Scrutinizer

Getting Started Guide

A message from Plixer International:

Thank you for taking the time to download and install Scrutinizer NetFlow & sFlow Analyzer. We believe that Scrutinizer is a useful tool for any Network industry professional.

Our goal when developing Scrutinizer was to make everything from installation to operation to removal as easy as possible. We feel that we have succeeded. However, if you struggle at any point, we strongly encourage you to contact the support team at plixer or that of your local distributor. You can even post your questions or findings to our forum. Someone will always be available to help.

Again, we thank you for supporting plixer and our products, and hope to hear any feedback you might have after using Scrutinizer.

Sincerely,

The plixer International Team

Table of Contents

Intro to NetFlow

What is NetFlow?

NetFlow is a protocol used for collecting network traffic information, which was developed by Cisco Systems, Inc.

NetFlow enabled devices, which include Cisco routers and switches (as well as switches and routers made by other supporting vendors) generate records, which are sent from the router in UDP packets. A NetFlow collector must then collect these packets as they stream from the router.

Some of the information that NetFlow provides is:

- What is the originating IP address, as well as destination IP of a conversation between network devices.
- When a specific network conversation ended and how long it lasted.
- How much traffic was generated by a conversation.

The information provided by NetFlow, can then be organized and stored by a software package (in this case Scrutinizer) for later analysis, or even real-time as conversations end. With NetFlow's information, Network Administrators can quickly have answers to the following questions:

- **Who** is the end system causing the traffic?
- **What** is the application/protocol being used?
- **When** was the traffic was occurring?
- **Where** is the network connection being affected?

Note: Routers will only send the information pertaining to a given conversation after it has ended. However, NetFlow does allow for routers to summarize conversation in user defined intervals which can make the information stream more accurately.

What devices support NetFlow?

Cisco Routers:

Use the chart below to determine if your routers are capable of sending NetFlow information to Scrutinizer. Just locate your IOS release and see if your router model is listed.

NetFlow Export Support by IOS Version

Cisco IOS release	NetFlow Version(s)	Models
11.1CA	v1, v5	Cisco: 7200, 7500 series were the first platforms in 11.1CA. v5 is now available for all IOS platforms.
12.3(1),12.0(24)S, 12.2(18)S, 12.3(2)T	v9	Cisco 800, 1700, 2600, 3600, 3700, 3800, 6400,7200,7300,7500, and12000
12.0(14)S	v5	Cisco 12000
12.0(6)S	v8	Cisco 12000
12.1(1)E/12.2SX **(see below)**	v5,v7,v8	Catalyst 65k
12.1(13)EW	v5	Catalyst 4k Supervisor 4
12.1(19)EW	v8	Catalyst 4k Supervisor 4
12.1(18)EW	v5,v8	Catalyst 4k Supervisor 5

Catalyst 65k/7600 NetFlow Version Support

Supervisor	Hybrid	Native 12.1E	Native 12.2SX
MSFCx	v5	v5	v5, v8*
Sup1a	V7, v8	v7	N/A
Sup2	v7, v8	v5, v7	v5, v7, v8
Sup720	v5, v7, v8	v5, v7	v5, v7, v8

Demand for NetFlow and sFlow support has grown exponentially over the last few years, as more and more vendors are realizing the benefits of the information that is provided by NetFlow and sFlow.

Other Vendors:

Here are a few of the major vendors that now support NetFlow or sFlow:

- Enterasys
- Foundry
- Juniper

Getting Started

Configuring your Cisco Routers to send NetFlow to Scrutinizer.

The beauty of NetFlow is that when using a supported router or switch, you simply need to telnet to each device and turn NetFlow on. There should never be a need to install any additional software or hardware if the device is compatible.

Once you have an open telnet session with your router or switch, please enter the global commands listed below:

```
(config)#ip flow-export source <interface number>
(config)#ip flow-export version 5 peer-as
(config)#ip flow-export destination<ip address> <port number>
(config)#ip flow-cache timeout active 1
```

Use the commands below to enable NetFlow on each physical interface of each device you are interested in collecting flows from (i.e. not virtual interfaces, as they are auto included). If SNMP parameters are not configured on the device, you will need to set the speed of the interface in kilobits per second. It is especially important to set the speed for frame relay or ATM virtual circuits.

