InvizBox User Guide

Table of contents

Introduction

InvizBox is a small, low power device that helps provide an easy-to-use method of protecting your privacy on the Internet. Just plug the InvizBox into your existing router / modem. A new "InvizBox" wifi hotspot will appear. Connect to the new hotspot and follow the one time configuration setup and you're ready to go! All devices that you connect to the InvizBox wifi will route their traffic over the Tor Privacy Network.

We all have a right to privacy, a right to protect our personal information, data, location and internet behavior. You may think you have nothing to “hide”, or you aren’t doing anything “wrong” that would require investigation by third parties but neither do we. That doesn’t mean that we have to leave ourselves open to tracking and profiling by people, governments, companies, hackers etc. who we neither know or trust. Invizbox provides an easy solution to give you back control over who & what you choose to disclose your personal information to.

Hardware

The InvizBox is a small router based on the MediaTek MT7620N Wi-Fi System-On-Chips (WiSOC). Specifications are as follows :

- CPU architecture: MIPS 24KEc (RT6352)
- 802.11n 2T/2R (2x2:2) 2.4 GHz 300Mbps MAC/BB/PA/RF
- Clocked @ 580 MHz
- DDR RAM 64MB
- Supports Wifi b/g/n
- MAC address filtering
- Support for WPA / WPA2, WPA-PSK / WPA2-PSK.
- Support System: Windows / Mac / Linux
- Colours - White.
- Power via micro USB (cable included).
- 16MB flash

Dimensions: 65mm X 45mm X 22mm

Quick Setup

In this section we will show you how to quickly setup the InvizBox in 6 easy steps.

Six Easy Steps

1. Connect the supplied ethernet cable to the WAN port on the InvizBox.
2. Connect the other end of the ethernet cable to an ethernet port on the router given by your internet service provider.
3. Connect the USB cable to a suitable power source.(Note: Many routers now have suitable USB ports which can be used instead of a separate power supply)
4. Connect the other end of the USB cable to the InvizBox.
5. Wait about 30 seconds for first boot. If you are using wifi, look for an "InvizBox" wifi access point.
6. Select the InvizBox wifi access point and enter the password that is printed on the bottom of your InvizBox.

Please see QuickStart Manual for more detail.

Overview

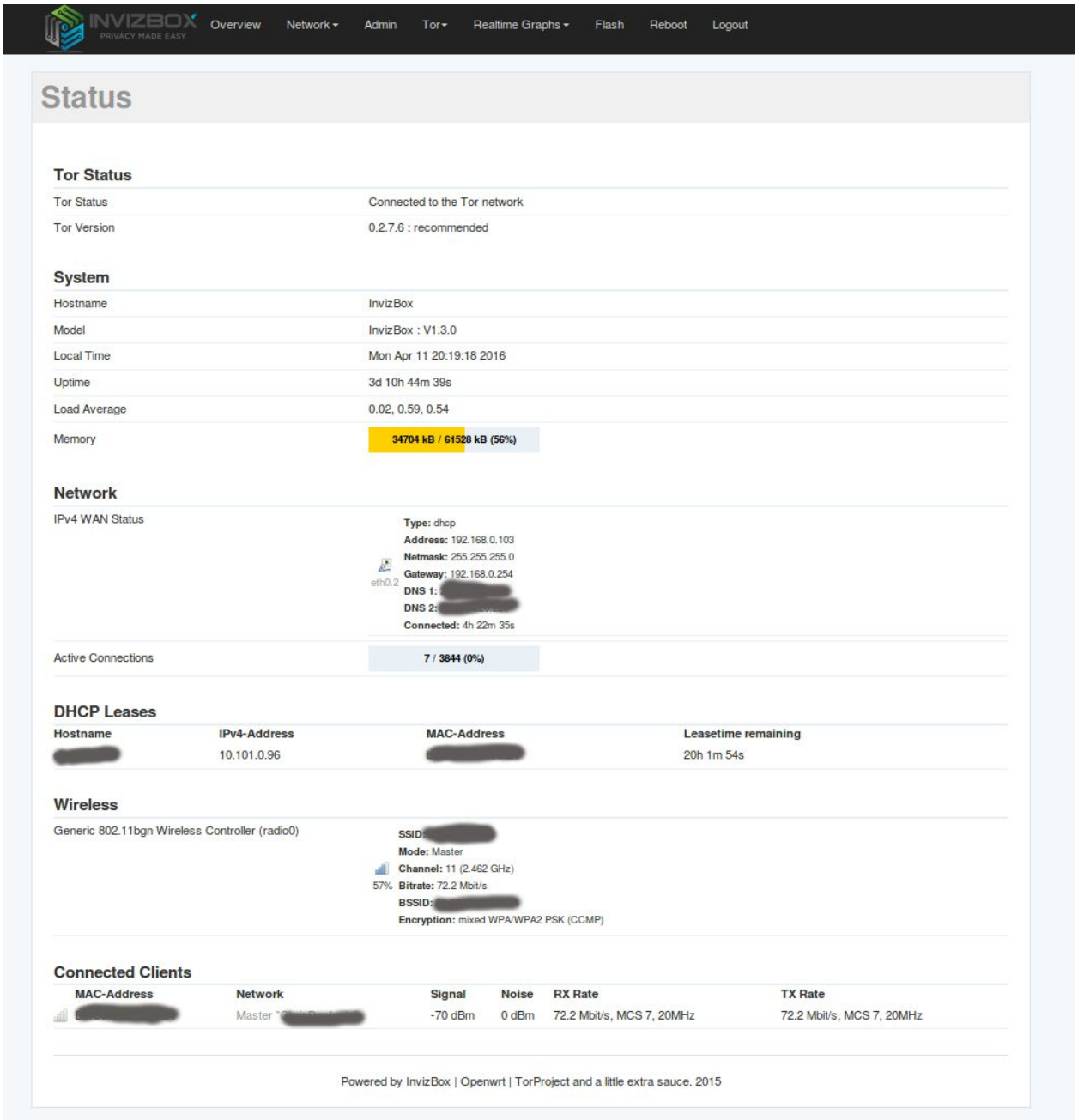
To access any of the admin pages outlined point your browser to :
http://10.101.0.1

General Status

The Overview page gives you a brief overview of a number of things:

- Tor Status
- Time, Date and other system information
- Network Overview
- DHCP Status
- Connected Clients

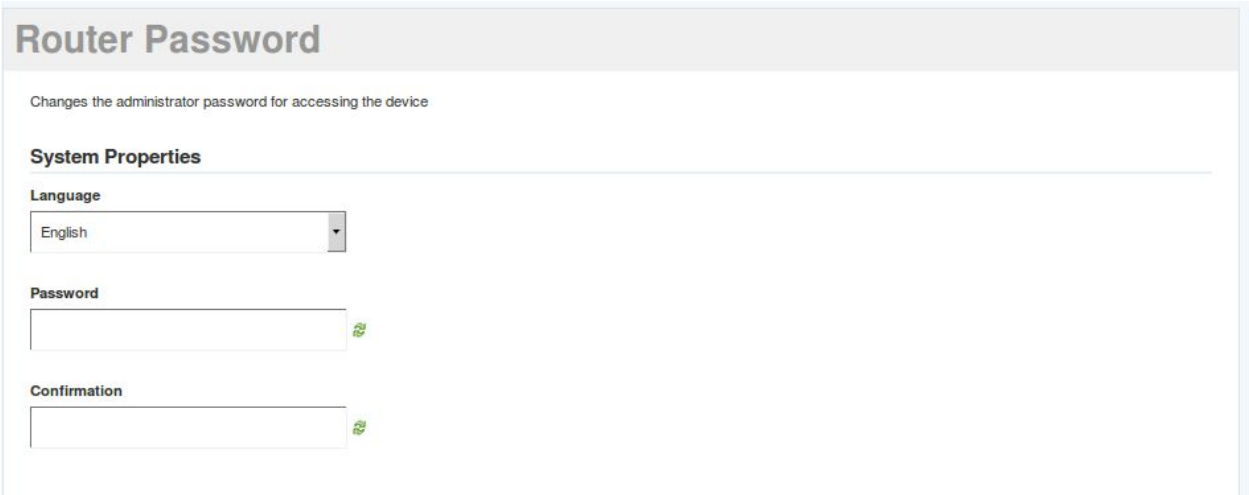
Below is a screenshot of how it will look



Admin

Password & Language

This section allows you to change the password for UI and SSH, along with the language of the UI.

