nBox User's Guide

ntop Software Web Management

Version 2.3

July 2015

Table of Contents

1. Introduction

Traffic measurements are necessary to operate all types of IP networks. Network admins need a detailed view of network traffic for several reasons and some of these could be security, accounting and management. The traffic compositions have to be analysed accurately when estimating traffic metrics or when finding network problems. All of these measurements have to be made by inspecting all the packets flowing into the network trunk analysed (such as router and/or switches). This analysis could be done on the fly or by logging all the packets and than post-processing them. But with the increasing network capacities and traffic volumes this kind of approach is not suitable for the most cases. Instead similar packets (packets with a set of common properties) can be grouped together composing what are called "flow". As an example, a flow can be composed of all packets that share the same 5-tuple, so a flow can be derived using only some fields of a network packet. On this way, similar types of traffic can be stored in a more compact format without loosing the information we are interested in. This information can be aggregated in a flow datagram and exported to a collector able to report network metrics in a user-friendly format.

When collected, this information provides a detailed view of the network traffic.

Precise network metric measurements are a challenging task so hard work has been done in this field. In commercial environments, NetFlow is probably the de-facto standard for network traffic accounting and billing. NetFlow is a technology which was originally created by Cisco in 1996 and is now standardised as Internet Protocol Flow Information eXport (IPFIX — RFC 3917). NetFlow is based on the probe/collector paradigm. The probe, usually part of network appliances such as routers or switches, is deployed on the measured network segment, it sends traffic information in NetFlow format towards a central collector.

nProbe is a software NetFlow v5/v9/IPFIX probe able to collect and aggregate network traffic, and export it using the standard Cisco NetFlow v5/v9/IPFIX format. It is available for most of the OSs on the market (Windows, Solaris, Linux, MacOSX). When installed on a PC, nProbe turns it into a Network-aware monitoring appliance.

Many users, who used nProbe, realised that running a network probe on a PC is not always the best choice for several reasons:

1. PCs have moving parts that can break making the probe unavailable.
2. PCs are large, need monitors and keyboards, whereas probes often need to be deployed on places where there is not much space available.
3. Administering PCs is not cheap and they require the purchase of an OS, its installation and maintenance.
4. In large networks divided in several trunks it is necessary to have several probes each analysing a trunk. This requires that multiple PC running nProbe are deployed across the network.

5. The cost (for both hardware and maintenance) of a PC+nProbe is not neglectable in particular if several probes need to be deployed.
6. In many cases, no technician are available at the monitored site and sometimes plug and play is needed.

To face these matters and to provide an All-in-One high-performance and reliable solution, nBox has been designed and developed.

nBox is based on Linux OS, and thanks to an optimised Linux kernel with the PF_RING module that significantly improves the packet capture process, nBox is able to monitor and analyse network trunks at full speed without the need of hardware accelerated cards.

The nProbe application has been carefully optimised and extended to run on the nBox server and deliver optimal performance.

If you are a user that does not want to bother with installing nProbe on a PC or you need to use a high performance and reliable network probe solution then you are probably an nBox user.

In some environments it would be nice to distribute light network probes on the network sending traffic information towards a central traffic analysis console such as ntopng or any other NetFlow/IPFIX compliant collector. In order to satisfy the above requirements nProbe and ntopng can be used together.

nBox includes both a NetFlow probe (nProbe) and a collector (ntopng) for v5/v9/IPFIX NetFlow flows.

Based on your network speed and traffic volumes different nBox server could be used.

nBox can be effectively used:

- To analyse NetFlow flows generated by your border gateway.
- To replace the embedded, low-speed NetFlow probe available on your router/switch
- As a NetFlow probe that sends flows towards one or more collectors either ntopng or a commercial one (e.g. Cisco NetFlow Collector or HP-OV).
- Both as a probe and collector at the same time. ntopng can be used as collector and analyser for nProbe-generated flows.

Finally it is worth saying that nBox is quite easy to administrate using the very intuitive embedded web interface. nBox is easy to setup and it is immediately ready to use with little configuration effort.

Throughout this document we are going to describe the main components of the nBox web interface.

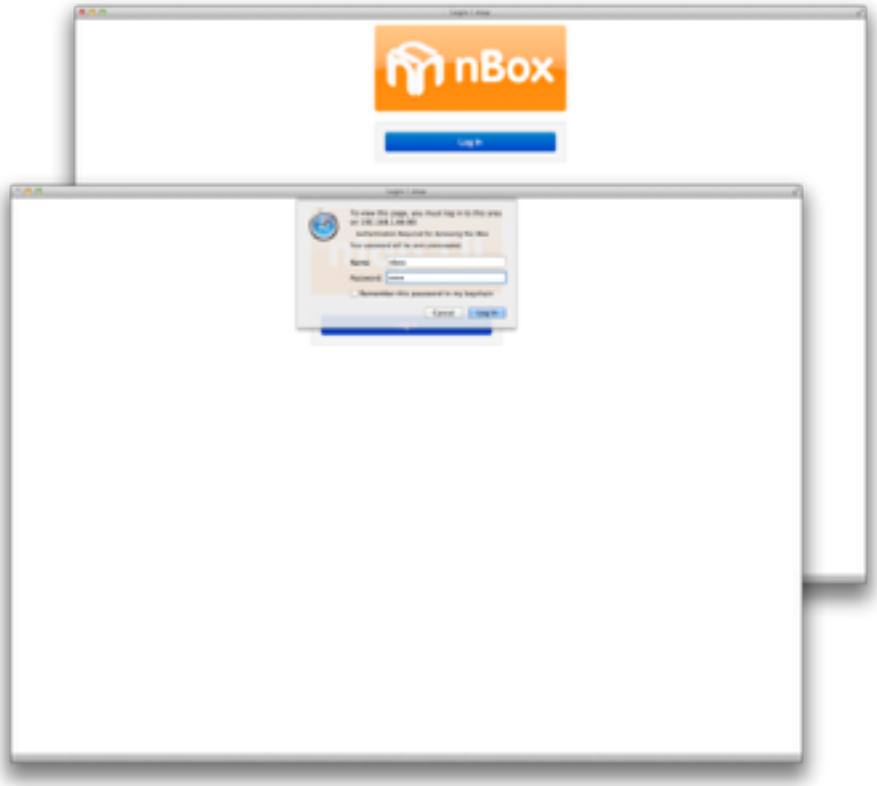
2. Using the nBox web interface

nBox has a web-based management interface used to configure and run the ntop software such as ntopng, nProbe, n2disk, disk2n and configure the packet capture framework including the PF_RING kernel module, Zero-Copy drivers and clustering.

2.1 Usage Guidelines

Starting using nBox is very simple. Startup the box, plug an Ethernet cable to its management interface and connect it to a network. From another PC open a web browser and visit http://192.168.160.10/ (the default IP address of your nBox).

Clicking on the login button the system will ask for credentials as follows:



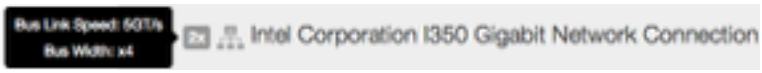
The default nBox configuration is the following:

- IP address 192.168.160.10
- Default SSH user is "root" with password "nBox"
- Default Web user is "nBox" with password "nBox"

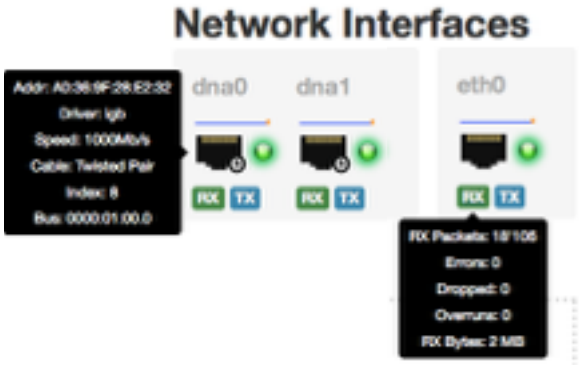
All of those could be changed using the web interface.

Upon the completion of the login process, the user is redirected to the dashboard page where most valuable informations are shown. CPU, memory, storage and network interfaces state indicators are displayed and updated in real time.

The page header displays the main characteristics of the nBox: running kernel, CPU type and number of CPU cores, RAID controller type, installed network cards, media types and link status.



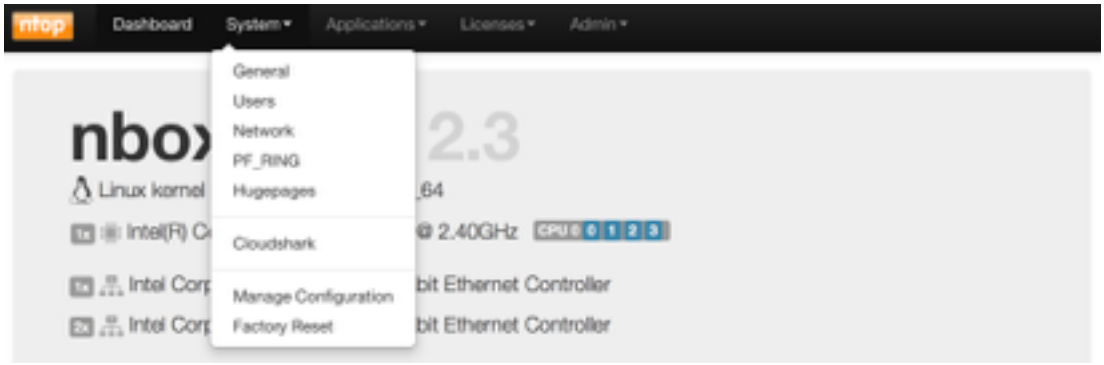
More information are provided via tooltips as shown below:



Each nBox web page comes in a three section format: header, where a menu bar is available to jump from a single configuration page to all the others quickly, the body, where the most important fields are displayed, and the footer, with additional infos. The web interface requires a javascript-enabled browser.

