Upgrades

SoftPI Company

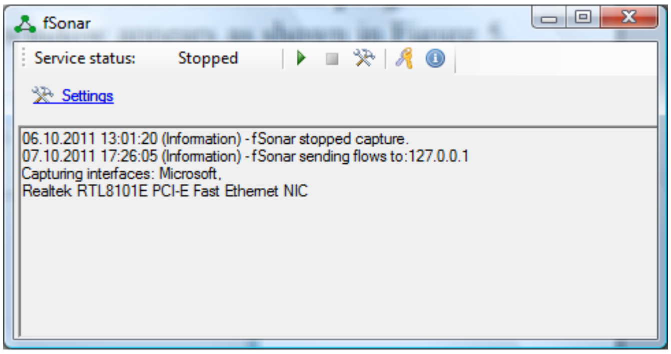
Figure 5

Click **Next**. The program will be installed.

Activation

If you plan to use the program, you should buy the licence and activate the program.

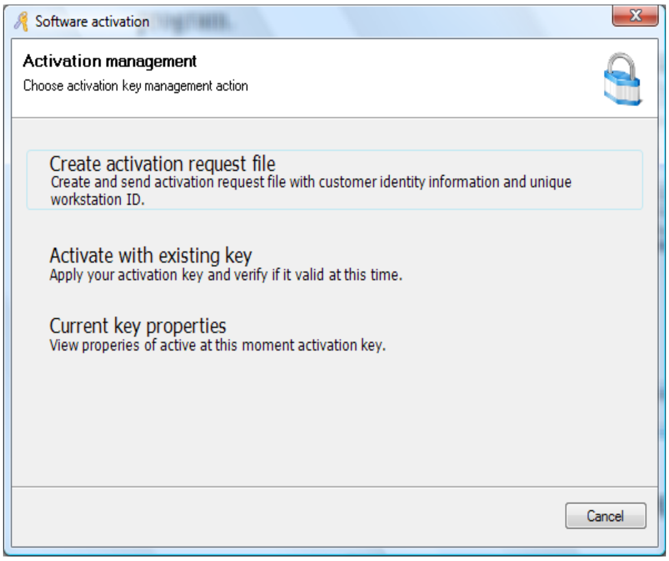
To activate the program, run it. Select from **Start** menu: **All programs** → **fSonar** → **Configure NetFlow sensor**. The window appears as shown in Figure 6.



```
06.10.2011 13:01:20 (Information) - fSonar stopped capture.
07.10.2011 17:26:05 (Information) - fSonar sending flows to:127.0.0.1
Capturing interfaces: Microsoft,
Realtek RTL8101E PCI-E Fast Ethernet NIC
```

Figure 6

Click on the button. As a result the window appears as shown in Figure 7.



Activation management

Choose activation key management action

Create activation request file
Create and send activation request file with customer identity information and unique workstation ID.

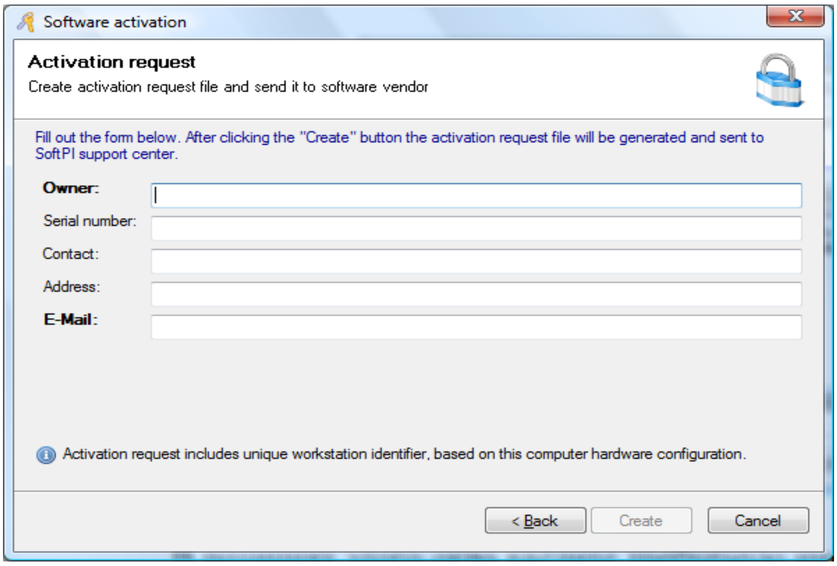
Activate with existing key
Apply your activation key and verify if it valid at this time.

Current key properties
View properies of active at this moment activation key.

