

NetFlow Auditor Manual

Getting Started

[^Top](#)

Setting up NetFlow

[^Top](#)

Check if your Routers or Switches Supports NetFlow.

Almost all Cisco devices support NetFlow since its introduction in the 11.1 train of Cisco IOS Software and because of this, NetFlow is most likely available in any devices in the network. Some caveats apply. Please check your Cisco documentation.

ref:

http://www.cisco.com/en/US/products/ps6601/products_white_paper0900aecd80406232.shtml

Device	Supported
Cisco 800, 1700, 2600	Yes
Cisco 1800, 2800, 3800	Yes
Cisco 4500	Yes
Cisco 6500	Yes
Cisco 7200, 7300, 7500	Yes
Cisco 7600	Yes
Cisco 10000, 12000, CRS-1	Yes
Cisco 2900, 3500, 3660, 3750	No

NetFlow commands quick start summary

This quick start will help you with the commands but we strongly advise you read the NetFlow commands for NetFlow Auditor explained

(<http://digitoll.net/forum/viewtopic.php?f=42&t=50>)

to understand why the options below were chosen.

General NetFlow commands:

Enable on each interface (Except when using CEF with a NetFlow Daughter card)

* ip route-cache flow

General Commands

```
* ip cef
* ip flow-export source Loopback0
* ip flow-export version [5/7/9] [peer-as | origin-as]
* ip flow-cache timeout inactive 15
* ip flow-cache timeout active 1
* ip flow ingress infer-fields
* snmp-server ifindex persist
* ip flow-export destination [DigiToll IP| NetFlow Auditor IP] 2055
```

When running NetFlow on Cisco 7600 switches in native mode use

Enable on each interface

```
* ip route-cache flow

* mls nde sender version 5
* mls flow ip interface-full
* mls aging long 64
* ip flow-export source Loopback0
* ip flow-export version [5/7/9]
* ip flow-export destination [DigiToll IP| NetFlow Auditor IP] 2055
* snmp-server ifindex persist
```

Software Platform Configuration

The following is an example of a basic router configuration for NetFlow. NetFlow basic functionality is very easy to configure. NetFlow is configured on a per interface basis. When NetFlow is configured on the interface, IP packet flow information will be captured into the NetFlow cache. Also, the NetFlow data can be configured to export the NetFlow data to a collection server if a server is deployed.

1. Configuring the interface to capture flows into the NetFlow cache. CEF followed by NetFlow flow capture is configured on the interface

```
Router(config)# ip cef
Router(config)# interface ethernet 1/0 .
Router(config-if)# ip flow ingress
Or
Router(config-if)# ip route-cache flow
```

Note: Either ip flow ingress or ip route-cache flow command can be used depending on the Cisco IOS Software version. Ip flow ingress is available in Cisco IOS Software Release 12.2(15)T or above.

2. This step is required if exporting the NetFlow cache to a reporting server. The version or format of the NetFlow export packet is chosen and then the destination IP address of

the export server.

The 2055 is the default UDP port NetFlow Auditor server will use to receive the UDP export from the Cisco device. You can setup multiple Port numbers and is required when using NetFlow Auditor Enterprise or Telco versions.

```
Router(config)# ip flow-export version [1|5|7|9]
Router(config)# ip flow-export destination [DigiToll|NetFlow Auditor IP] 2055
```

Ensure SNMP is enabled and you have secured it appropriately and that you have the SNMP community string and password available to configure NetFlow Auditor auto discovery.

http://www.cisco.com/en/US/tech/tk648/tk362/technologies_tech_note09186a0080094aa4.shtml

Logging into Netflow Auditor

[^Top](#)

The Netflow Auditor front end is a web application. You can enter it from any browser with an internet connection.

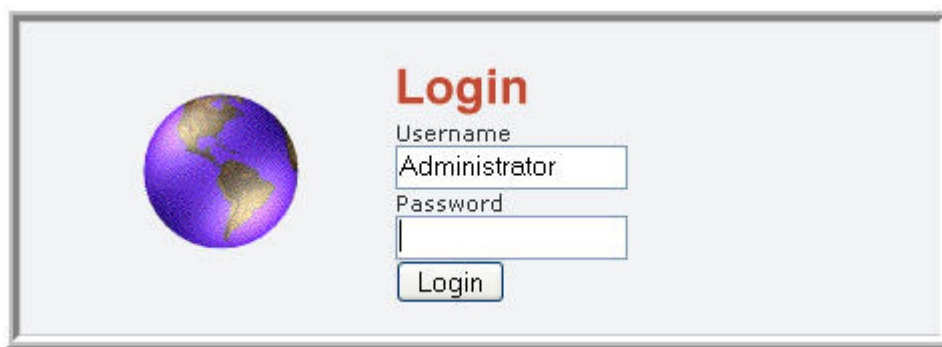
To log into the Netflow Auditor front end:

1. Enter the following IP in you browser's address bar:

`http://{host-address}/digitoll/login.do`

NOTE: The {host-address} path is supplied by your Network Administrator.

You will be presented with the Login screen.