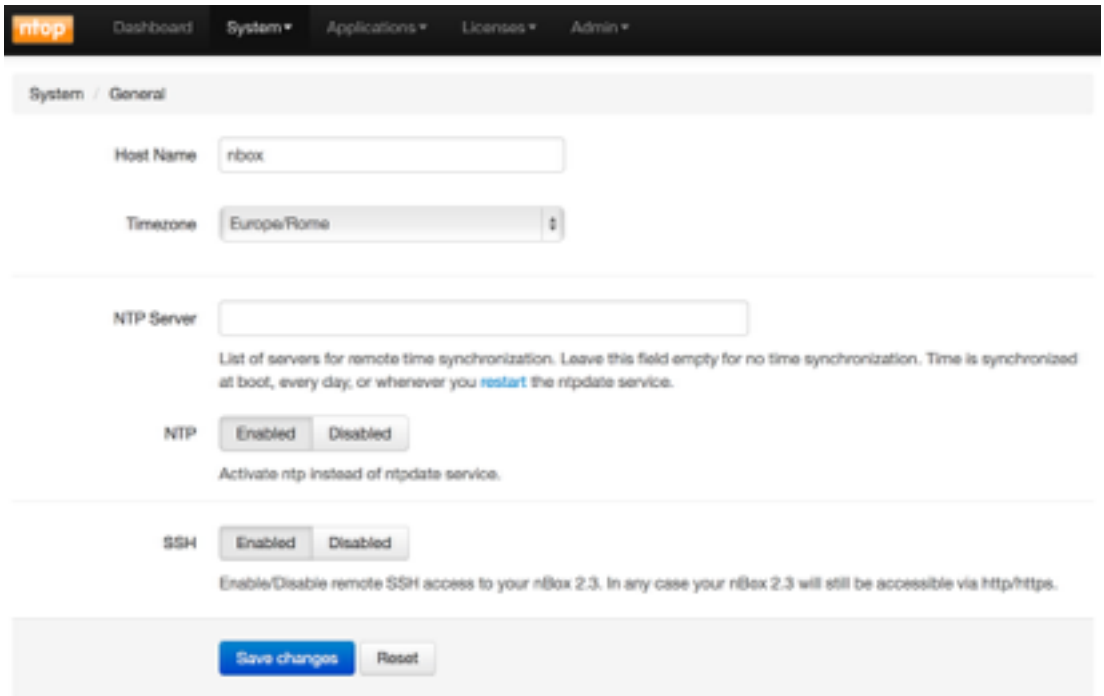
2.2 System

The System menu presents to the user a submenu where he can choose the section to configure.



General

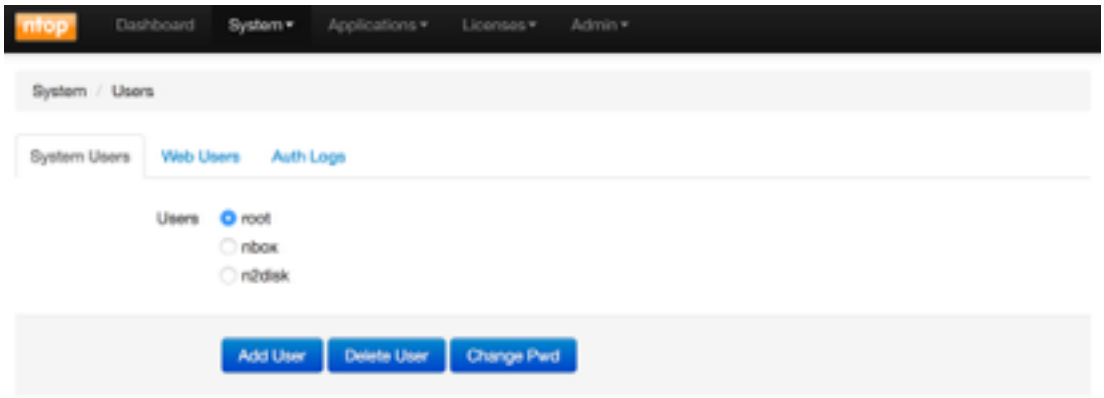
The General section contains the information about the hostname, the system timezone, the NTP and the SSH services, as displayed in the following picture:



All of those values can be changed by the user and saved into the system using the "Save Changes" button. On a successful save. a green boxed message is returned on top of the page.

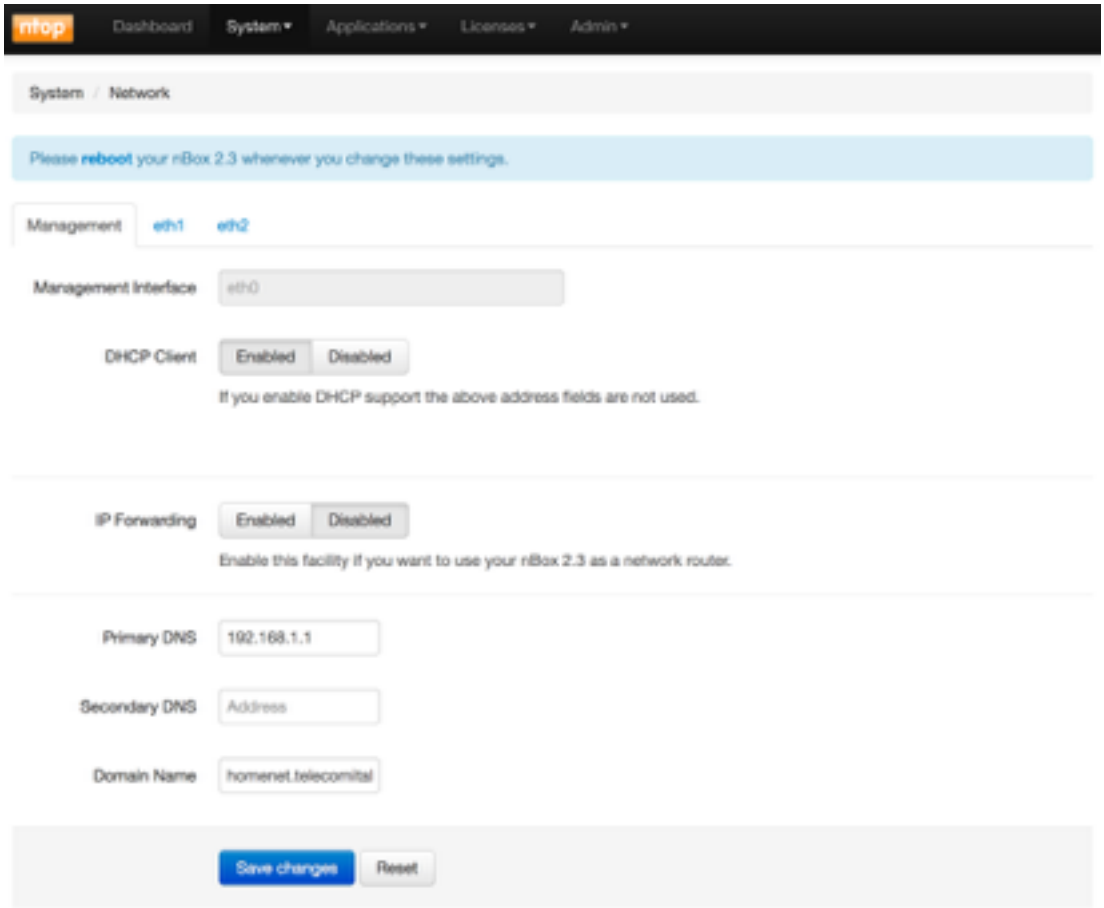
Users

The Users section should be used to control accesses to the system, managing system users and web users. The administrator switches from the system users to the web users using the available tabbed view.
On listed users, the administrator can perform some actions such as removing or changing password, or create a new one.



Network

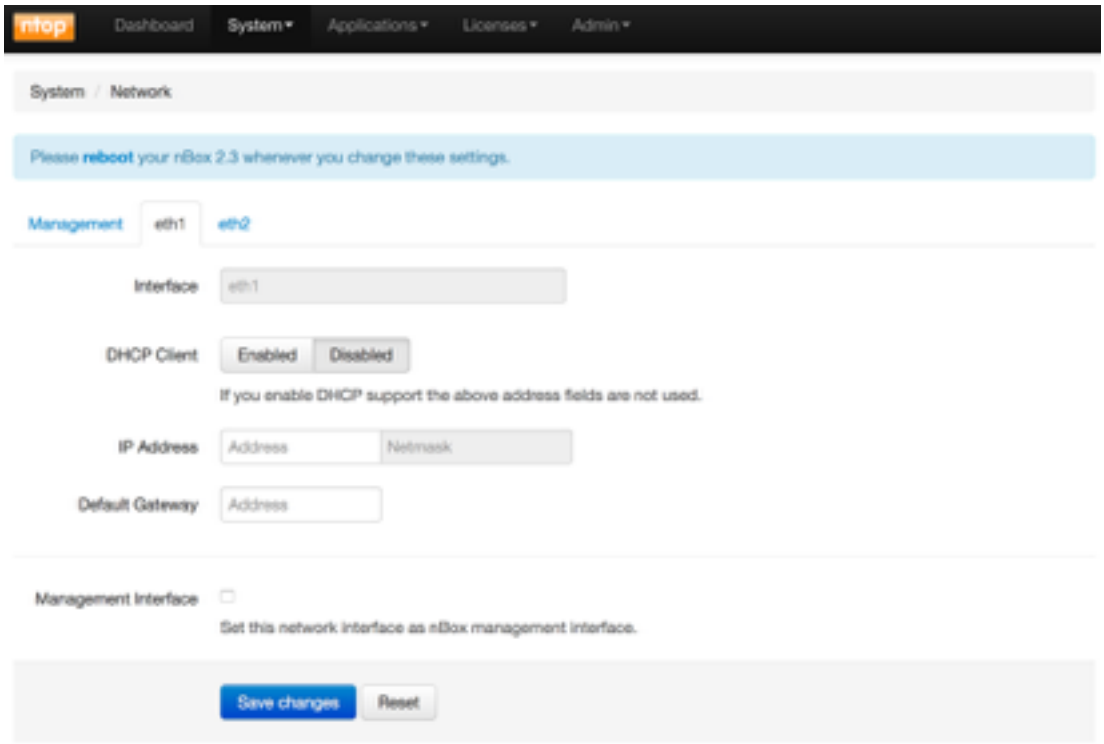
Network administration has to be performed in the Network section.