Command to type: **interface <interface>**
Command to type: **ip route-cache flow**
Command to type: **bandwidth**

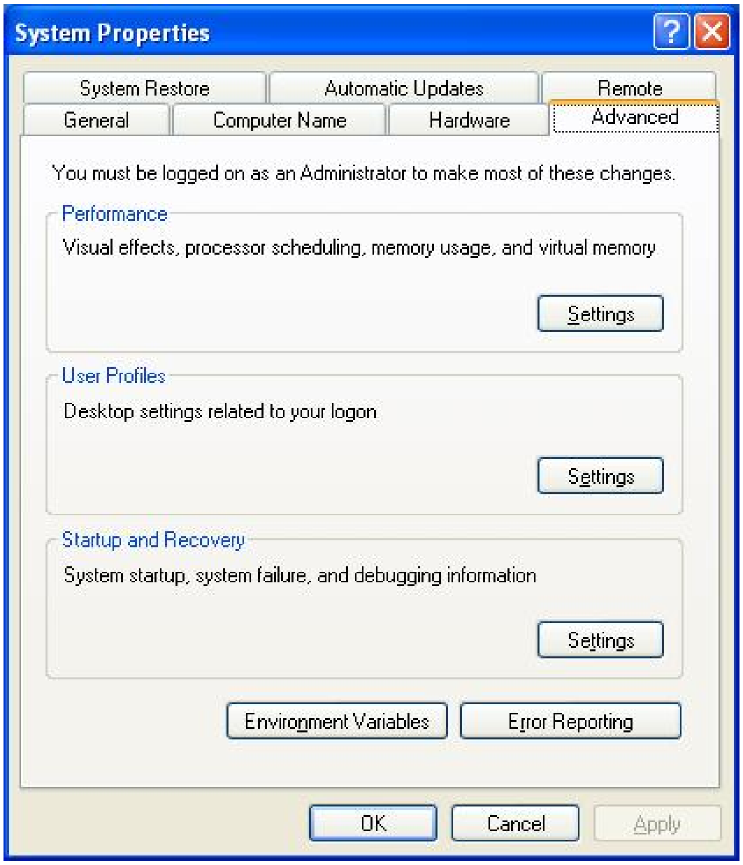
To make sure you are getting the most up-to-date information on how to correctly configure your existing routers to work with Scrutinizer, and for a more detailed list of optional commands, please visit the following link:

http://www.plixer.com/products/scrutinizer_activate-netflow.php

The Product Installation Process

First, if you have not already downloaded the installation executable, you may do so here: http://www.plixer.com/support/download_request.php.

Before installing, there are some changes that may need to be made to your DEP settings.



You must be logged on as an Administrator to make most of these changes.

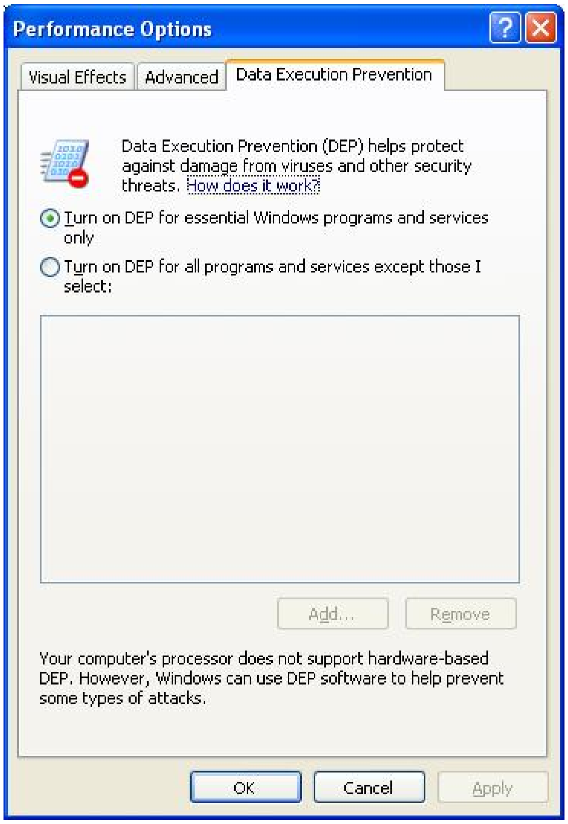
Visual effects, processor scheduling, memory usage, and virtual memory

Desktop settings related to your logon

System startup, system failure, and debugging information

Data Execution Prevention (DEP) is a set of hardware and software technologies that perform additional checks on memory to help prevent malicious code from running on a system. If certain Scrutinizer related files are prevented by DEP, then installation will fail.