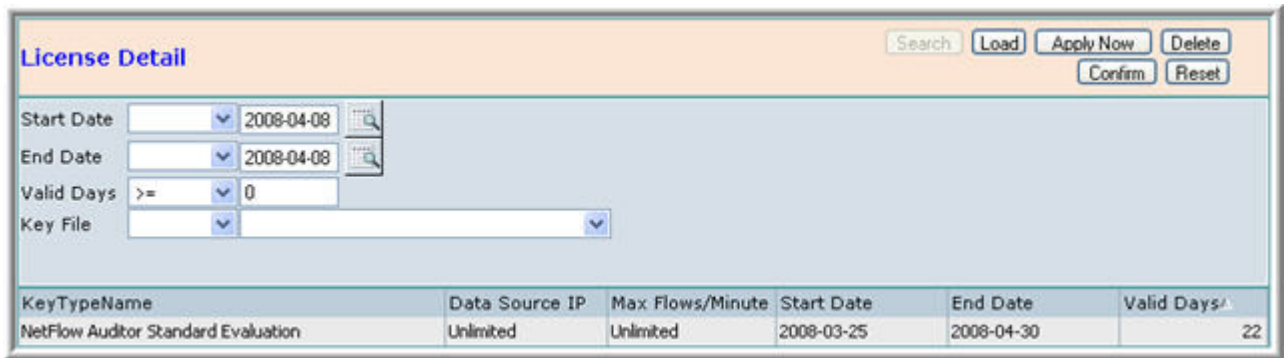
2. Enter you Username and Password in the appropriate boxes.
3. Click [**Login**] to proceed.

Successful login will send you to the Control Centre, Netflow Auditor's main screen.

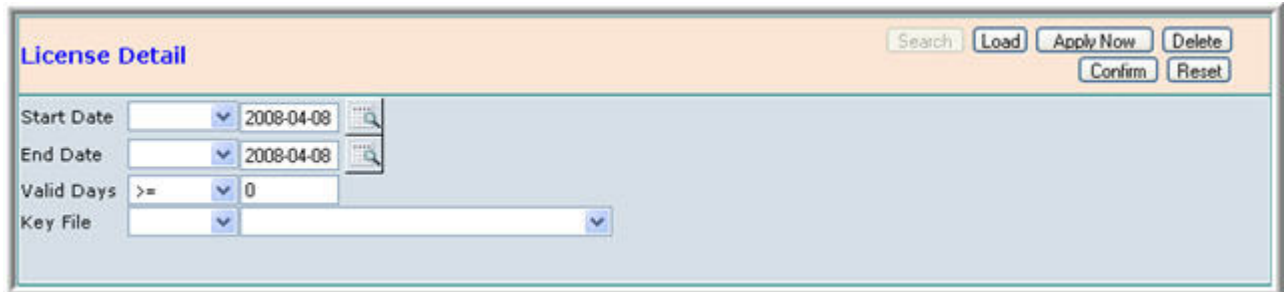
To load your license key. Click **Configuration -> Administrator -> License**



On selecting the License menu, the right side of the screen should look like the screenshot below. Note the screen is made up of two components, the top section is used to manipulate the data, you have at hand. The bottom section presents the data in a tabular form.



The screen below is used to edit, find, and delete license details. Here the screen is in its default search mode, this can be seen in the image below. To search for the details of the license, you can press the **Search** button and enter criteria to search for a license.



The table can be seen more clearly below.

KeyTypeName	Data Source IP	Max Flows/Minute	Start Date	End Date	Valid Days^
NetFlow Auditor Standard Evaluation	Unlimited	Unlimited	2008-03-25	2008-04-30	22


If this is the first time you are installing NetFlow Auditor delete the freeware license key. **Click on the license key, click Delete and Confirm**



License Detail Search Load Apply Now Delete
Confirm Reset

Start Date
End Date
Valid Days
Key File

In order to use NetFlow Auditor, you will need to have a valid license that can be verified by the program. To do this once you have received your license, you can load it into the program by simply pressing the **Load** button.



License Detail Search Load Apply Now Delete
Confirm Reset

Start Date
End Date
Valid Days
Key File
License Key Browse... **Press Confirm Button to Run !!!**

Once the license is loaded, press the **Apply Now** button to finalise the procedure, you will then be prompted to press the **Confirm** button.



License Detail Search Load Apply Now Delete
Confirm Reset

Start Date **This will restart DigiToll Backend !!!**
End Date **Press Confirm Button to Run**
Valid Days
Key File

The Netflow Auditor Main Screen

[^Top](#)



Navigation Pane

[^Top](#)

The navigation pane allows you to navigate between the various Netflow Auditor features.

Netflow Auditor's main features are represented by the following sections:

- **Long-Term** - produce pre-structured traffic analysis reports for:
 - The last month
 - The last year
- **Real-Time** - produce pre-structured traffic analysis reports for:
 - The last hour
 - The last week
- **My Analytics** - manage and configure previously saved custom reports. This includes:
 - One-off historical reports
 - Report templates for repetitive use
 - Scheduling the automatic production and delivery of these reports
- **My Alerts** - displays system alerts. These include:
 - Critical alerts (red column)
 - Warning alerts (yellow column)
 - Information alerts (green column)
- **Configuration** - define and configure the following:
 - Business Groups
 - Devices
 - Applications
 - Administrators

Toolbar

[^Top](#)

The Toolbar provides the following options:

- Navigate to previously produced report
- Navigate to next produced report
- Drill down into the current report to reveal more details.
- Configure graph display.
- Navigate to the Filter screen, where you can fine-tune the current report or produce a new custom report.
- Save the current report for future production and delivery.
- Refresh the screen.
- Print the current report.

Display Window

[^Top](#)

You can toggle between different forms of display:

- view the report as a Timeline Graph display.
- view the report as a Stacked Timeline Graph display.
- view the report as a Bar Chart display.
- view the report as a 3D Bar Chart display.
- view the report as a Stacked Bar Chart display.
- view the report as a 3D Stacked Bar Chart display.
- view the report as a Pie Chart display.
- view the report as a 3D Pie Chart display.