It is possible to switch from the management interfaces to the other available network interfaces using the tabbed view.

The Management tab gives the possibility to change the management ip address, using either static ip or DHCP. User can also add to the primary network interface a secondary address (Interface Alias).
By default network routing through the available interfaces is disabled, but its status can also be changed on this page.
Custom DNS server could be specified by the user.

For all the other network interfaces available on the system, the user can decide to use them as management or just configure an address on some of them.



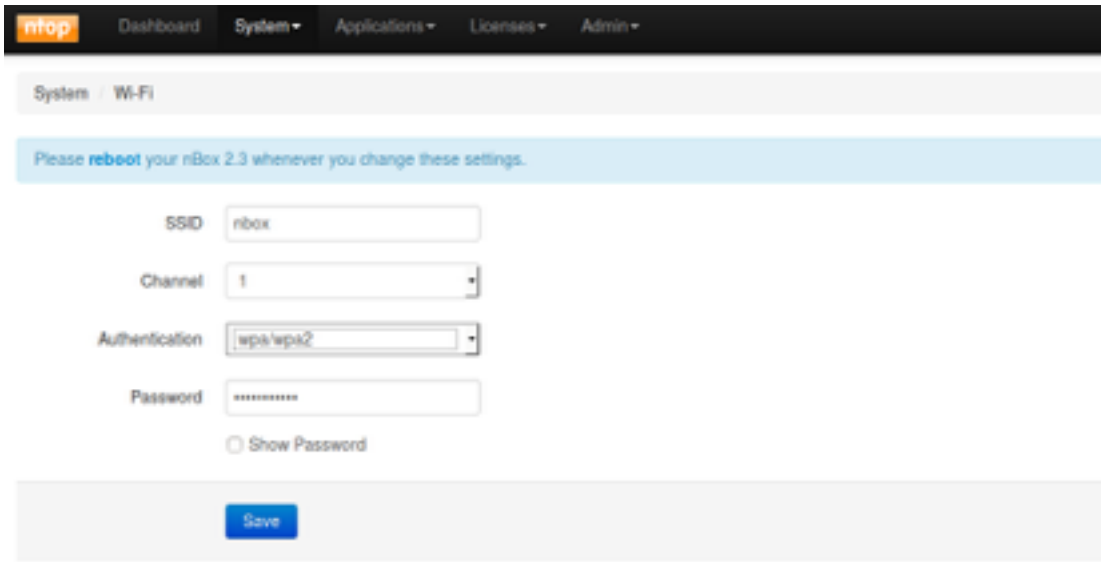
WiFi

In case a WiFi card is installed into the box, nBox creates a default configuration with the settings below:

SSID: nbox
Channel: 1
Authentication: wpa/wpa2
Password: nbox_passwd

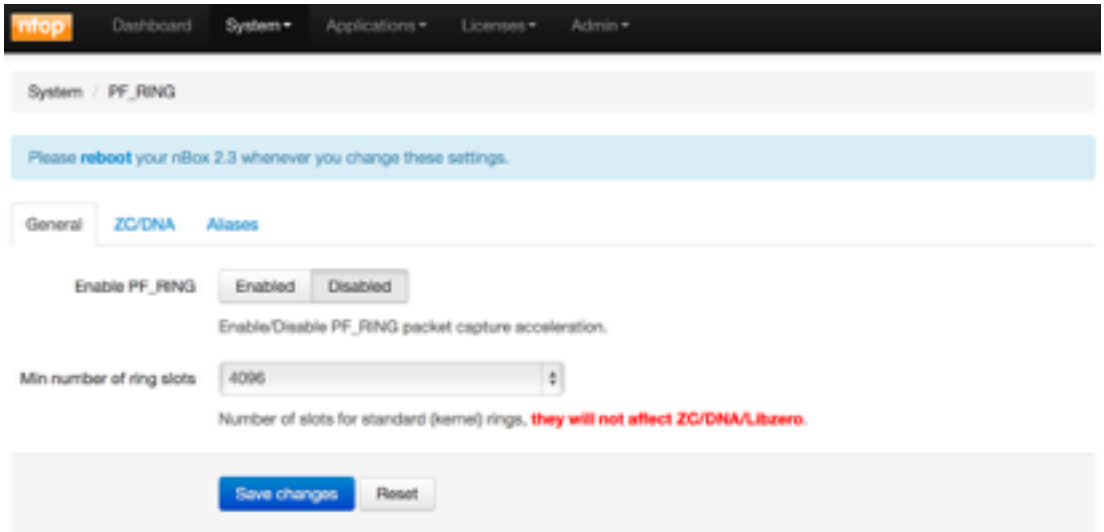
Please note that no DHCP server is configured. Running ntopng it is possible to bridge the Wireless interface to an Ethernet interface, using an external device (i.e. router) for assigning IPs to the WiFi clients.

The WiFi section allows the user to change the wireless configuration, including SSID, Authentication type and password.



PF_RING

The PF_RING section in the System menu lets the user configure the packet capture framework, including kernel module and Zero-Copy drivers.



As in the other pages, "Save Changes" is needed to commit any changes, however a reboot is required for the changes to take effect.

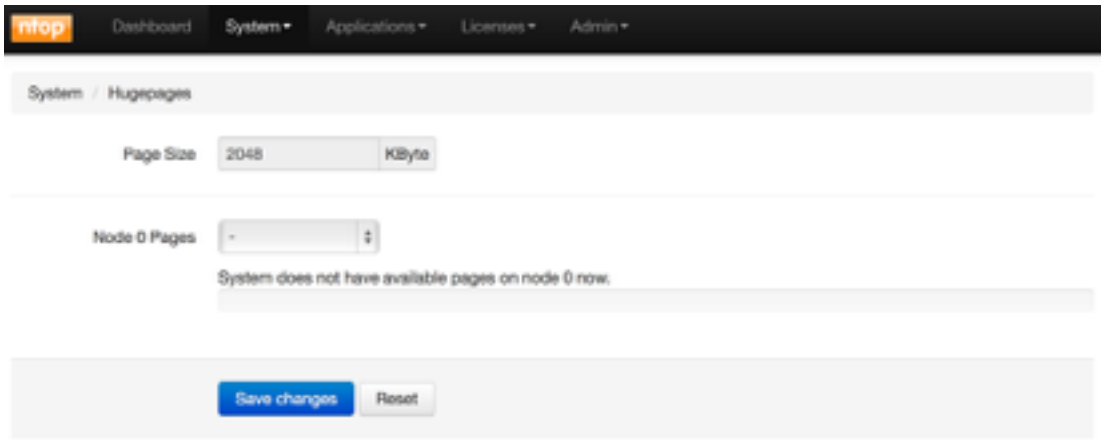
The PF_RING configuration contains the Enable/Disable button to set automatic startup and module load upon system boot, and the number of ring slots (i.e. buffer size) to be used for packet capture using vanilla drivers.

The ZC section can be used to enable or disable the Zero-Copy drivers, if licensed, on each network card with the exception of the management interface. The number of slots for RX and TX rings and the number of RSS (Receive Side Scaling) queues for hw hashing/ load balancing can be chosen.

Hugepages

nBox can exploit the advantage of using big memory pages in order to optimise performance in packet processing configuring HugePages[1].

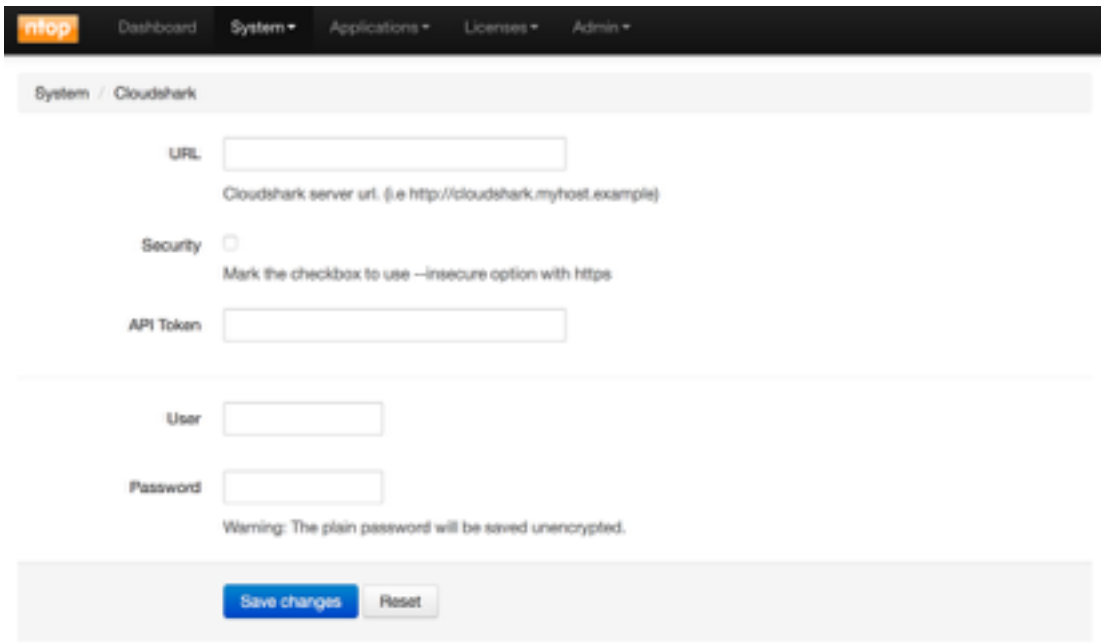
The Hugepages section allows the user to configure and load the requested number of hugepages, selecting the number of pages and committing using "Save Changes".