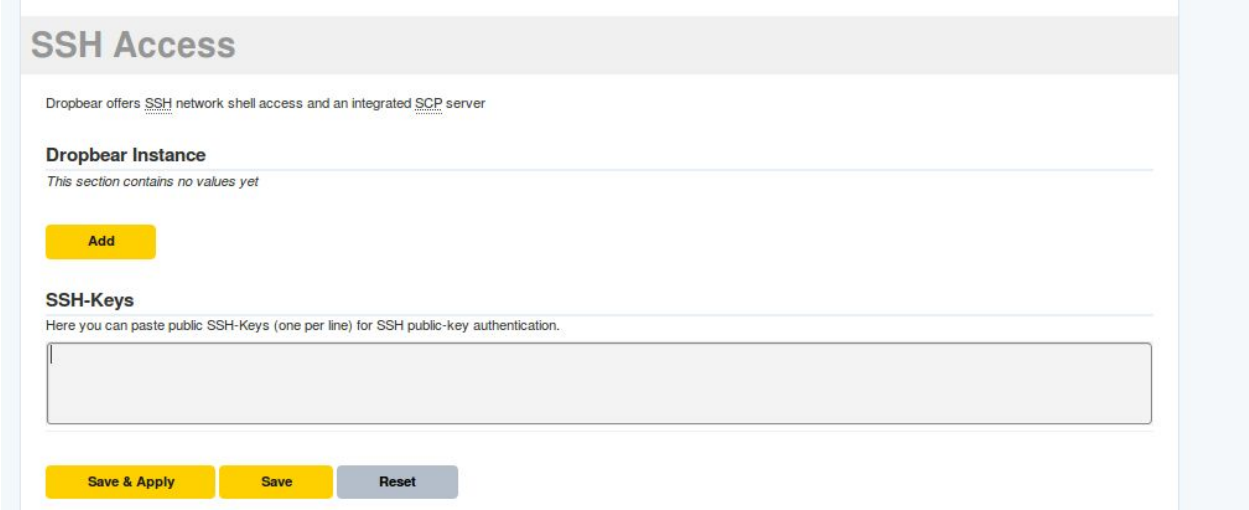


To change Password just enter in the new password into both Boxes and click “Save & Apply” at the bottom of the screen.

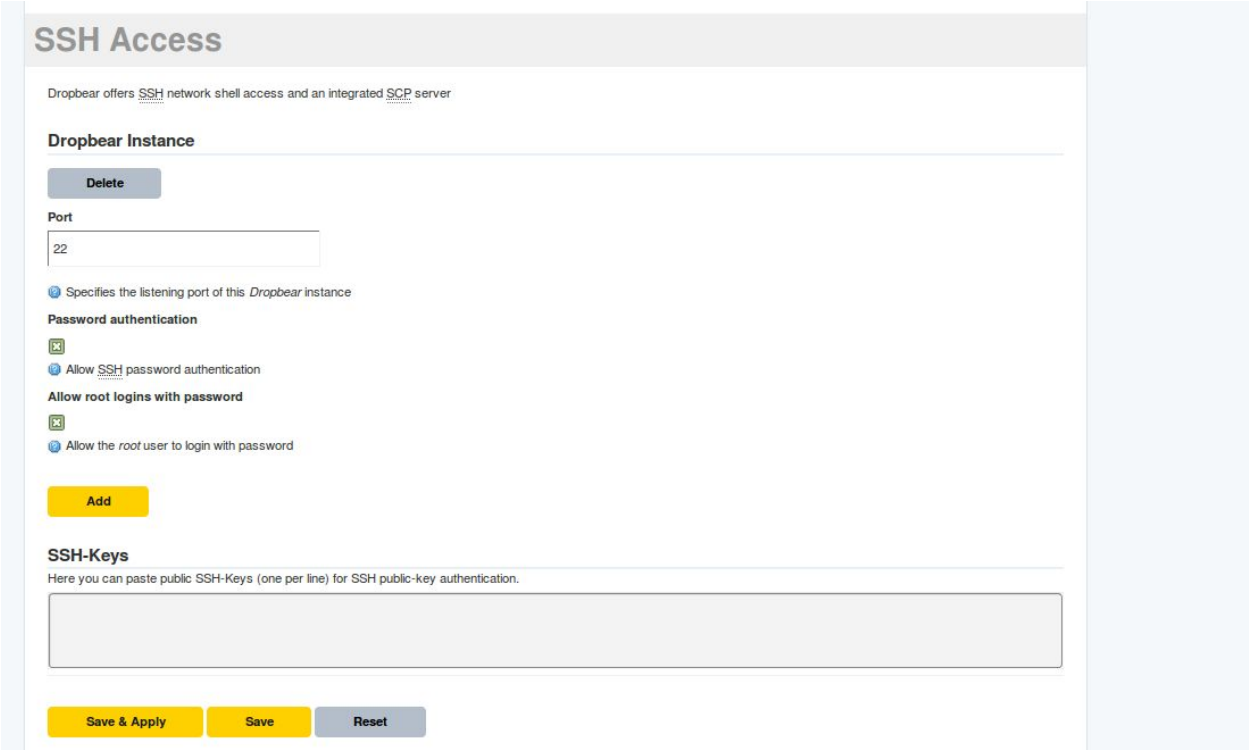
To Change language, Select the language from the dropdown and click “Save & Apply” at the bottom of the screen.

DropBear SSH

This section describes how to setup SSH access to the InvizBox. Out of the box, SSH is disabled.



To enable SSH you have to click “Add”. Once that is done to can configure the options as seen below.

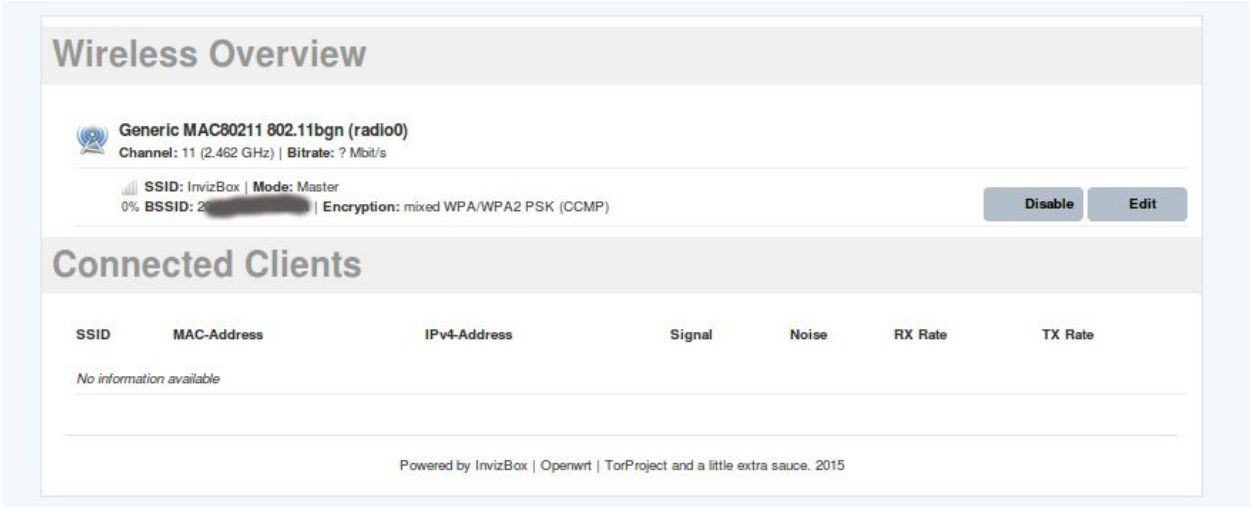


Here you can configure the port and other options displayed. You can also add SSH-Keys (one per line) into the appropriate section. Once you change any of these click the "**Save & Apply"** button at the bottom of the screen.