On any Windows XP (SP2) or Windows Server 2003 the **“collectd.exe”** and **“index.cgi”** files should be excluded from DEP or set to Windows Services only. In order to exclude these files: Right click My Computer, select Properties and click the Advanced Tab. Next, click "Settings" under Performance and select Data Execution Prevention.



Data Execution Prevention (DEP) helps protect against damage from viruses and other security threats. How does it work?

● Turn on DEP for essential Windows programs and services only

○ Turn on DEP for all programs and services except those I select:

Your computer's processor does not support hardware-based DEP. However, Windows can use DEP software to help prevent some types of attacks.

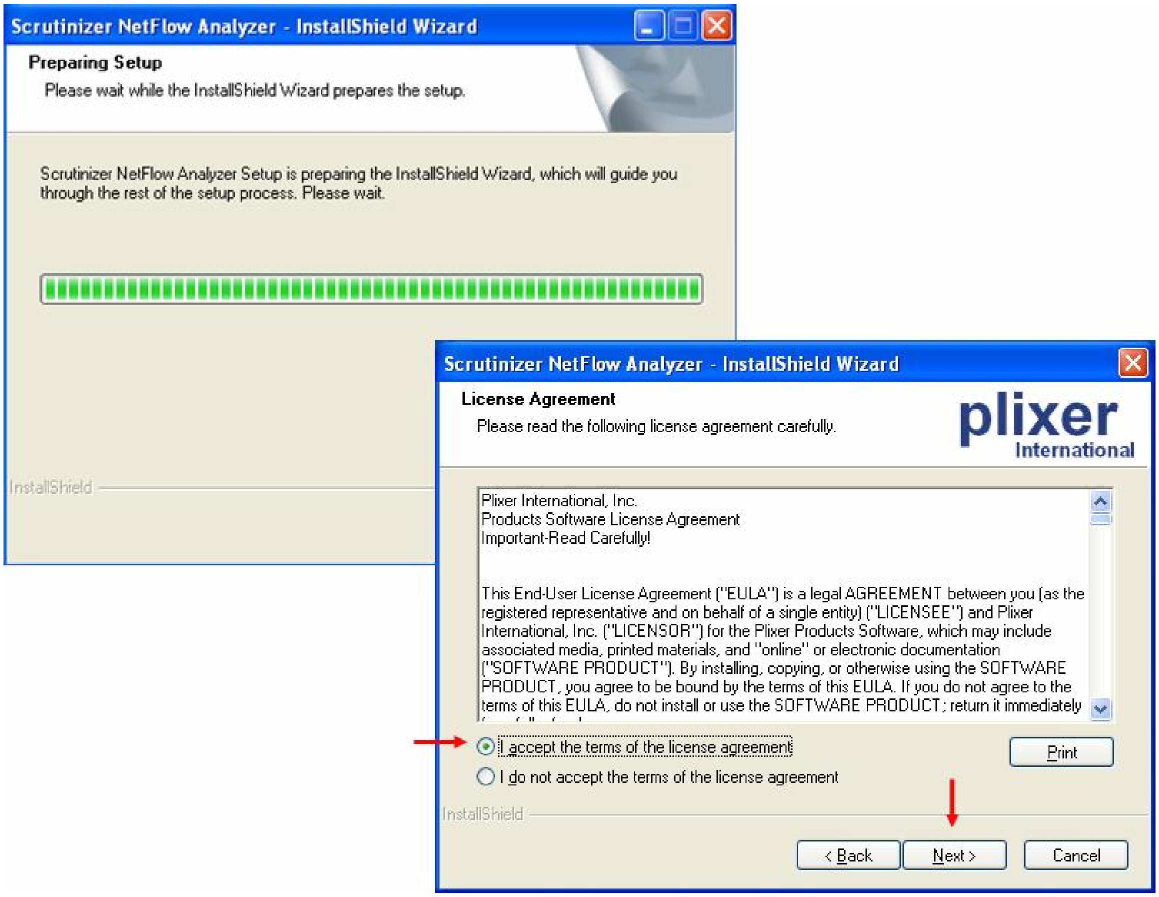
Here you have the option to "Turn on DEP for essential Windows programs and services only" or "Turn on DEP for all programs and services expect those I select:"