[1] More informations on Hugepages on http://en.wikipedia.org/wiki/Page_(computer_memory)#Huge_pages

Cloudshark

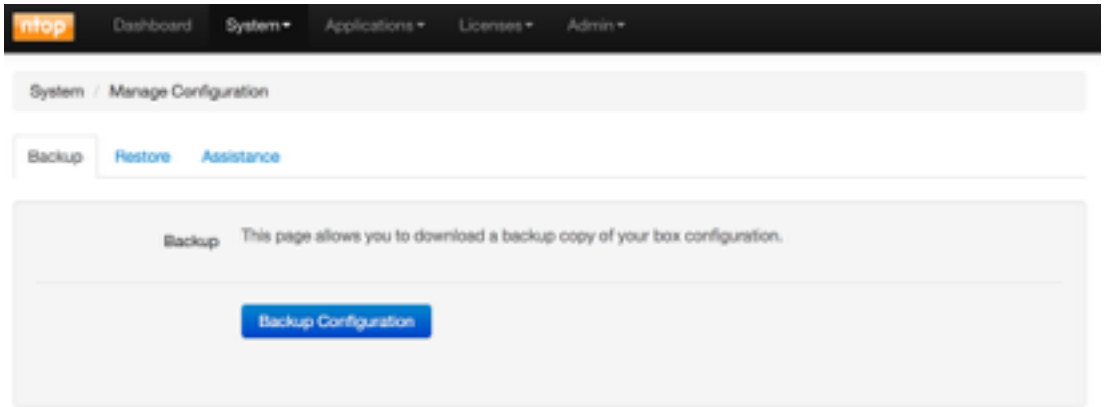
nBox is also integrated with Cloudshark, which is similar to Wireshark for the cloud. Configuring the Cloudshark section it is possible to analyse and share PCAPs with CloudShark appliances.



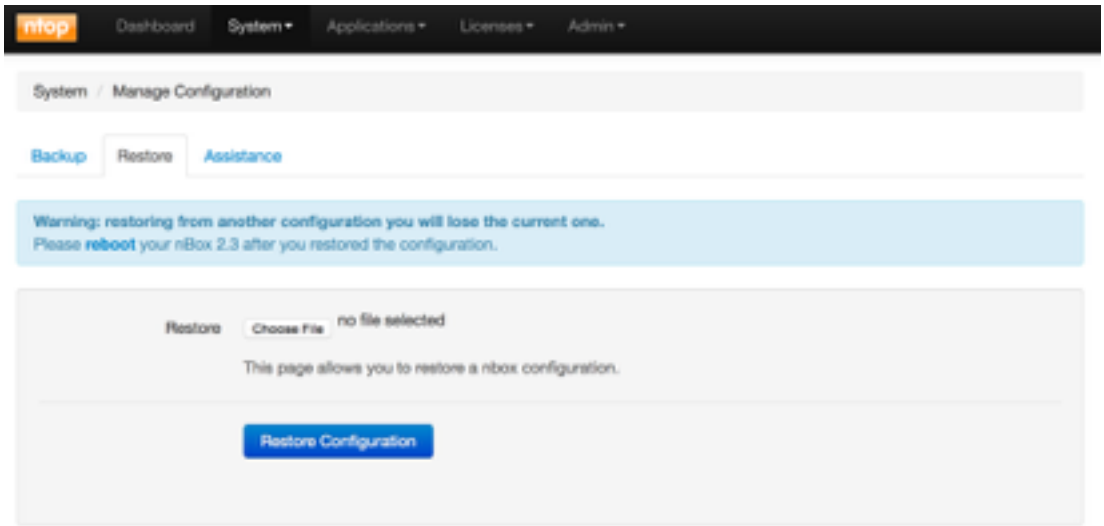
Manage Configuration

The Manage Configuration section is useful for:

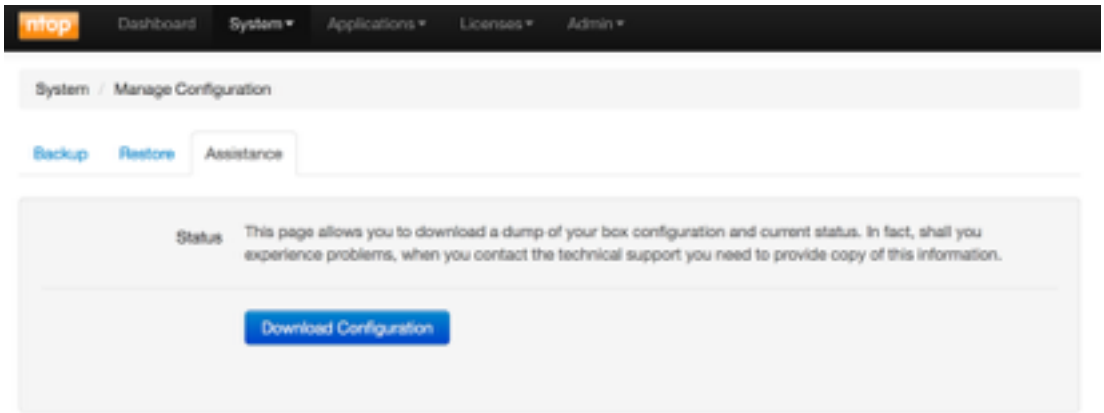
- Backing up the system configuration



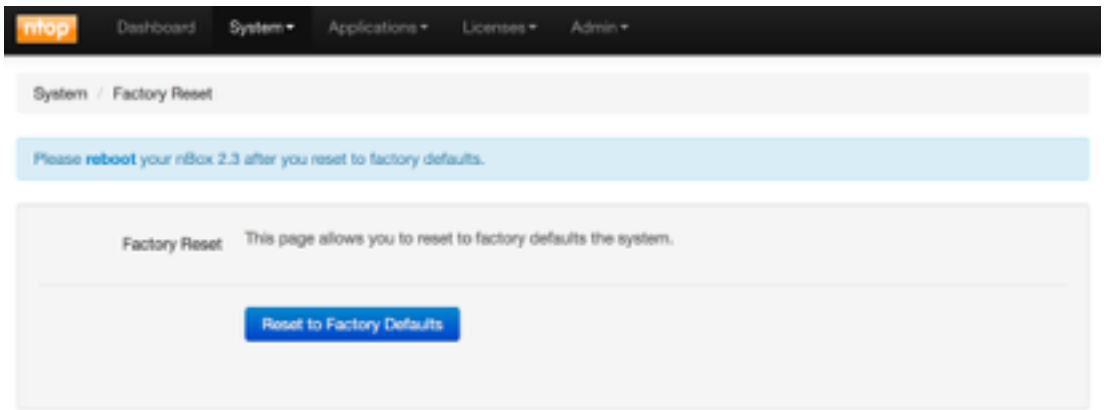
- Restoring a system configuration previously stored



- Creating a system snapshot to provide to the technical support in case assistance is needed. This way the support team has all the needed information to reproduce the issue and help the user as fast as possible.



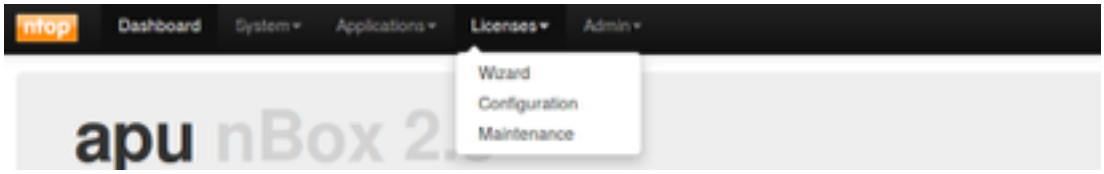
It is also possible to reset the system to factory defaults using the Factory Reset section. This is useful for instance in case the nBox doesn't work because of a wrong configuration. Please note this also cleans all the licenses, thus please backup them before resetting the system using the Manage Configuration section or manually using the Licenses Configuration section.



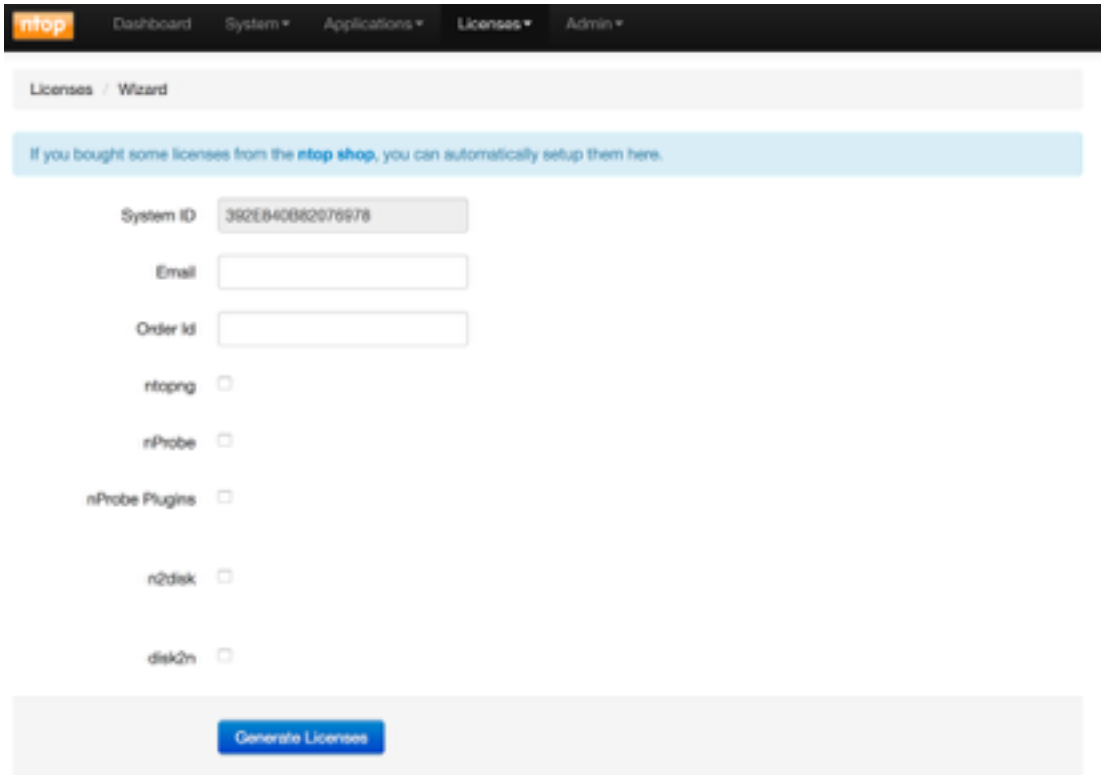
2.3 Licenses

nBox appliances are usually delivered with all the software installed and licensed, thus there is no need for the user to enable the software. If this is not the case, under the Licenses section, users can configure licenses for the applications.
Licensing the software allows the user to update the applications for 1 year since the first registration. After this period applications will continue to run but any further update cannot be installed.