Network

Wifi

The WIFI section allows you to go deeper and configure the wifi access point to your own setup. Ideally it is only recommended to change the wifi **ESSID,** access point password and channel.



In the Wireless Overview page you can see the general status of the Wifi connections and connected clients. You can also disable and edit the wifi from this page.

Disable: Clicking this button will stop the Wifi access point. Tor and LAN will continue to work normally. This is good for if all you want is LAN and want to stop wifi from eating those precious air waves.

Edit: This bring you to a more detailed section which allow more precise configuration of the Wifi access point.

Customizing Wifi

On the Wireless Overview select **Edit**. The following page will appear

Wireless Network: Master "InvizBox" (wlan0)

The *Device Configuration* section covers physical settings of the radio hardware such as channel, transmit power or antenna selection which are shared among all defined wireless networks (if the radio hardware is multi-SSID capable). Per network settings like encryption or operation mode are grouped in the *Interface Configuration*.

Device Configuration

General Setup | Advanced Settings

Status

Mode: Master | **SSID:** InvizBox
BSSID: 20[redacted] | **Encryption:** mixed WPA/WPA2 PSK (CCMP)
0% **Channel:** 11 (2.462 GHz) | **Tx-Power:** 20 dBm
Signal: 0 dBm | **Noise:** 0 dBm
Bitrate: 0.0 Mbit/s | **Country:** 00

Wireless network is enabled

Disable

Channel

11 (2.462 GHz)

Transmit Power

20 dBm (100 mW)

dBm

Interface Configuration

General Setup | Wireless Security | MAC-Filter

ESSID

InvizBox

Mode

Access Point

Network

- [x] **lan:**
- [ ] **tor:**
- [ ] **wan:**
- [ ] ***create:***

Choose the network(s) you want to attach to this wireless interface or fill out the *create* field to define a new network.

Hide ESSID

- [ ]

WMM Mode

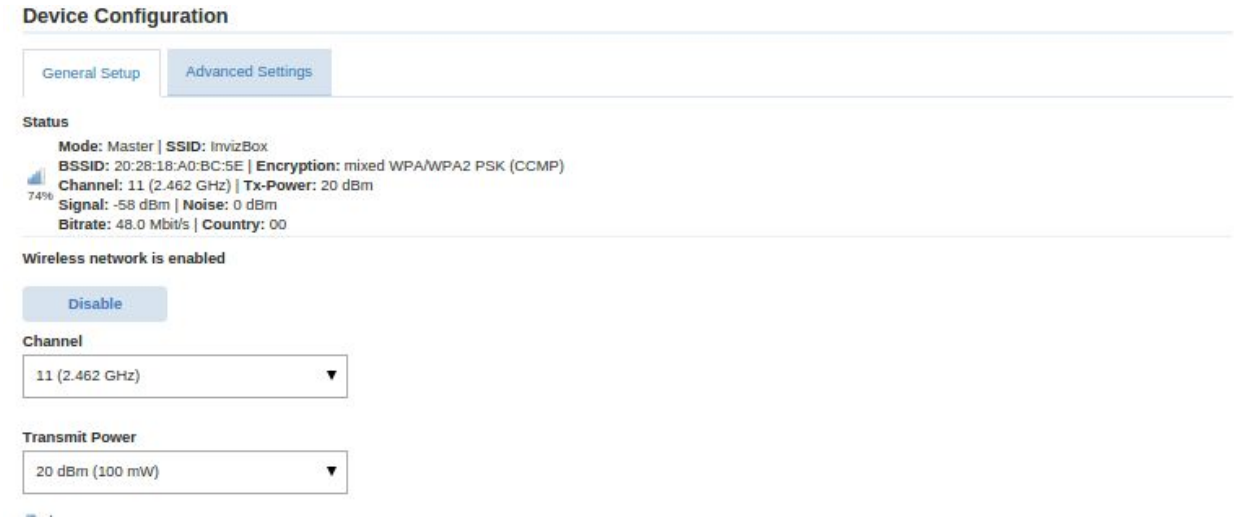
- [x]

Save & Apply | **Save** | **Reset**

Device Configuration

General Setup

In this section you can see the status. You can also change the Channel and Transmission Power. Once you change any of these click the "**Save & Apply"** button on the bottom of the screen

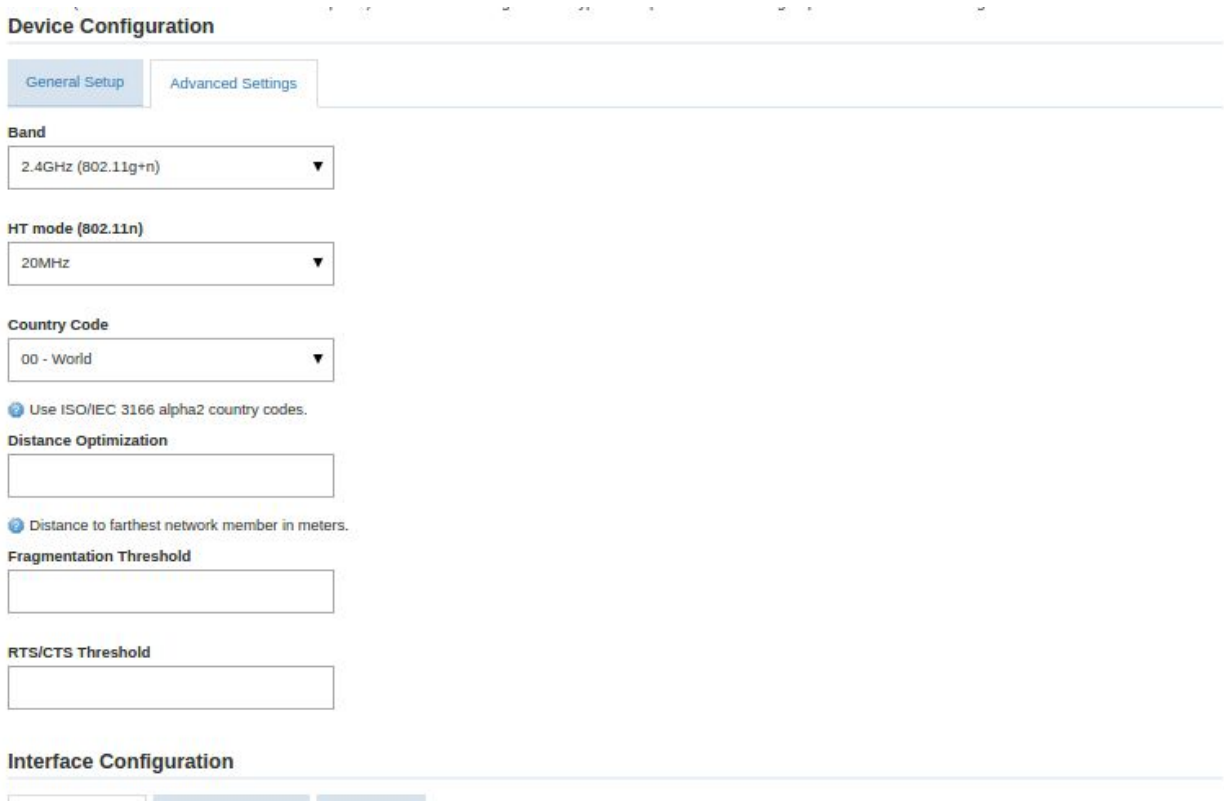


Advanced Settings

In this section you can edit the following :