If you choose to disable DEP for only applications of your choice, then you will need to manually add the **"collectd.exe"** and **"index.cgi"** files found in the "\SCRUTINIZER\html\" directory.

Launch the Install Program:

Click Apply and OK when done; then OK again to exit.

Once you have successfully downloaded the "**plixer-scrutinizer-win32.exe**" file to a local directory, click the install icon to launch the Scrutinizer Installation.



Scrutinizer NetFlow Analyzer - InstallShield Wizard

Preparing Setup

Please wait while the InstallShield Wizard prepares the setup.

Scrutinizer NetFlow Analyzer Setup is preparing the InstallShield Wizard, which will guide you through the rest of the setup process. Please wait.

Scrutinizer NetFlow Analyzer - InstallShield Wizard

License Agreement

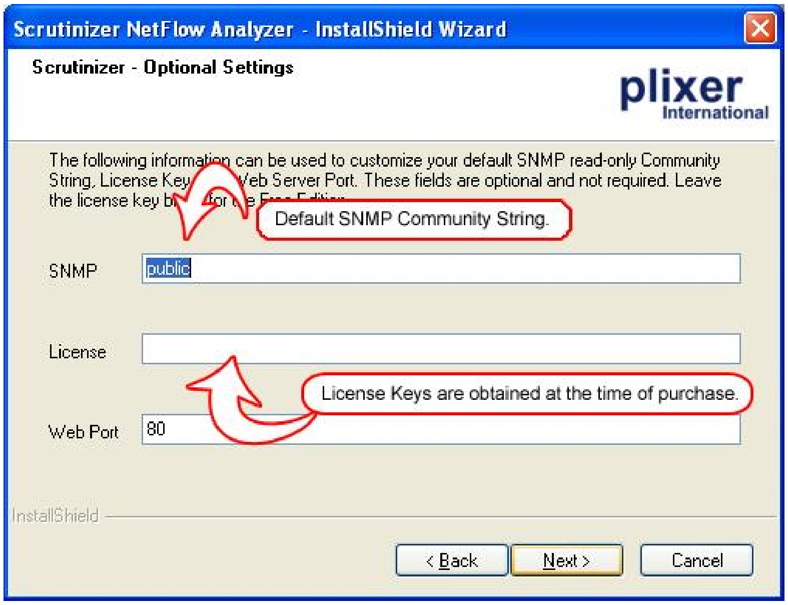
Please read the following license agreement carefully.

Plixer International, Inc.
Products Software License Agreement
Important-Read Carefully!

This End-User License Agreement ("EULA") is a legal AGREEMENT between you (as the registered representative and on behalf of a single entity) ("LICENSEE") and Plixer International, Inc. ("LICENSOR") for the Plixer Products Software, which may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). By installing, copying, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or use the SOFTWARE PRODUCT; return it immediately

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement



Scrutinizer NetFlow Analyzer - InstallShield Wizard

Scrutinizer - Optional Settings

The following information can be used to customize your default SNMP read-only Community String, License Key, and Web Server Port. These fields are optional and not required. Leave the license key blank for the Free Edition.

Default SNMP Community String.

SNMP: public

License:

License Keys are obtained at the time of purchase.