The Licenses section contains three pages, a Wizard for automatically configure the system with all the needed licenses providing an order ID, a Configuration page where the user has to manually insert licenses for all the needed applications, and a Maintenance section where software maintenance expiration status is reported.

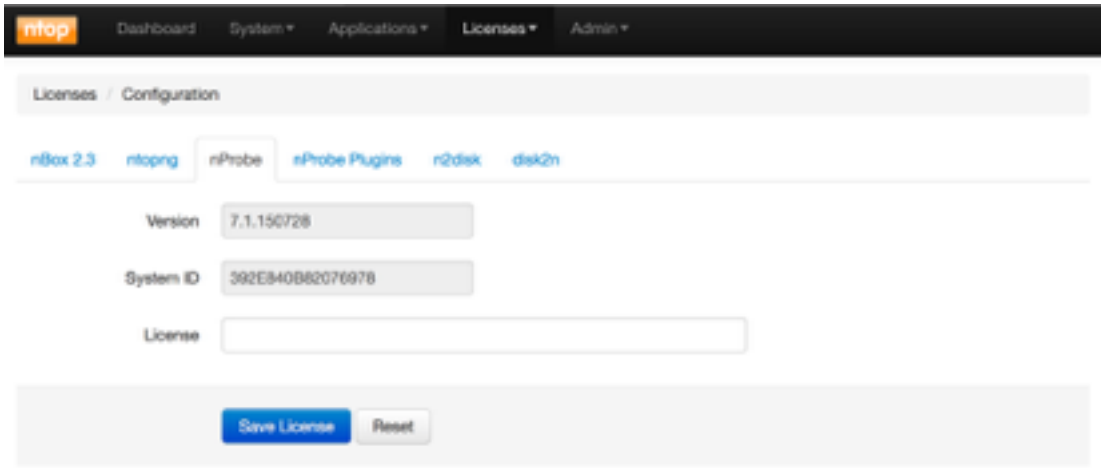


Using the Wizard page, after inserting email and order ID, selecting the needed application, and pressing the "Generate Licenses" button, the nBox automatically generates licenses. It is possible to retrieve those licenses in the Configuration page.

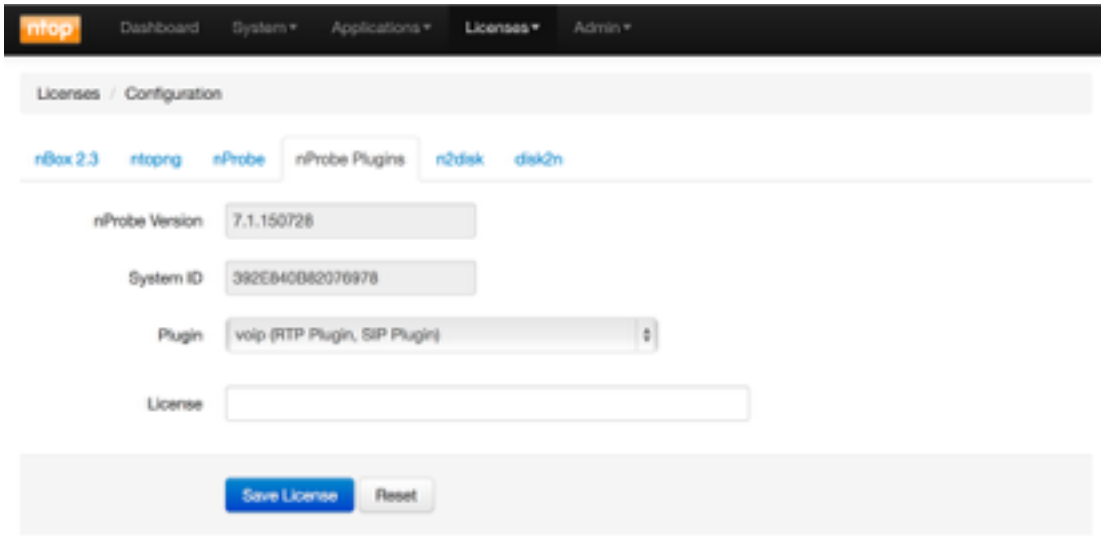


In the Configuration page is possible to retrieve or add licenses for the nBox components: nProbe, nProbe plugins, n2disk, ZC. Licenses are based on System ID (for nProbe, nProbe plugins, n2disk, disk2n) or MAC address (for ZC).

The first page in the Configuration page displays the System ID. On the other tabs, users can add their licenses as in the nProbe example below.
In the nProbe tab, the application version and the system ID are displayed. Users will find the license field already filled with their licenses if present, or it can be reinstalled if needed.



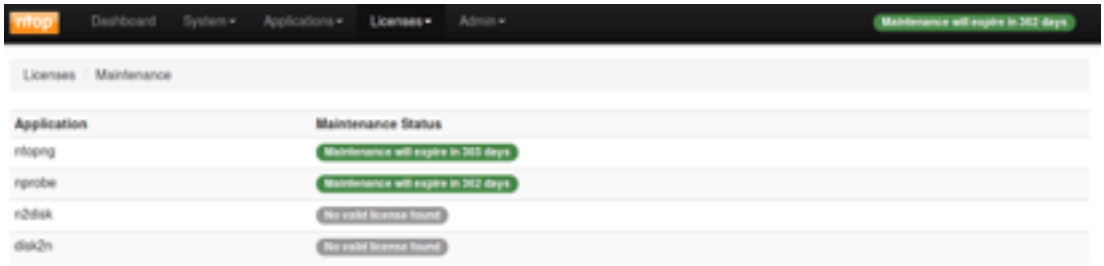
nProbe can be extended using nProbe plugins. They improve traffic decoding and storing features and are available for purchase on the ntop shop. Plugins come in single license (e.g. DNS plugin) or in bundle license (e.g. VoIP that contains both RTP and SIP plugins).



n2disk is licensed based on speed. This way the user can reduce costs acquiring only the license for the required capture speed. Different flavours are for 1 Gbit/s, 5 Gbit/s and 10 Gbit/s. Please note that a 10 Gbit/s license does not guarantee wire speed capture unless on top of adequate hardware.

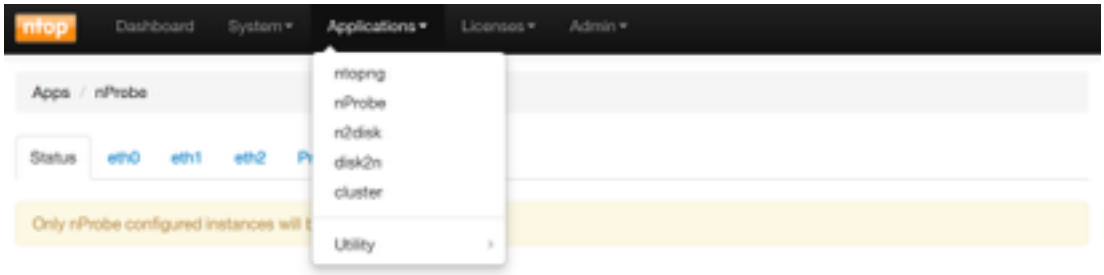
Unlike the applications, ZC drivers licensing model is on a per-MAC-address basis, hence each network interface that supports this kind of technology might be enabled using a different license.
In the same way as nProbe plugins, ZC licenses can be purchased upon user request and added to the nBox during its life cycle.
The ZC technology extends and increases the packet capture and forward-to-application speed, giving each captured packet available to user application without extra copies from and to the memory.

In the Maintenance page is reported the status of the software maintenance, showing the number of days left to expiration for each installed product.