- Band
- HT mode (802.11n)
- Country Code
- Distance Optimization
- Fragmentation Threshold
- RTS/CTS Threshold

Once you change any of these click the "**Save & Apply"** button on the bottom of the screen



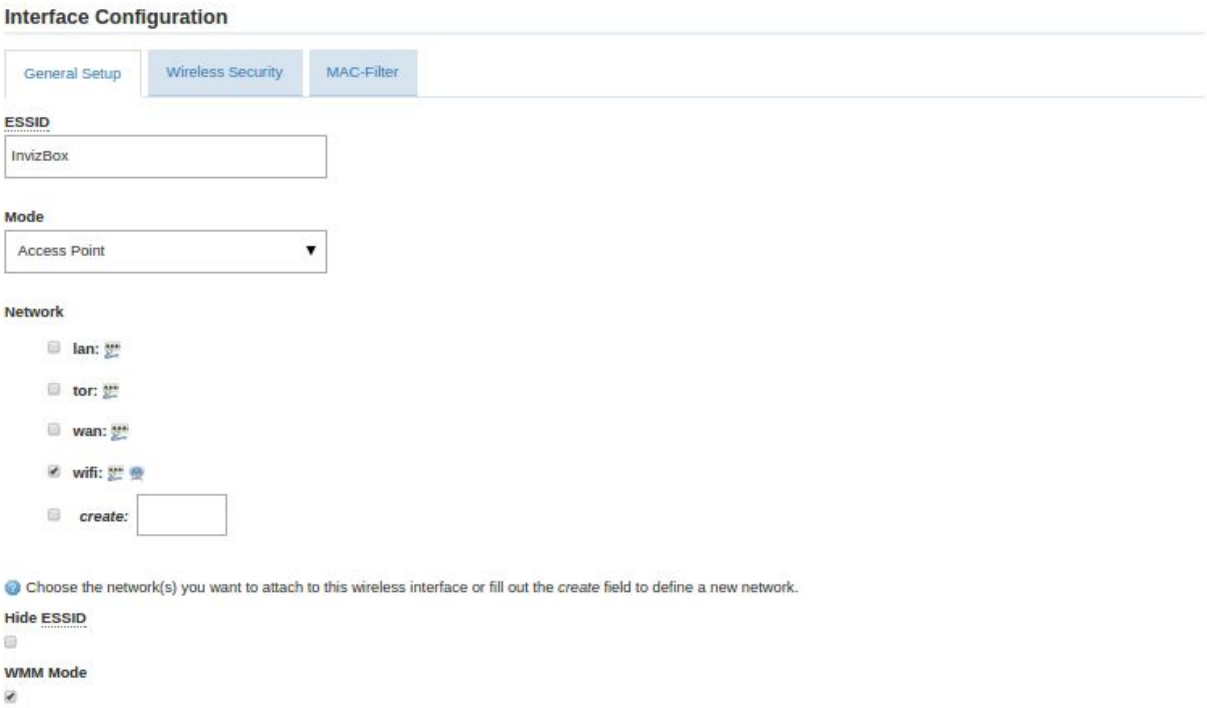
Interface Configuration

General Setup

In this section you can edit the following :

- ESSID
- Mode
- Network
  - lan: VLAN Interface: "eth0.1"
  - tor: VLAN Interface: "eth0.3"
  - wan: VLAN Interface: "eth0.2"
  - wifi: VLAN Interface: "eth0.4" Wireless Network: Master "InvizBox"
- Hide ESSID
- WMM Mode

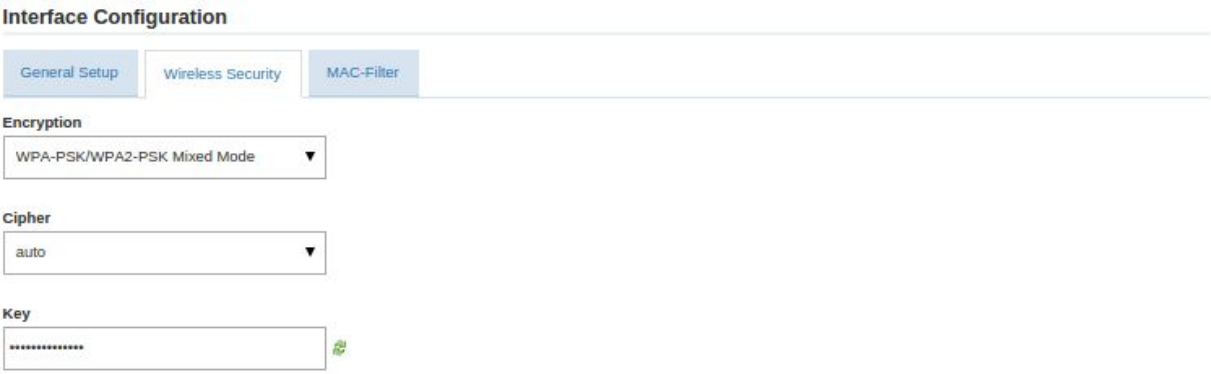
It is advised only to change the **ESSID.** Once you change any of these click the "**Save & Apply"** button on the bottom of the screen**.**



Wireless Security

In this section you can edit the following :

- Encryption
- Cipher
- Key

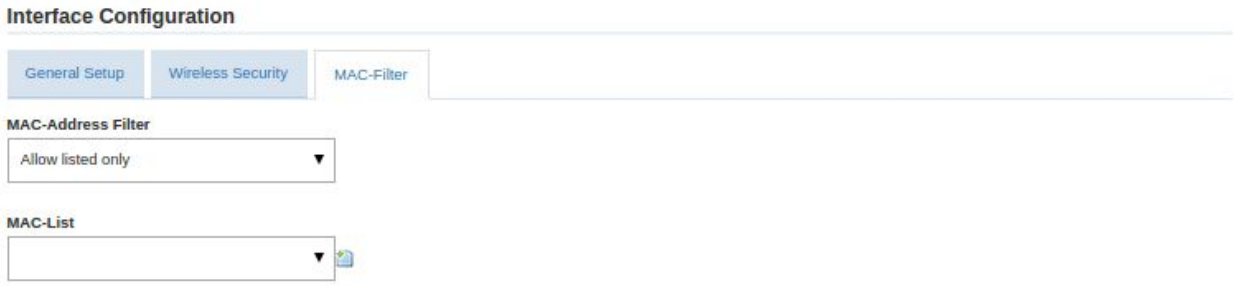


Once you change any of these click the “Save & Apply” button on the bottom of the screen

Mac-Filter

In this section you can setup MAC based filter for wireless access point. Select the options you wish from