Figure 7

Click on the **Create activation request file**. The **Software activation** window appears as shown in Figure 8.
Type the appropriate information in the **Owner**, **Serial number**, **Contact**, **Address** and **E-Mail** boxes.

<u>**Note**</u>. *Check the correctness of data, especially for parameters such as:* ***Owner, Serial number*** *and* ***E-Mail****. Incorrectly entered value of first two parameters do not allow to identify the owner and, accordingly, to create a registration key. The incorrect e-mail address will not allow you to get the activation key.*


Software activation

Activation request

Create activation request file and send it to software vendor

Fill out the form below. After clicking the "Create" button the activation request file will be generated and sent to SoftPI support center.

Owner:

Serial number:

Contact:

Address:

E-Mail:

Activation request includes unique workstation identifier, based on this computer hardware configuration.

Figure 8

Click on the **Create** button. If your computer has access to Internet, activation key automatically sends to owner.

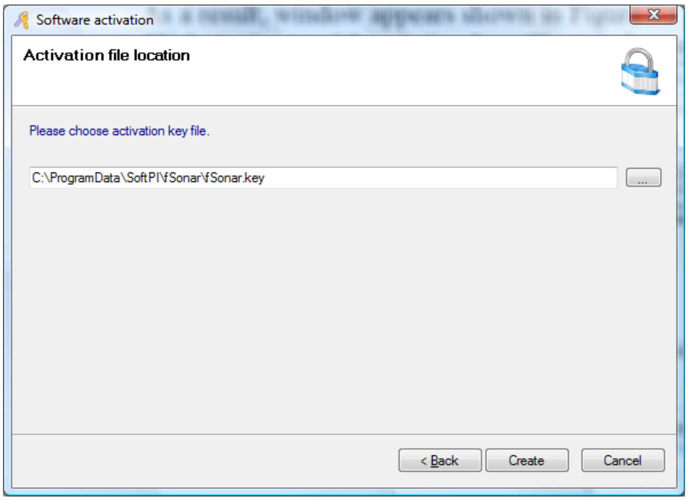
Otherwise, the window appears where requested to send your registration information via e-mail manually to the specified email address (support@softpiua.com). Click **OK**. The window appears where you should select the desired folder to save the **register.rk** file.

Click **Save** and send the file to SoftPI support service.

Based on the send registration file will be generated activation key, which is an e-mail will be sent to you.

After receiving the activation key, you should click on the 🔑 button again. As a result, window appears shown in Figure 7.

Click **Activate with existing key**. The window appears as shown in Figure 9.


Software activation

Activation file location

Please choose activation key file.

C:\ProgramData\SoftPI\fSonar\fSonar.key

Figure 9

Enter the required folder where the activation key is located.

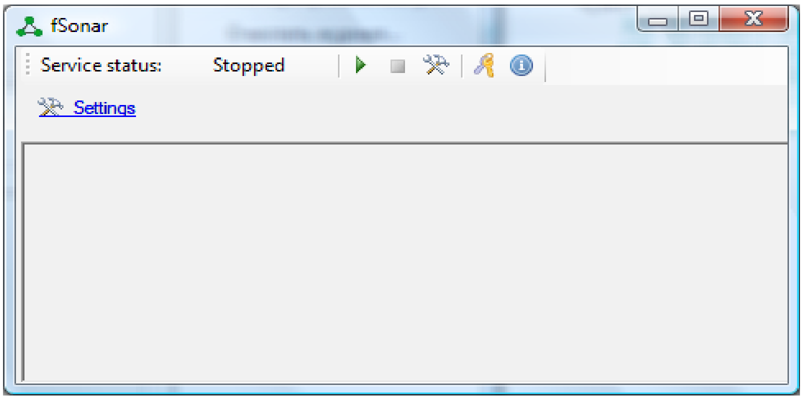
Click **Create**. The window appears where you can validate key information.

Click **Create**. On this activation is finished.

If you wish to view the parameters of the activation key, in the window shown in Figure 7, select **Current key properties**.

Settings

Start **fSonar** from Windows Menu: **Start** → **All programs** → **fSonar** → **Configure NetFlow sensor**. The **fSonar** window appears as shown in figure 10.