2.4 Applications

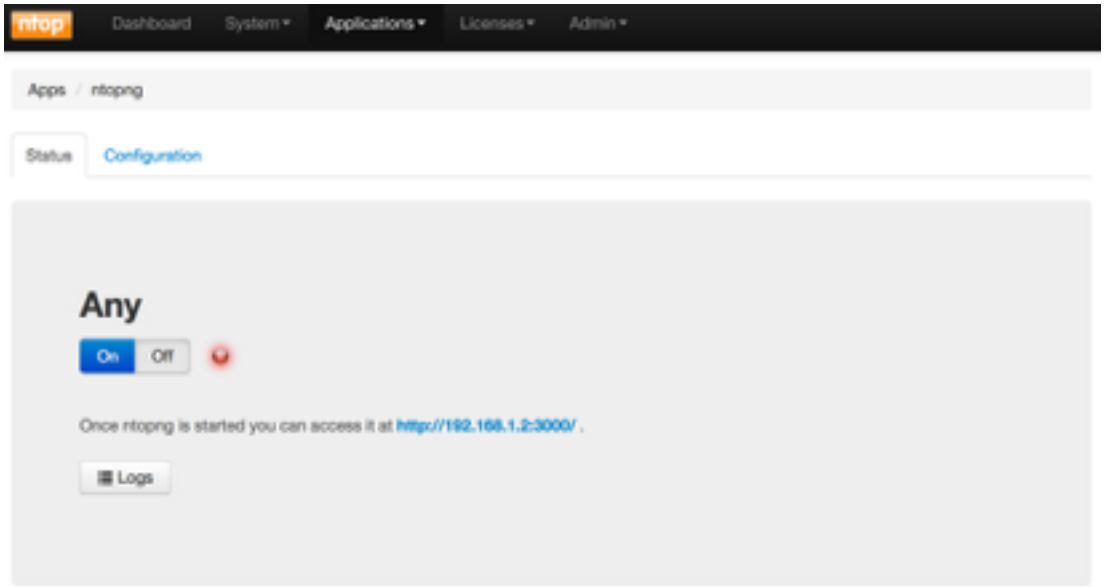
The Application menu allows the user to customise and control all the ntop applications installed and licensed.



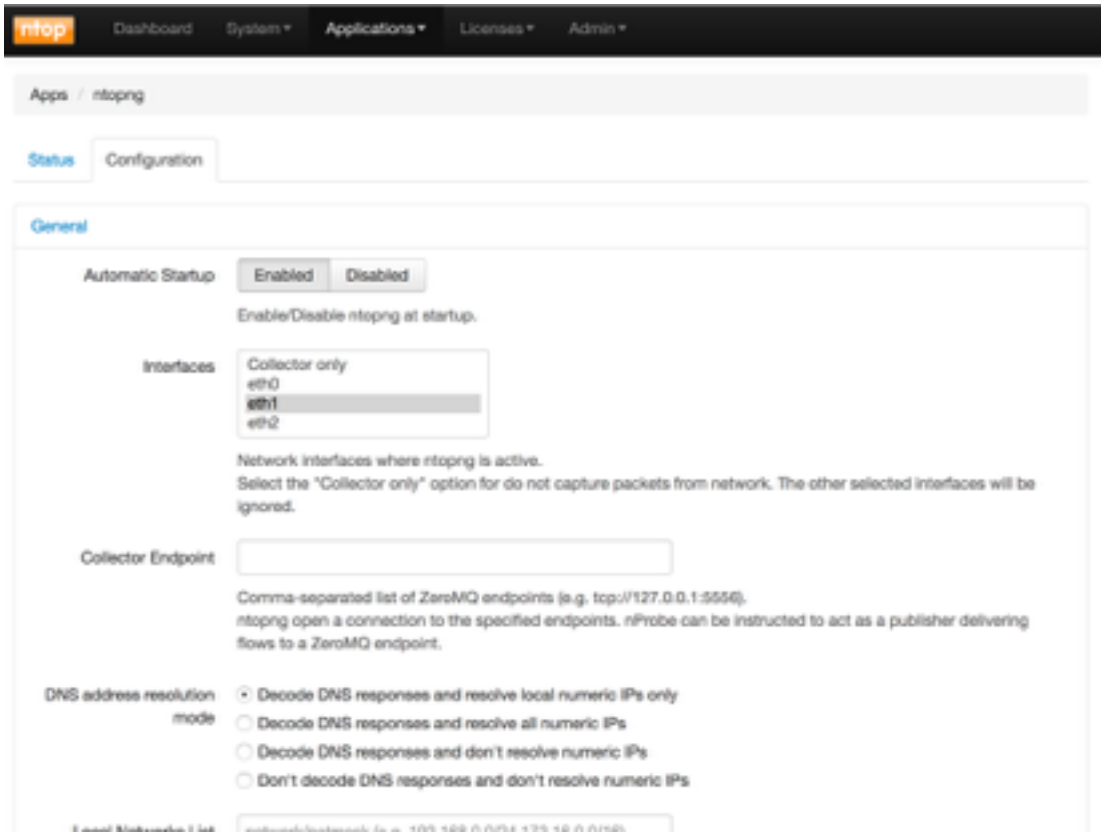
Applications include ntopng, nProbe, n2disk, disk2n. The cluster is also part of the applications and it is used to load balance traffic across application instances, or to send the same traffic to multiple application instances (or combinations of both). The Utility section contains pfsend, a simple traffic generator, and the nBox Activity Scheduler.

The ntopng menu can be used to configure and enable the ntopng application. The page is provided to the user in a tabbed form, where its first tab is the status page for the application, used to start and stop it, while through the configure tab it is possible to customise ntopng directly from the web interface.
A page with the same structure is available for all the applications.

A grey box with the interface name is displayed in the status tab for each enabled instance. The presence of the grey box means that at least an instance of the application is configured. A button On/Off is available to start and stop the instance.

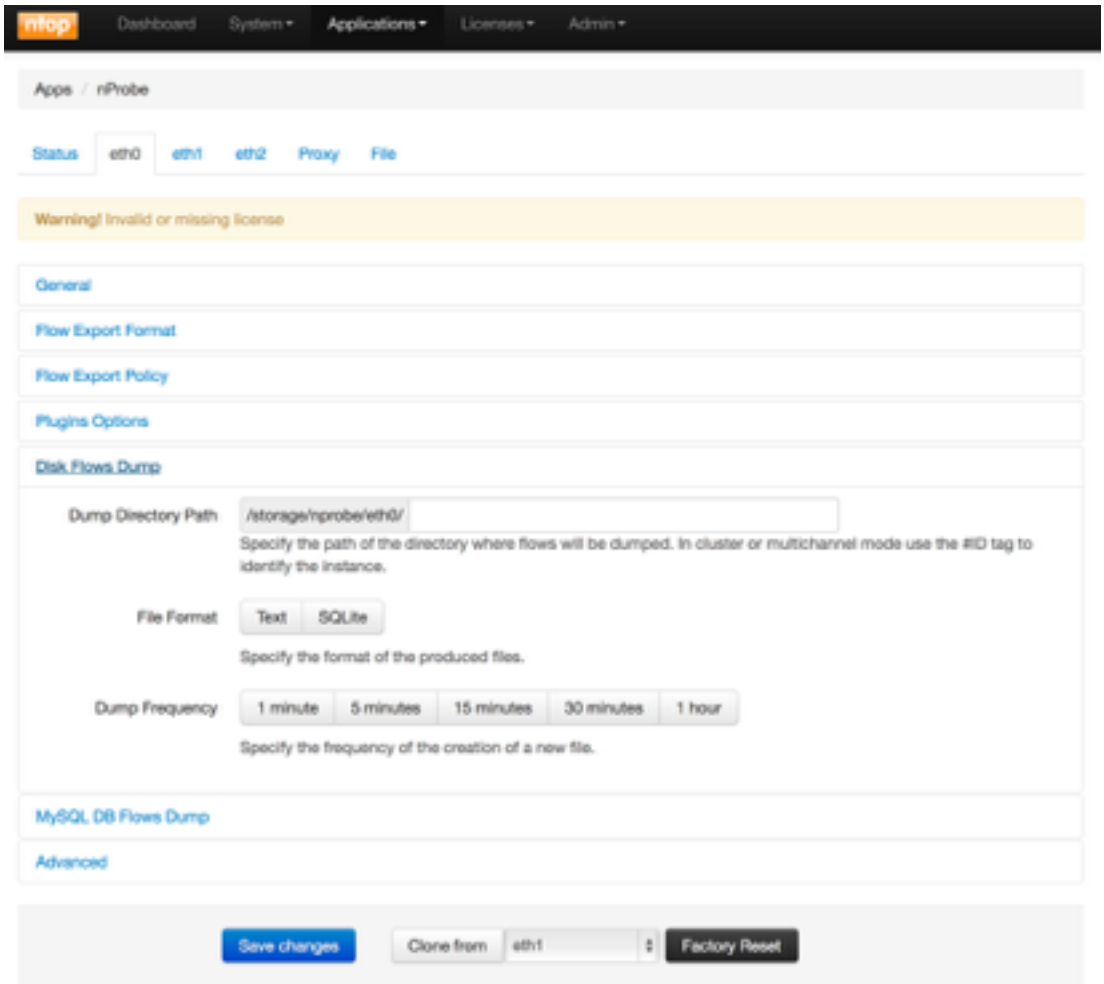


In the configuration tab, the user can select the automatic startup for ntopng, to automatically start upon reboot, and the interface where ntopng will listen for incoming packets. All the physical interfaces will be prompted to user, but also a "Collector only" can be chosen. This selection is normally used when ntopng is used as a Netflow collector, in this case ntopng does not need to capture packets directly from the network card.