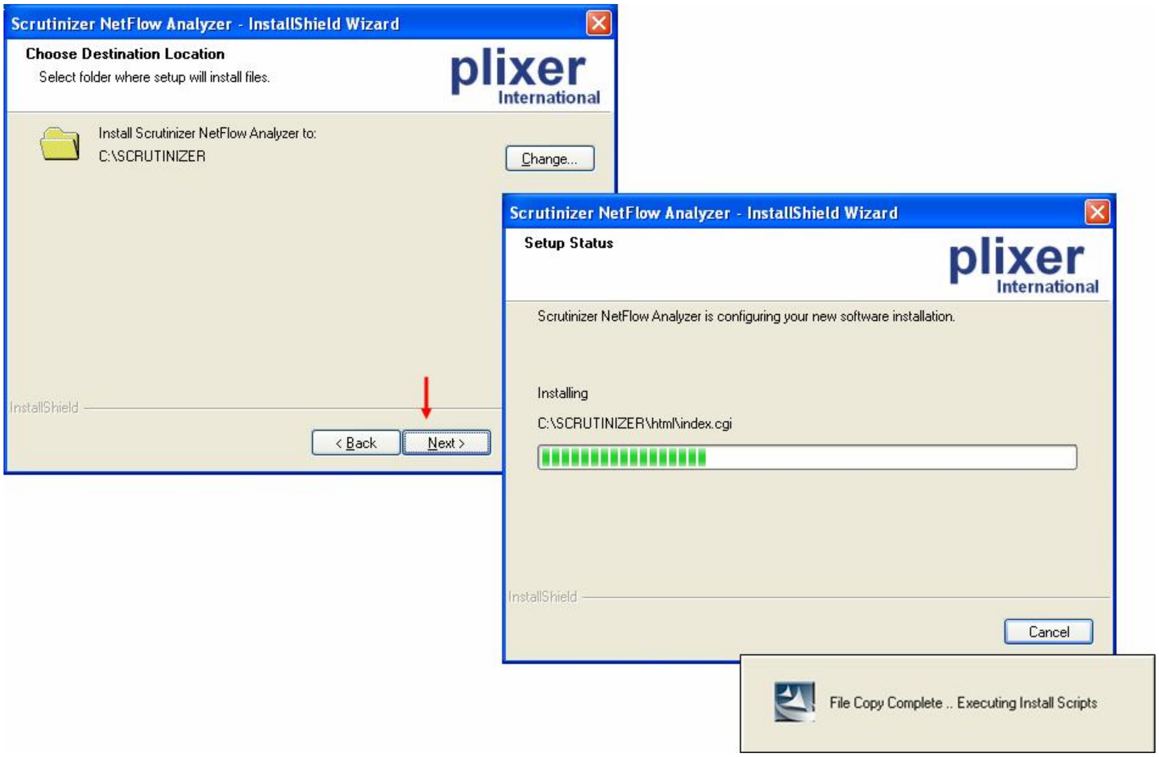
Web Port: 80

Scrutinizer does not actively poll for SNMP. However, by adding a default community string, Scrutinizer can later retrieve SNMP details from routers, as needed; in order to supplement the information provided by NetFlow for additional features and device details, such as interface speed.

To activate a commercial copy of Scrutinizer, you can enter the License Key that was provided at the time of purchase. If a key is not provided at this time, one can be entered later within the Scrutinizer settings. If you do not have a valid License Key and are interested in purchasing one, visit the link below:

http://www.plixer.com/products/purchasing.php

If you are planning to use the free version of Scrutinizer (which is limited to 1 router/ unlimited interfaces and lacks some functionality found in the commercial versions, such as real-time statistics), then simply leave the License field blank.


Scrutinizer NetFlow Analyzer - InstallShield Wizard
Choose Destination Location
plixer International
Change...
InstallShield
< Back
Next >
Scrutinizer NetFlow Analyzer - InstallShield Wizard
Setup Status
plixer International
InstallShield
Cancel

Select folder where setup will install files.

Install Scrutinizer NetFlow Analyzer to:
C:\SCRUTINIZER

Scrutinizer NetFlow Analyzer is configuring your new software installation.