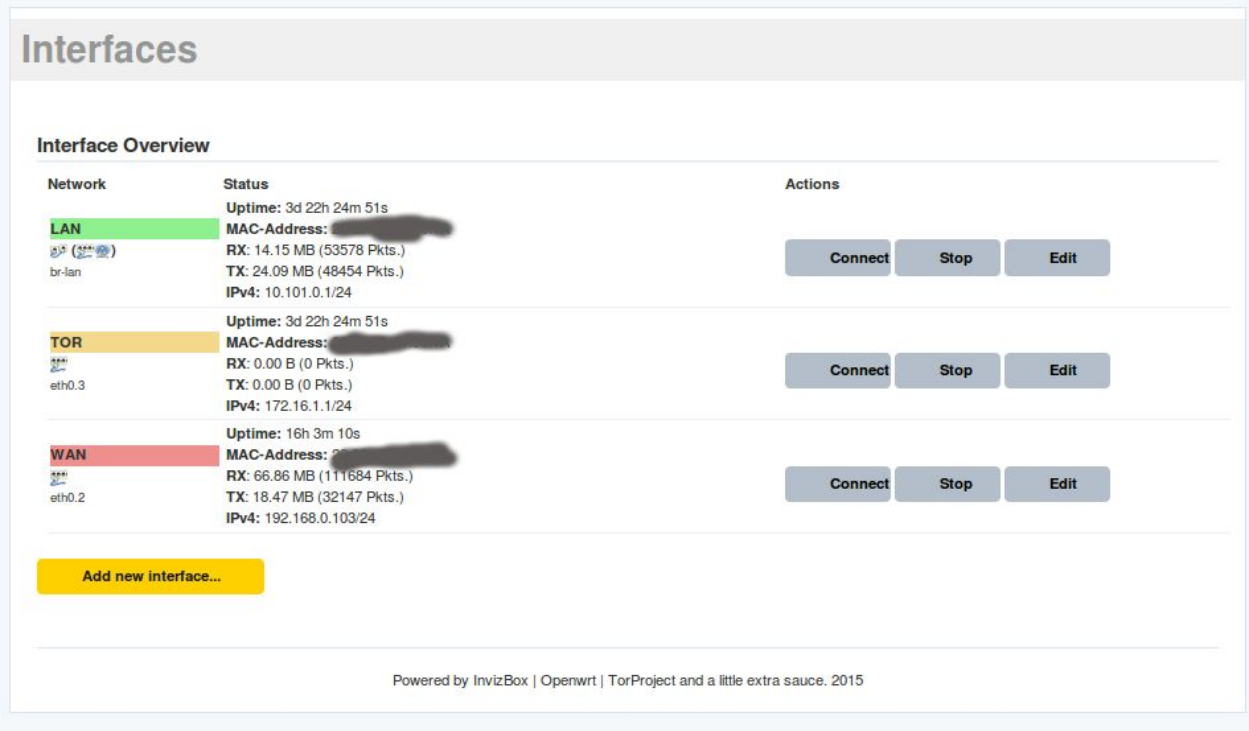
- None
- Allow Only Listed
- Allow All Except Listed



In the dropdown “MAC-List” select the MAC that you want allowed or denied. Once you change any of these click the “**Save & Apply”** button on the bottom of the screen

Network

The Network section allows you to go deeper and configure the wifi access point to your own setup. Ideally it is only recommended to change the wifi **ESSID** and access point password.



It is advised not to edit any of these setting in this section. Doing so can break

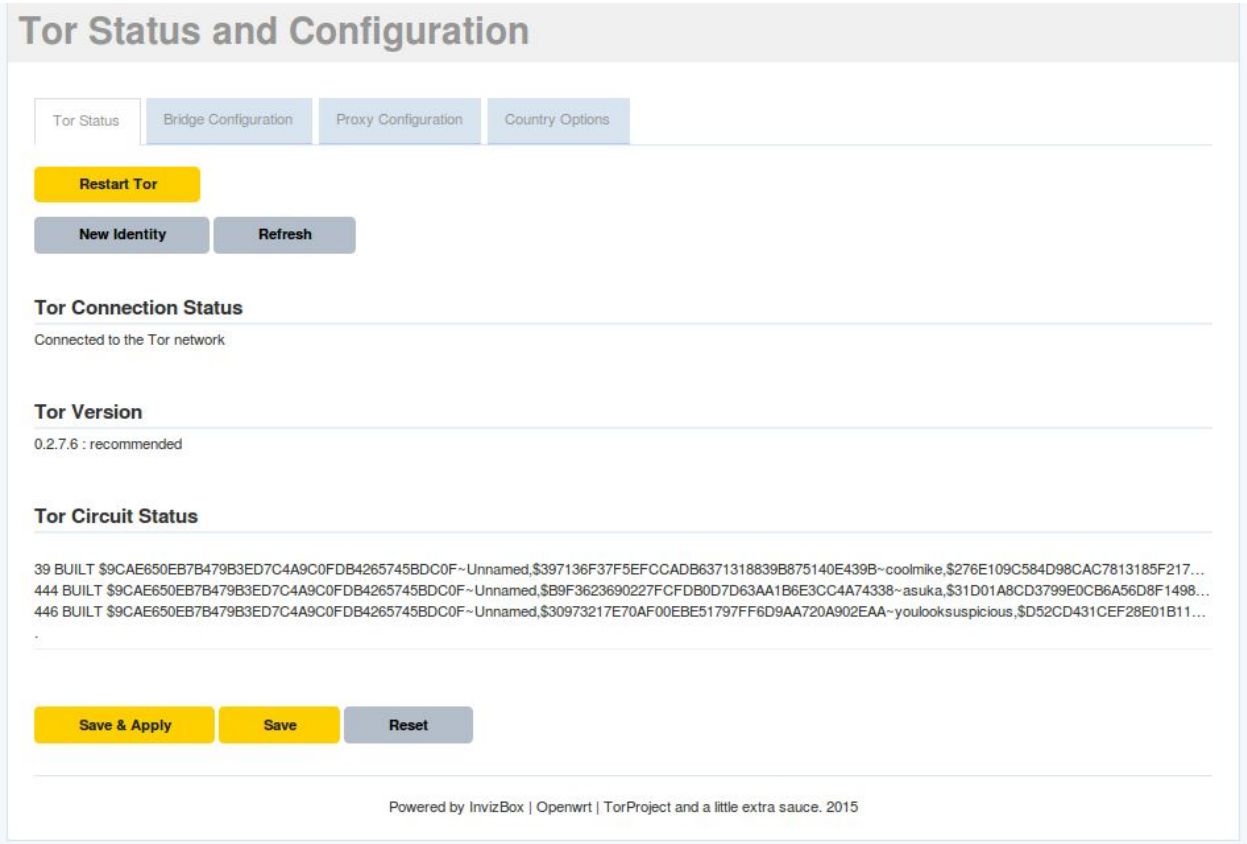
functionality of your InvizBox and you may need to do a hard reset.

Tor

In this section you can Restart Tor, Configure Proxy and Bridges, Select Exit Nodes and Advanced Config. It also shows you a general running status of Tor.

Tor Status

This page shows if the InvizBox is connected to the Tor network. It also shows the Tor version, current bandwidth and Tor circuit status.



If Tor is not connected click the “Restart Tor” button and wait approximately 30 seconds then “Refresh”. Tor should connect. If not wait another 30 seconds and hit “Refresh” again. If you still cannot connect to the Tor network, you may need to configure a bridge or proxy (see below).