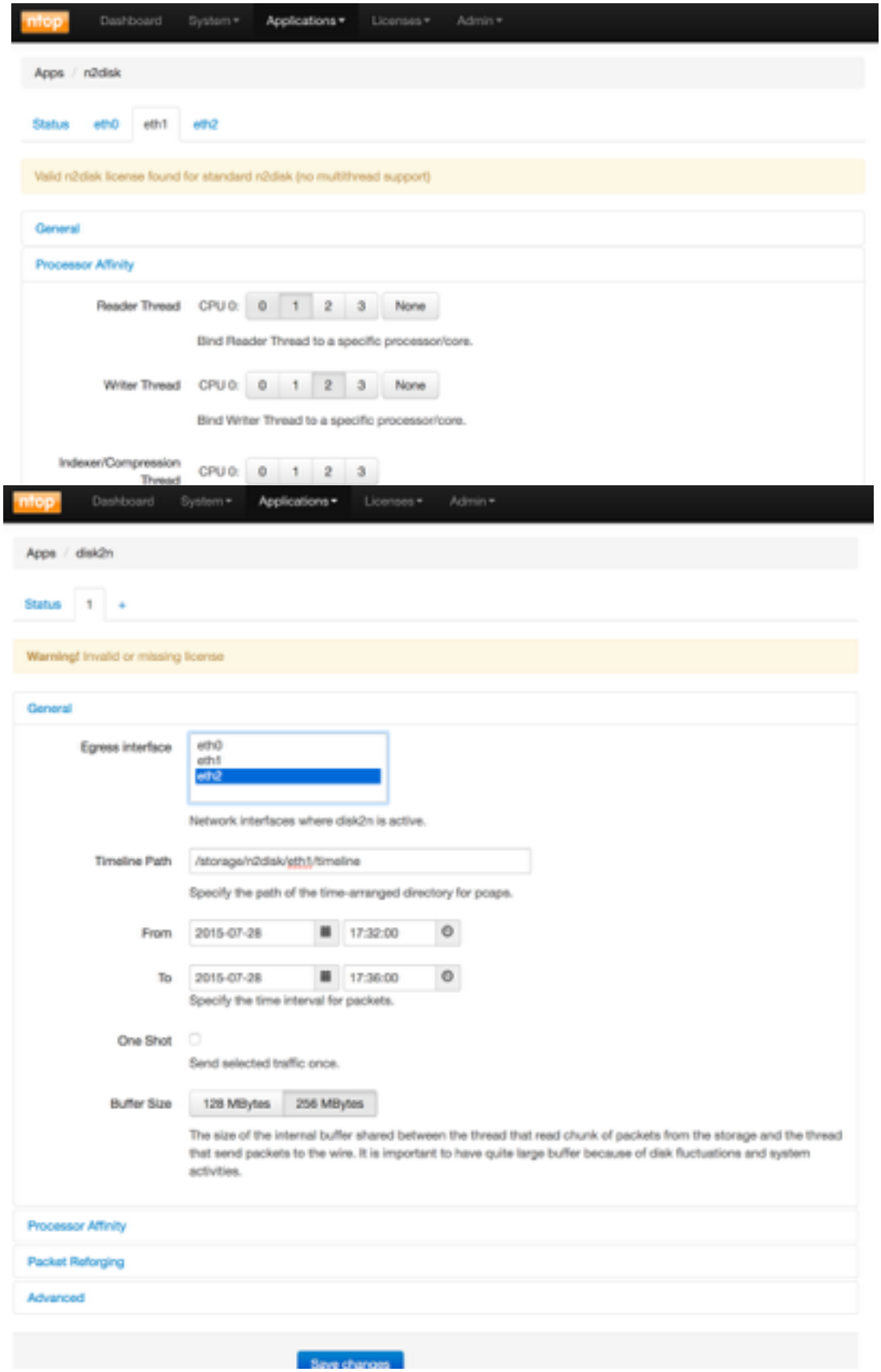
Many other settings are available through the configuration page, such as DNS resolution mode, local network subnets, etc. After configuring the ntopng instance, the "Save" button allows to store the configuration. Please note that is is not possible to change a configuration while the application instance is running.

The nProbe menu also contains several option that can be tweaked by the user. As in the ntopng menu, the nProbe configuration page is available in tabs. The first is the status tab and the following are configurations for each available network interface. The last one is for the Netflow proxy configuration.
Several sections permit the customisation of nProbe for example in terms of flow export type and policy, disk based flow dump or database based flow dump. Some sections are dedicated to the customisation of some plugins.

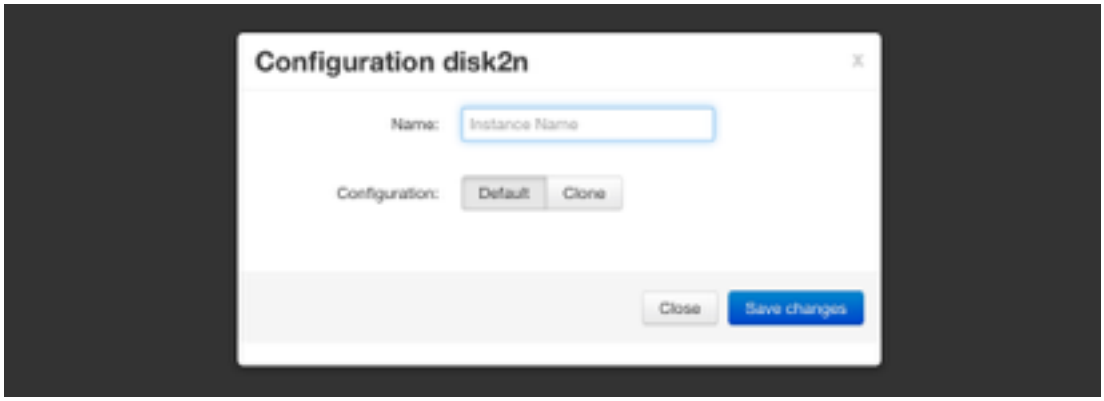


Use the "Save Changes" button on the bottom of the page to commit changes as in all other pages. nBox gives to the user the ability to easily clone configuration among all the available interfaces using the "Clone from" button and selecting the configuration source.
Please refer to the nProbe user manual for further informations about the nProbe configuration.

The n2disk section can be used to customise the configuration of n2disk, a network traffic recording applicaiton. It is possible for instance to set buffer and PCAP file size, snapshot length, CPU affinity, and so on. The figure below displays all the configurable sections.



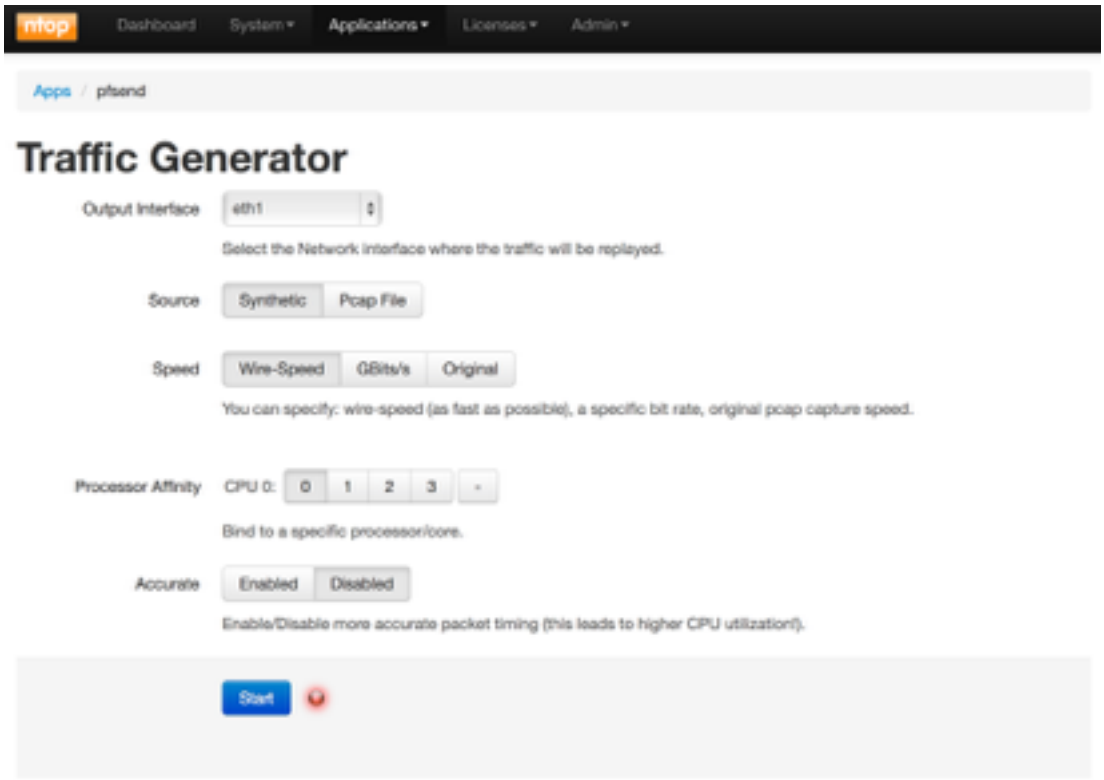
The disk2n section can be used to customise the configuration of the traffic replay application, used to reproduce traffic recorded with n2disk. In this section, user can show the disk2n instance configured or create a new one using the "+" tab.



In the instance configuration tab, the user can tweak disk2n parameters such as egress interfaces, timeline path, source traffic time interval, buffer size, CPU affinity. The figure below displays the configurable sections.

The traffic generator, based on pfsend, under the Utility sub-menu, is a tool used to inject packets into the network using the selected interface. It is able either to forge synthetic

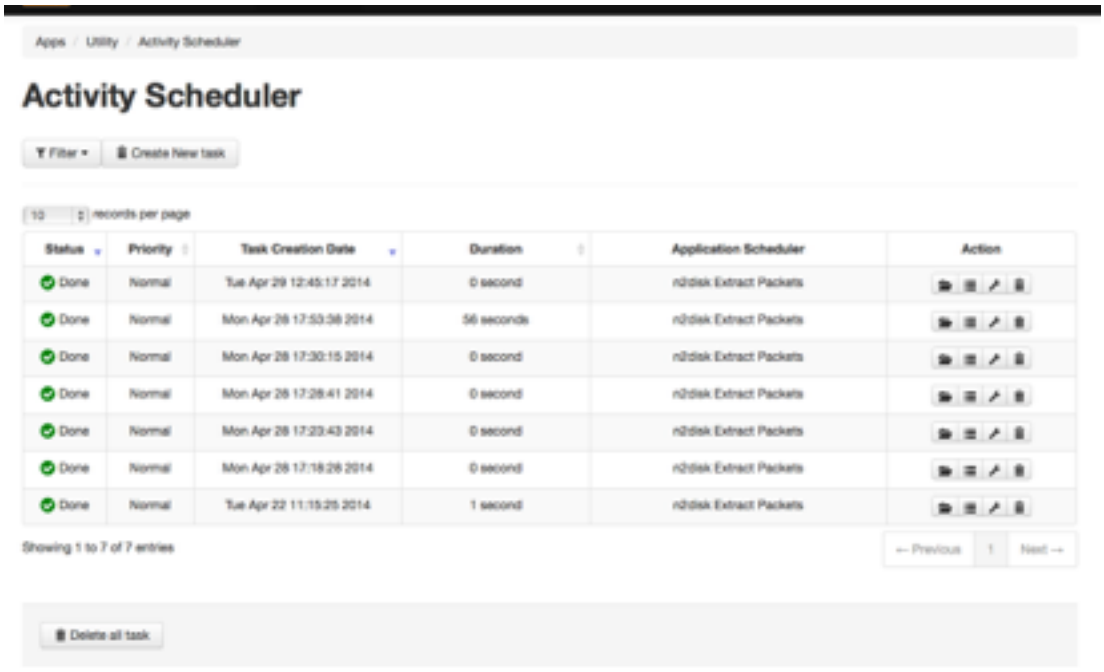
packets or send small PCAP files. Emitted packets are sent with the original speed or they



can be sent at wire speed or even at a selected bit rate.