Installing
C:\SCRUTINIZER\html\index.cgi

File Copy Complete .. Executing Install Scripts

Using Scrutinizer

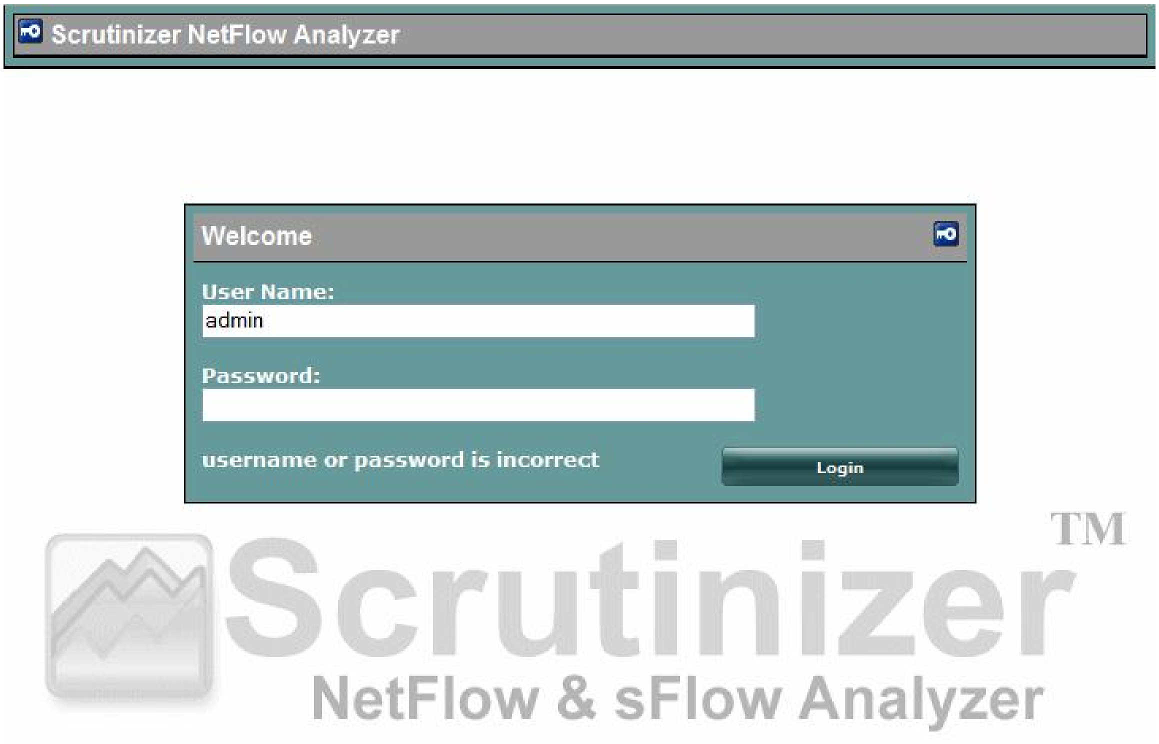
Launching Scrutinizer for the first time.

Scrutinizer

After the install has finished, double-click the newly created shortcut located on the desktop. This will launch Scrutinizer in the default web browser.

The first screen that appears is the Scrutinizer Log In screen. To protect the sensitive network information found in Scrutinizer, authentication is always enabled and a password must be entered to view the user interface.

At first log in, a User Name and Password of admin/admin must be entered. This should be changed to a more secure alternative as soon as possible.



User Name: admin

Password:

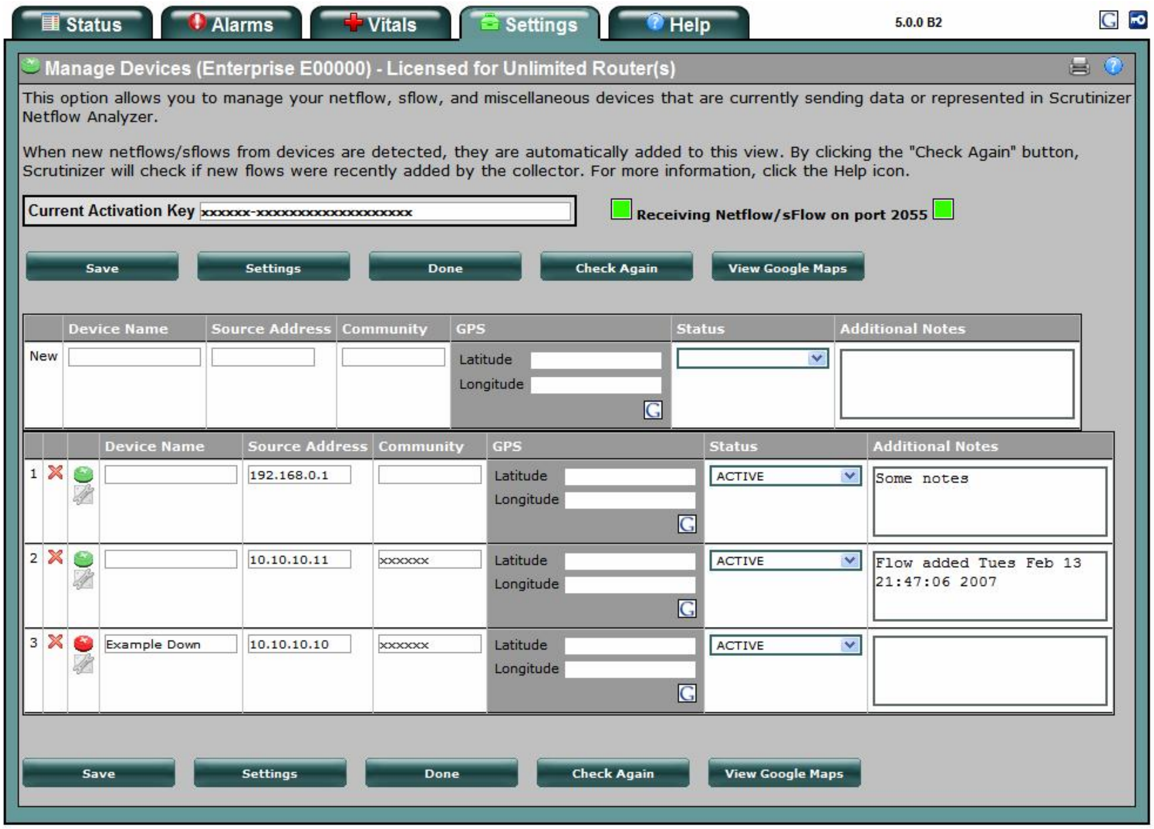
username or password is incorrect

For more information on managing user accounts and passwords, please reference the Scrutinizer Product Manual, which can be accessed by clicking the icon in the upper right hand corner of any screen.

An online version of the Scrutinizer Product Manual can be found at: http://www.plixer.com/manual/index.html.

Assuming that your routers are configured correctly, you will be directed to the status screen, where you will start receiving flows.

If Scrutinizer is not receiving NetFlow, it will direct you to the MANAGE NETFLOWS screen. Scrutinizer is smart enough to recognize incoming NetFlow from any number of routers or switches without any kind of configuration within the product.



Manage Devices (Enterprise E00000) - Licensed for Unlimited Router(s)

This option allows you to manage your netflow, sflow, and miscellaneous devices that are currently sending data or represented in Scrutinizer Netflow Analyzer.

When new netflows/sflows from devices are detected, they are automatically added to this view. By clicking the "Check Again" button, Scrutinizer will check if new flows were recently added by the collector. For more information, click the Help icon.

Current Activation Key xxxxxx-xxxxxxxxxxxxxxxxxxxx

🟩 Receiving Netflow/sFlow on port 2055 🟩

	Device Name	Source Address	Community	GPS	Status	Additional Notes
New				Latitude Longitude		