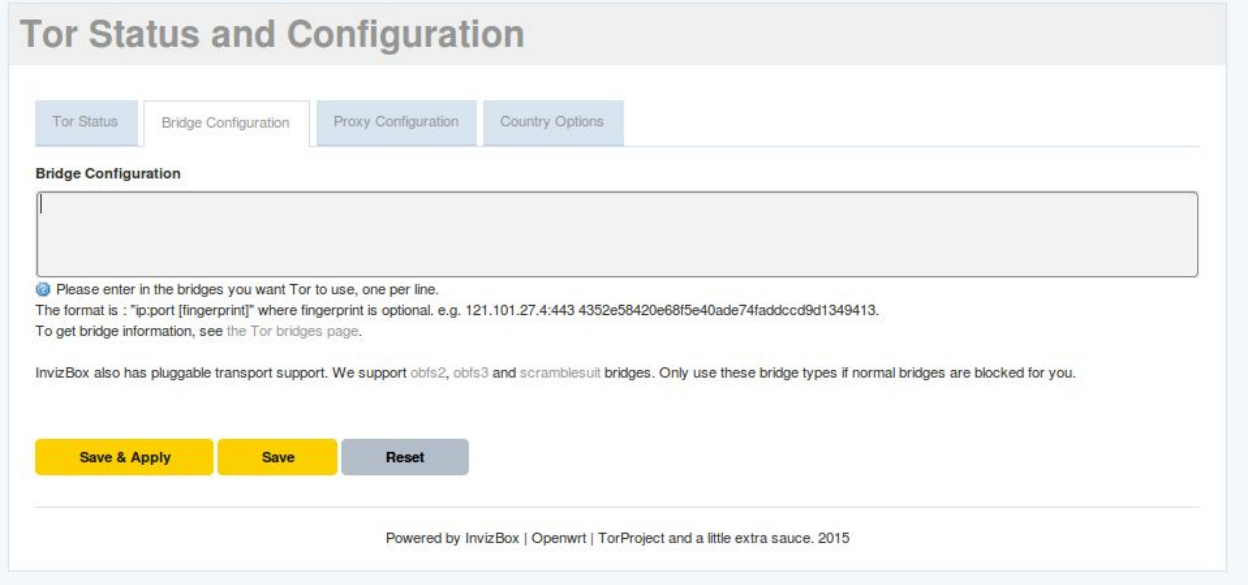
Bridge Configuration

Bridges are Tor relays that help you circumvent censorship. Bridge relays (or "bridges" for short) are Tor relays that aren't listed in the main Tor directory. Since there is no complete public list of them, even if your ISP is filtering connections to all the known Tor relays, they probably won't be able to block all the bridges. If you suspect your access to the Tor network is being blocked, you may want to use bridges.

The addition of bridges to Tor is a step forward in the blocking resistance race. It is perfectly possible that even if your ISP filters the Internet, you do not require a bridge to use Tor. So you should try to use Tor without bridges first, since it might work.

InvizBox also has pluggable transport support. We support obfs2, obfs3 and scramblesuit bridges. Only use these bridge types if normal bridges are blocked for you.

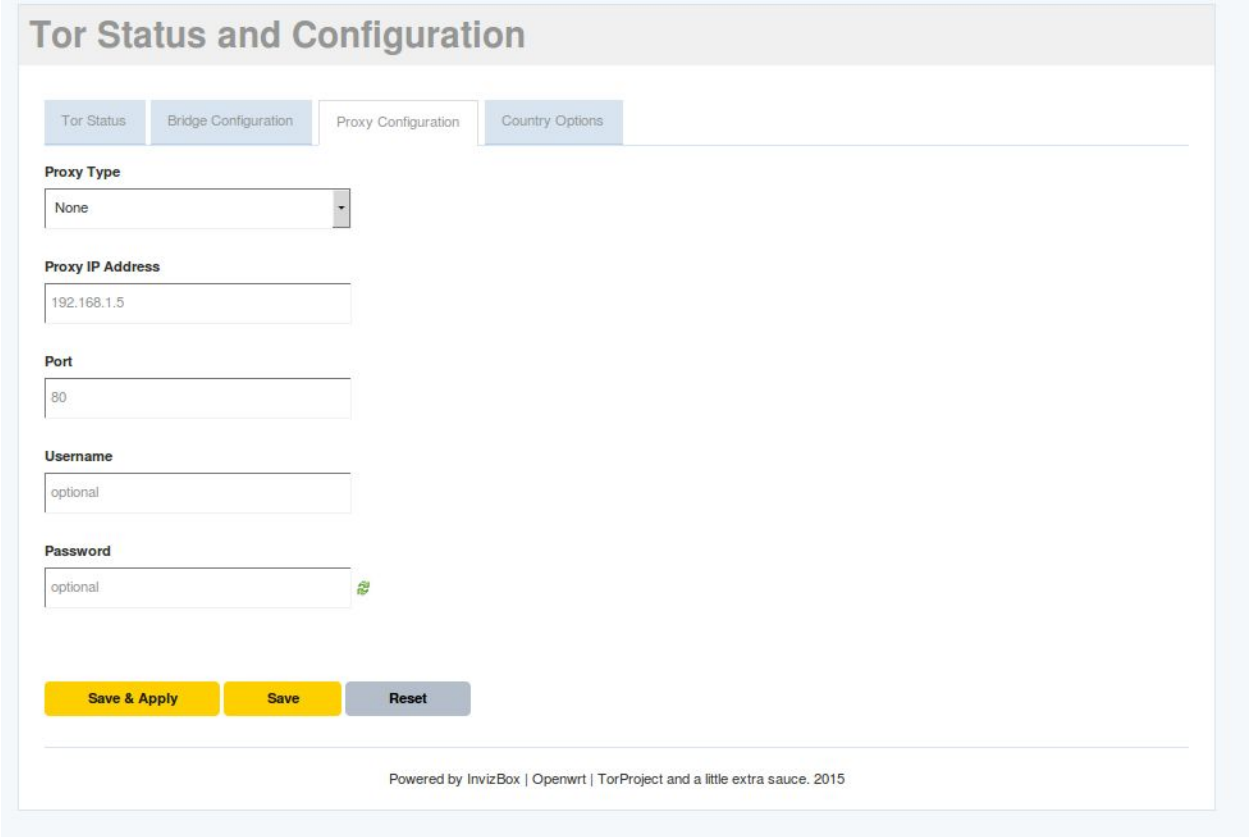
To use Bridges on InvizBox. Input the bridges into the textbox and click “Save & Apply”. You can get usable bridges from here.



Proxy Configuration

InvizBox has the ability to configure Tor to use any HTTPS or SOCKS proxy to get access to the Tor Network. This means even if Tor is blocked by your local network, open proxies can be safely used to connect to the Tor Network and on to the uncensored Internet. A caveat is that the open proxy host will see you are using Tor, but it will not be able to read your traffic as it is still wrapped in layers of encryption.

These steps assume you have have a valid proxy of type HTTPS, SOCKS4, or SOCKS5. (To clarify, an HTTPS proxy is an HTTP proxy that also supports CONNECT requests.)



1. Choose the Type of proxy you are using, whether HTTP/HTTPS, SOCKS4, or SOCKS5.
2. Proxy IP Address: Enter the open proxy address. This can be a hostname or IP Address.
3. Port: Enter the port for the proxy.
4. Generally, you do not need a Username and Password. If you do, enter the information in the proper fields.
5. Once you change any of these click the "**Save & Apply"** button on the bottom of the screen.
6. Tor will restart and the status can be seen on the Tor Status tab.