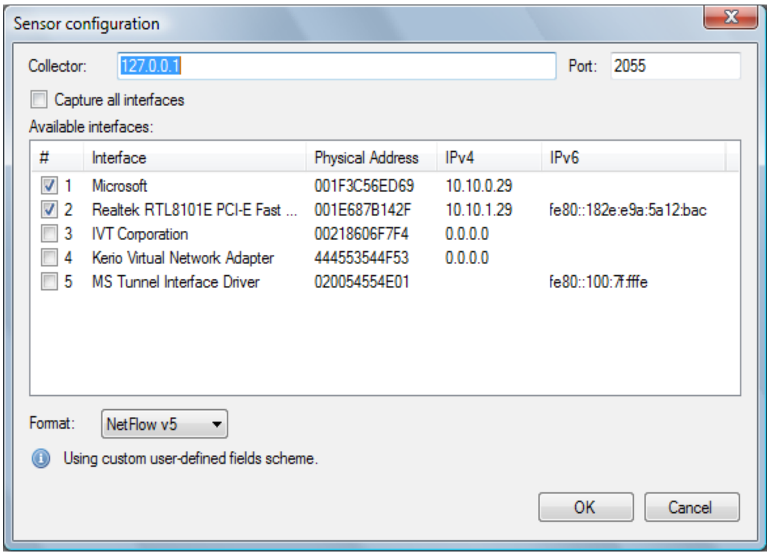
Service status: Stopped

Figure 10

The window contains toolbar, where the current status of the **fSonar** service is displayed, and icons. In the figure the service status is **Stopped**. Descriptions of icons are listed in the table below.

Icon	Name	Description
▶	Start	Start of service
■	Stop	Stop of service
🛠	Settings	Settings of the service
🔑	Activation	Creation of registration information, activation of service, view the current parameters of the activation key
ℹ	About	Displays information about the program

When you first start the program should set the parameters of the service. Click on the **Settings** link. The **Sensor** configuration windows appears as shown in Figure 11.



Sensor configuration

Collector: 127.0.0.1 Port: 2055

□ Capture all interfaces

Available interfaces:

#	Interface	Physical Address	IPv4	IPv6
☑ 1	Microsoft	001F3C56ED69	10.10.0.29	
☑ 2	Realtek RTL8101E PCI-E Fast ...	001E687B142F	10.10.1.29	fe80::182e:e9a:5a12:bac
□ 3	IVT Corporation	00218606F7F4	0.0.0.0	
□ 4	Kerio Virtual Network Adapter	444553544F53	0.0.0.0	
□ 5	MS Tunnel Interface Driver	020054554E01		fe80::100:7f:fffe

Format: NetFlow v5

Using custom user-defined fields scheme.

Figure 11

In the **Collector** box, type IP address of computer, where NetFlow collector works, in IPv4 or IPv6 format.

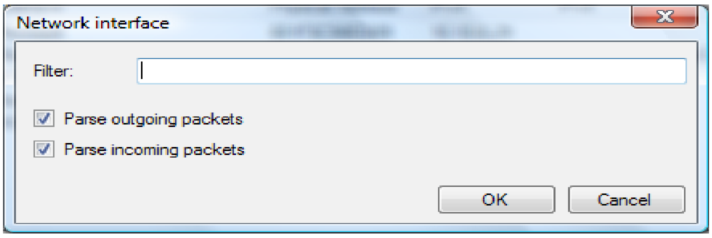
In the **Port** box, type IP port number, which is used on the computer with NetFlow Collector to collect NetFlow information.

In the **Available interfaces** table the list of available network interfaces on the computer with fSonar is displayed. The table contains the following columns:

- #;
- Interface;
- Physical address;
- IPv4;
- IPv6.

To select the required interfaces, check the box of appropriate row in the # column. If you wish to select all available interfaces, check on the **Capture all interfaces** box.

You can restrict the list of network packets is processed using a filter for a specific interface. Twice click on the required row of the table. The **Network interface** window appears as shown in Figure 12.



Network interface

Filter:

☑ Parse outgoing packets

☑ Parse incoming packets

Figure 12

If you wish to process only outgoing packets, click on the **Parse outgoing packets** box.

If you wish to process only incoming packets, click on the **Parse incoming packets** box.