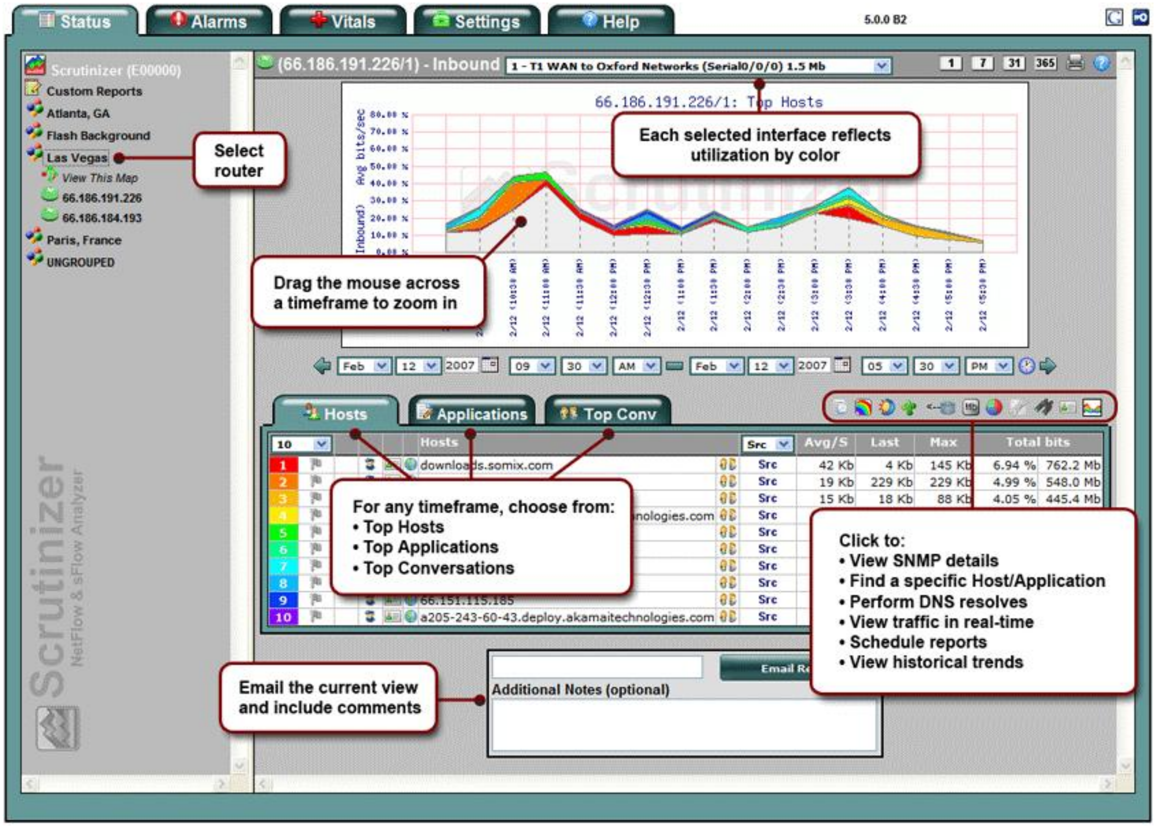
			Device Name	Source Address	Community	GPS	Status	Additional Notes
1	✗	●		192.168.0.1		Latitude Longitude	ACTIVE	Some notes
2	✗	●		10.10.10.11	xxxxxx	Latitude Longitude	ACTIVE	Flow added Tues Feb 13 21:47:06 2007
3	✗	●	Example Down	10.10.10.10	xxxxxx	Latitude Longitude	ACTIVE	

If you are directed to this page, please refer to the configuring NetFlow section of this guide, configure your routers, and click “Check Again”.

The only thing left to do is wait several minutes for the NetFlow intervals to build up.

Scrutinizer Interface Screen Tips

Below is a quick look at some of the functionality found on the Scrutinizer "Interface Page".



Select router

Each selected interface reflects utilization by color

Drag the mouse across a timeframe to zoom in

For any timeframe, choose from:
- Top Hosts
- Top Applications
- Top Conversations

Click to:
- View SNMP details
- Find a specific Host/Application
- Perform DNS resolves
- View traffic in real-time
- Schedule reports
- View historical trends

Email the current view and include comments

Your Scrutinizer NetFlow & sFlow Analyzer should now be fully operational and displaying the information you are looking for. Hopefully this "Quick Start Guide" was useful in helping to get Scrutinizer up and running quickly.

For a more detailed reference, the user manual can be accessed by clicking on the ? icon in the upper right hand corner. Accessing the product manual in this manner is highly recommended, as the product help is context sensitive to the page currently being viewed.

An up-to-date online version of the Scrutinizer Product Manual can be found at: http://www.plixer.com/manual/index.html.