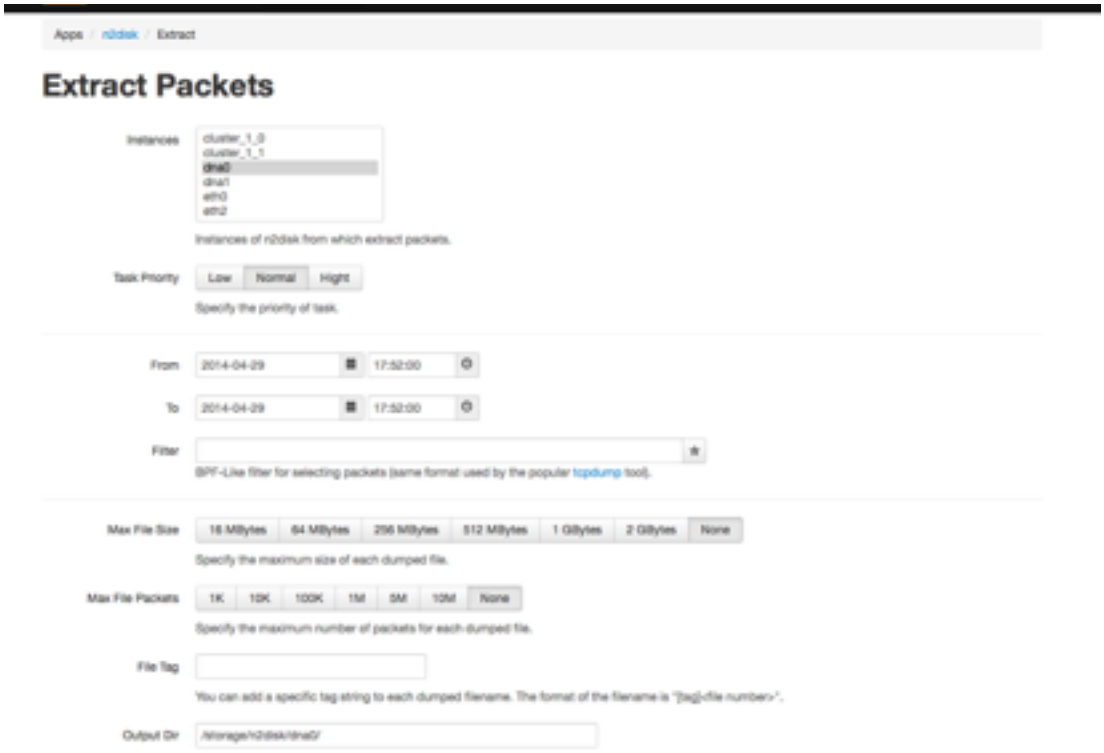
A green led on the bottom of the page shows that the instance is running.

The Activity Scheduler, under the Utility sub-menu, is a tool used to schedule tasks such as traffic extractions from the n2disk storage.



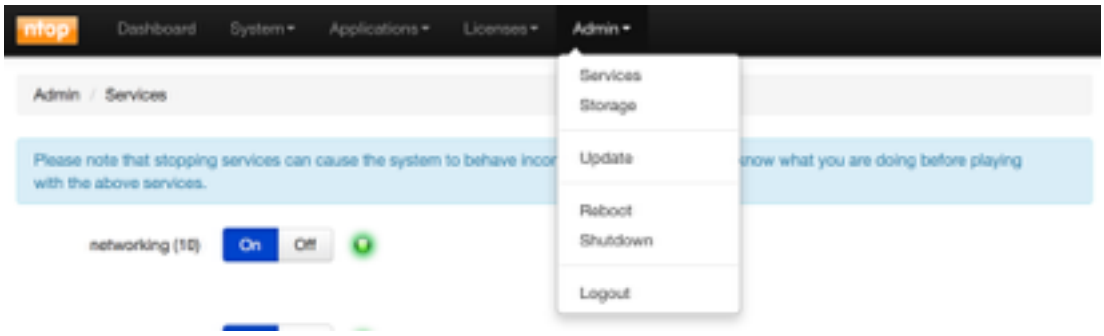
In this section, the user can see all the scheduled tasks, retrieve the log, the PCAP files extracted, the task configuration, or delete a task and the corresponding files.

The user can create a new extraction task from an existing n2disk instance using the Extract button in the n2disk status page.
Interfaces, task priority, time interval, bpf filter, output directory are some of the options available.

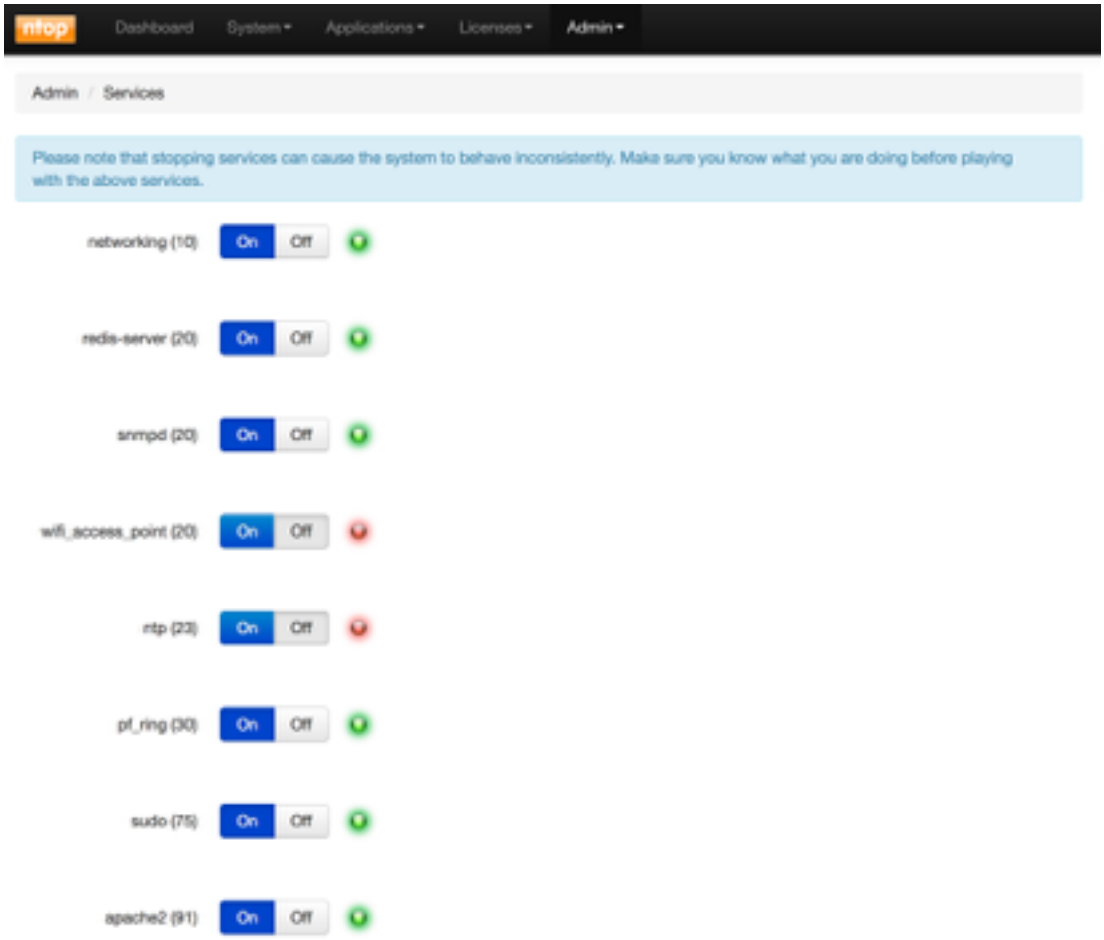


2.5 Admin

The admin section allows the user to manage running services, storages, updates and shutdown or reboot the machine.



In the Services page system services can be started, stopped or restarted simply toggling the On/Off button.



The system can be updated to latest available packages using the Update section, or in case of maintenance or if necessary, it can be remotely powered off or rebooted using the specific Reboot and Shutdown menus.

The ntop software nBox is in continuous development. New feature and bug fixes are out every day. We suggest all the user to perform regular updates to the box.

If you have an old nBox which is missing the Update button and want to update it, connect to the system via SSH (default ip address: 192.168.160.10 user: root password: nBox) and run the following commands:

apt-get update
apt-get upgrade

If you are using CentOS instead of Ubuntu, please replace apt-get with yum. Please note you need root privileges to do this. After updating your nBox, you can find the "Update" button in the Admin menu for future updates.

In case of issues please file a bug on our ticketing system to keep a trace of the experienced problems.

Follow us on http://www.ntop.org/