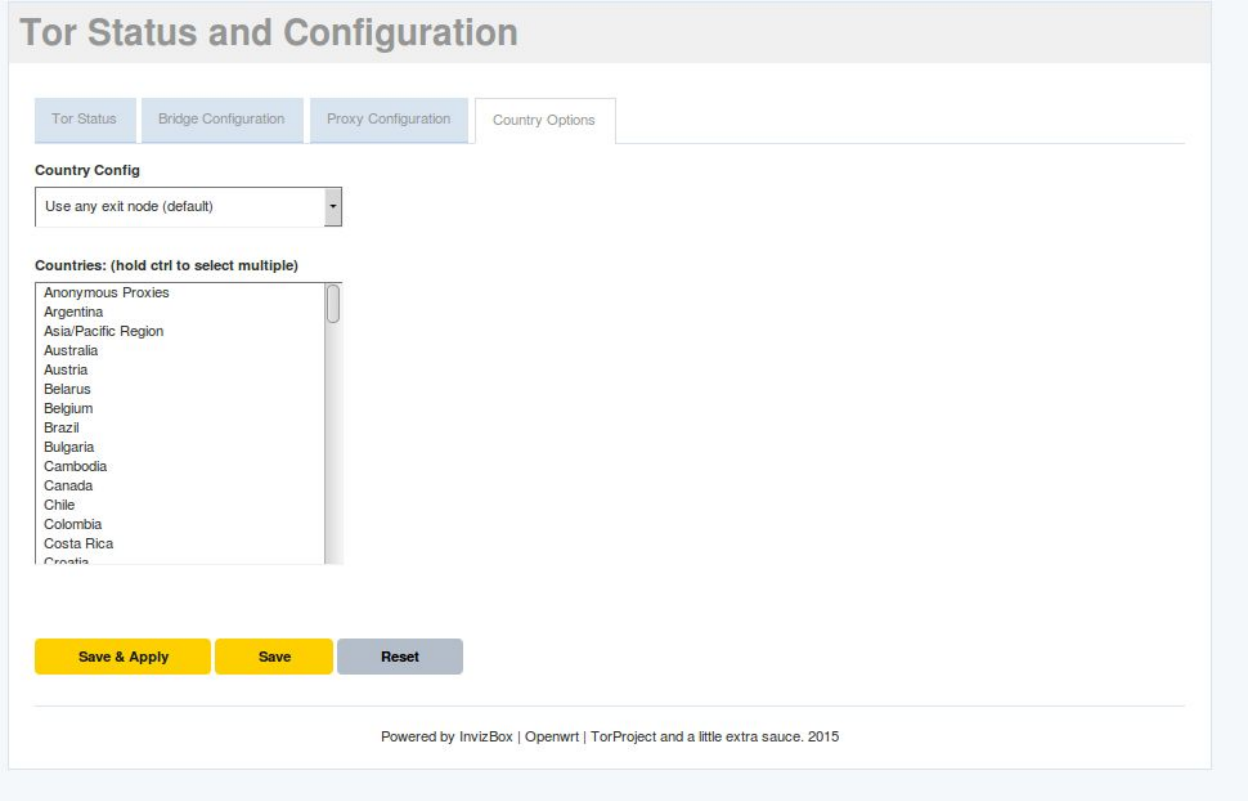
Country Configuration

InvizBox has the ability to configure which exit nodes Tor uses. There are multiple options detailed below

1. Use any exit node (default)
   This is the Tor default. Tor will decide the best route using this method.
2. Exclude "Five Eyes" countries
   This option will exclude Australia, Canada, New Zealand, the United Kingdom and the United States for the Tor route selection.
3. Allow only countries selected below

This option allow you to select from the list below and **only use** those selected Countries as exit Nodes

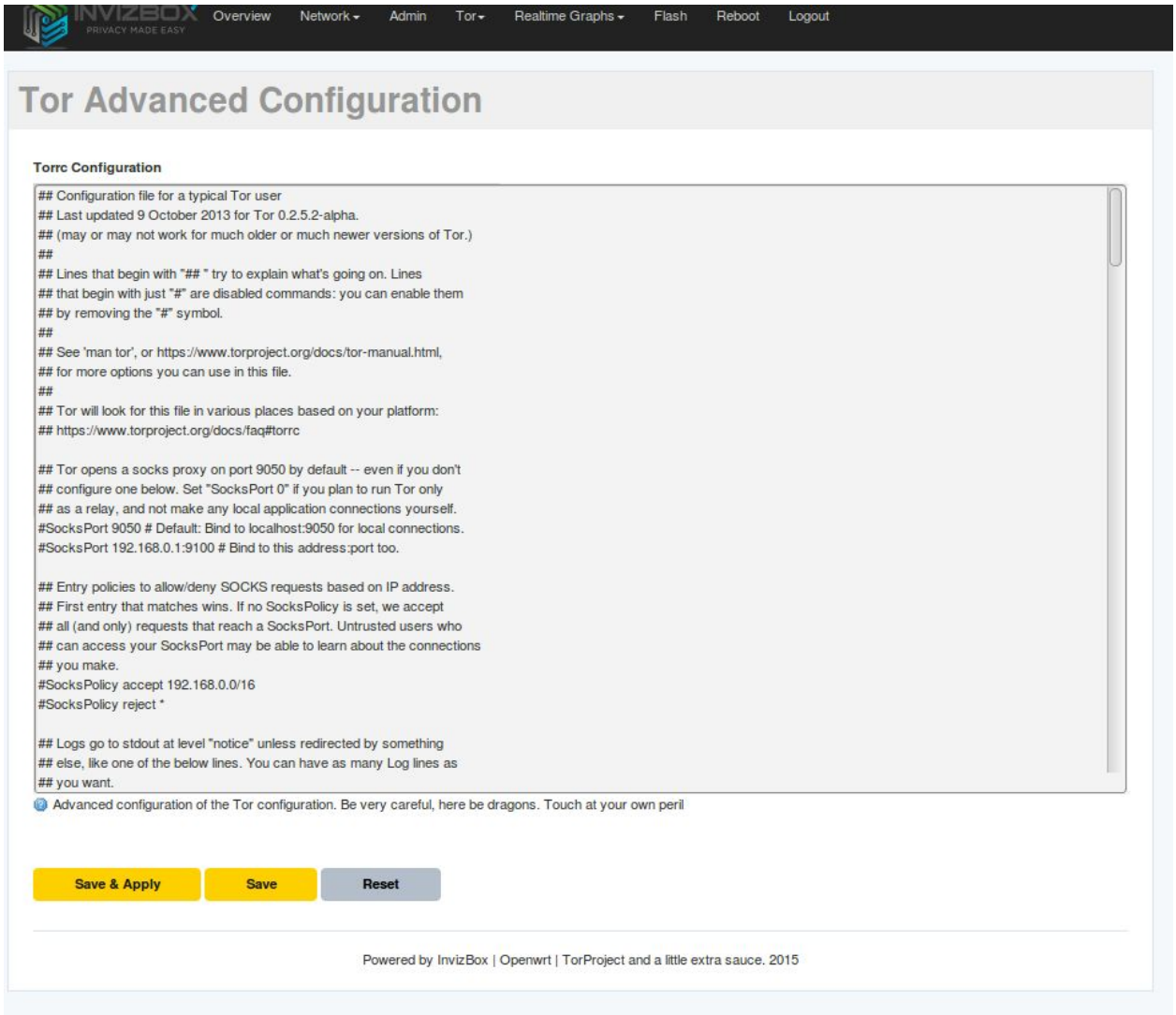
4. Do not use countries selected below
   This option allow you to select from the list below and it will **exclude** using those selected Countries as exit Nodes



N.B - From Tor Project *We recommend you do not use these* — they are intended for testing and may disappear in future versions. You get the best security that Tor can provide when you leave the route selection to Tor; overriding the entry / exit nodes can mess up your anonymity in ways we don't understand.

Tor Advanced Configuration

InvizBox now has the ability to edit the /etc/tor/torrc config file from the GUI.You can use this section to write any config options from the Tor Project manual



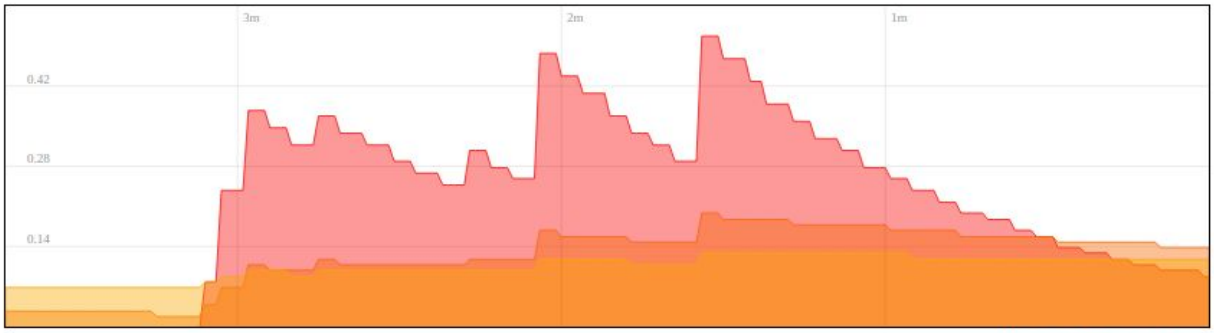
Notes:
Changing this config will overwrite any changes you have made in the normal Tor Config section. Also be aware that an incorrect option here can break Tor and possibly affect your anonymity.