Type filter parameters in the **Filter** box. The capture filter syntax is the same as in tcpdump, Wireshark and others. Description of syntax you can see, for example: http://www.tcpdump.org/tcpdump_man.html

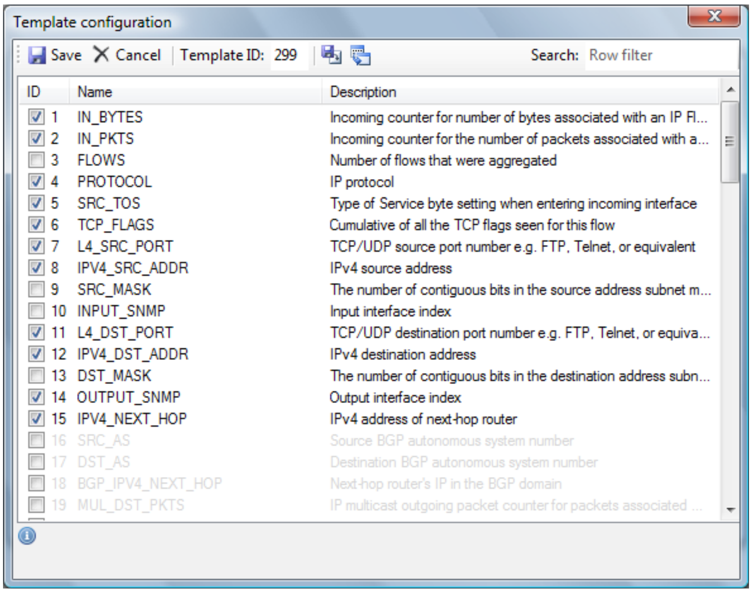
If the user does not need data on all information passing through a specific interface, we recommend to set a filter selecting only the required information. This will reduce the load on the processor and the interface through which to send the data flow if the flow collector is located on another computer on the network.

In the **Sensor configuration** window (Figure 11), select the required protocol:

- NetFlow v5,
- NetFlow v9.

In order to determine which protocol is best suited to you, you should review the list of fields that are supported by each of the protocols. It should be borne in mind that not all the fields specified for NetFlow version 9 supported (they appear in the program in gray).

For NetFlow v9 you can customize the template - a set of fields to be exported. NetFlow v5 has a fixed set of fields, all of which are exported. To select the required fields, NetFlow v9, select this protocol in the **Format** list and click on the **Scheme** button, which will lead to the appearance of the window shown in the Figure 13.



Template ID: 299

ID	Name	Description
☑ 1	IN_BYTES	Incoming counter for number of bytes associated with an IP Fl...
☑ 2	IN_PKTS	Incoming counter for the number of packets associated with a...
□ 3	FLOWS	Number of flows that were aggregated
☑ 4	PROTOCOL	IP protocol
☑ 5	SRC_TOS	Type of Service byte setting when entering incoming interface
☑ 6	TCP_FLAGS	Cumulative of all the TCP flags seen for this flow
☑ 7	L4_SRC_PORT	TCP/UDP source port number e.g. FTP, Telnet, or equivalent
☑ 8	IPV4_SRC_ADDR	IPv4 source address
□ 9	SRC_MASK	The number of contiguous bits in the source address subnet m...
□ 10	INPUT_SNMP	Input interface index
☑ 11	L4_DST_PORT	TCP/UDP destination port number e.g. FTP, Telnet, or equiva...
☑ 12	IPV4_DST_ADDR	IPv4 destination address
□ 13	DST_MASK	The number of contiguous bits in the destination address subn...
☑ 14	OUTPUT_SNMP	Output interface index
☑ 15	IPV4_NEXT_HOP	IPv4 address of next-hop router
□ 16	SRC_AS	Source BGP autonomous system number
□ 17	DST_AS	Destination BGP autonomous system number
□ 18	BGP_IPV4_NEXT_HOP	Next-hop router's IP in the BGP domain
□ 19	MUL_DST_PKTS	IP multicast outgoing packet counter for packets associated ...

Figure 13

You can select the fields that should be present in the exported flow. To speed up the search for the required field, you can type the required word in the **Search** box. When you type characters in this box records will be filtered that contain a set of typed characters. After you have selected the required fields, click on the **Save** button, which will ensure the continued use of this selected fields.

You can save a template in an external file for using this template in the future or on an other computer, for example, if you configure a specific set of fields that must be set on multiple computers. To do this, click on the **Save options** button and select the desired folder and enter a file name.

To specify a list of fields from a template file, click on the **Load options** button, window appears, where you must select the desired file.

At this the program configuration is completed.

Start and stop of service

Click on the **Start** button for starting the service.

Click on the **Stop** button for stopping the service.

Managing the fSonar is also possible via the **Services** control of Windows, where it is called "**fSonar sensor**".

The window of the **Configure NetFlow sensor** program displays the service log. Displays the date and time of start/stop service fSonar, a list of interfaces on which NetFlow flow is generated, as well as errors that may occur during operation.

Technical Support

For any technical issues with the fSonar program please contact Technical Support:

E-mail: support@softpiua.com

Site: http://www.softpiua.com