Realtime graphs

Load

This shows the realtime load on the router for 1 min, 5 min and 15 min. Fairly self explanatory, but if not read more on load statistics here

Realtime Load

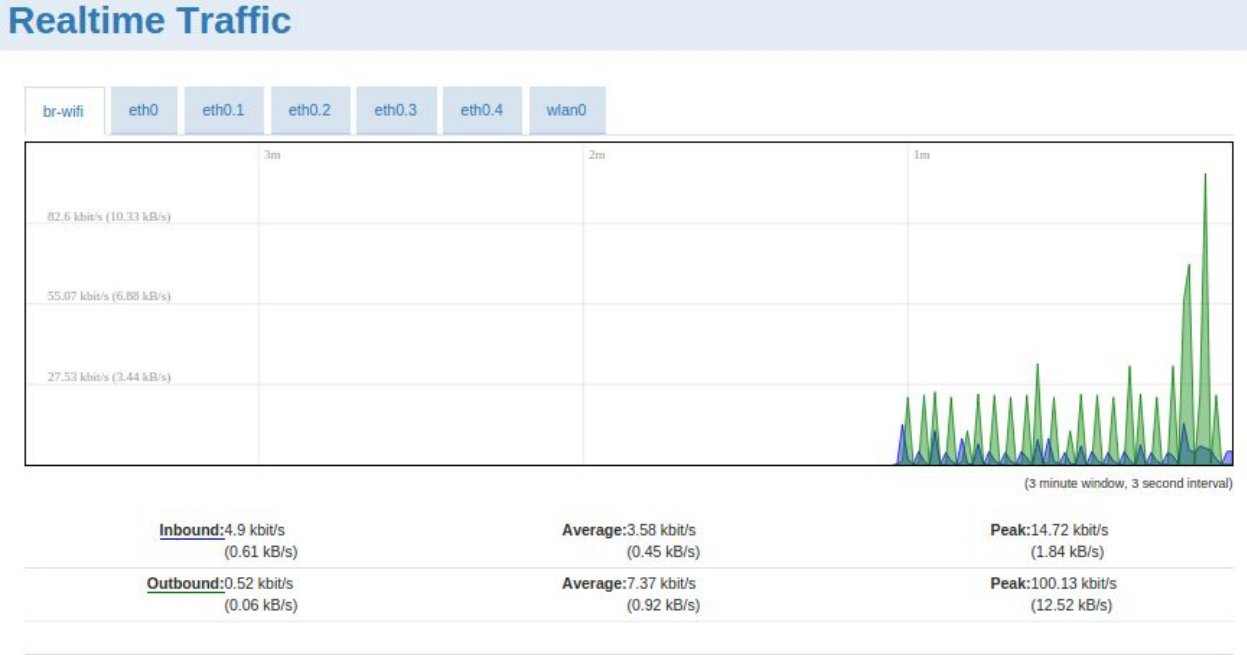


(3 minute window, 3 second interval)

1 Minute Load:0.09	**Average:**0.10	**Peak:**0.51
5 Minute Load:0.14	**Average:**0.14	**Peak:**0.20
15 Minute Load:0.12	**Average:**0.12	**Peak:**0.13

Traffic

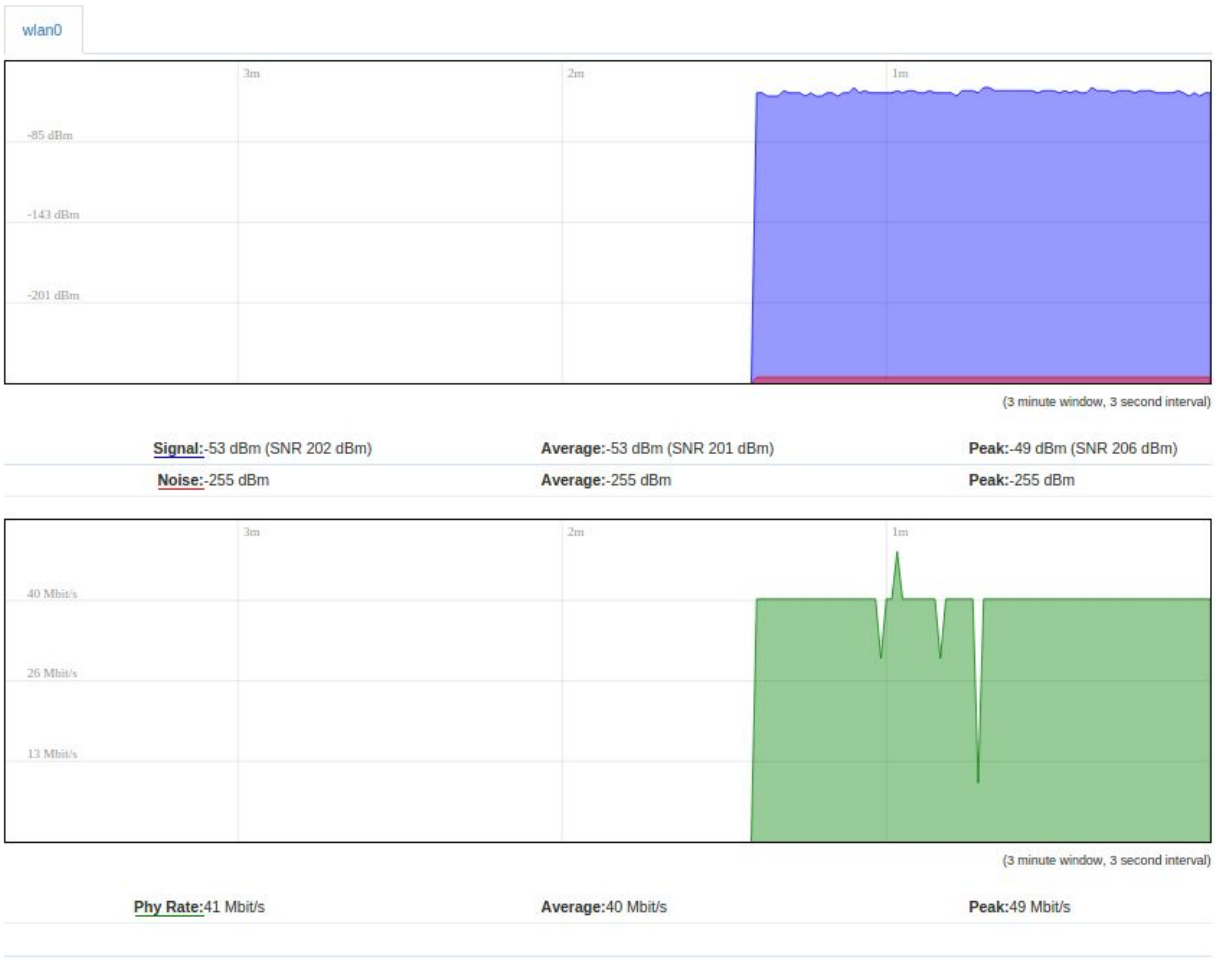
To check the traffic flow on any of the interfaces WAN,Tor,LAN,Wifi etc. Open Realtime GRaphs -> Traffic. It shows the Inbound/Outbound Average and Peak traffic rates.



Wireless

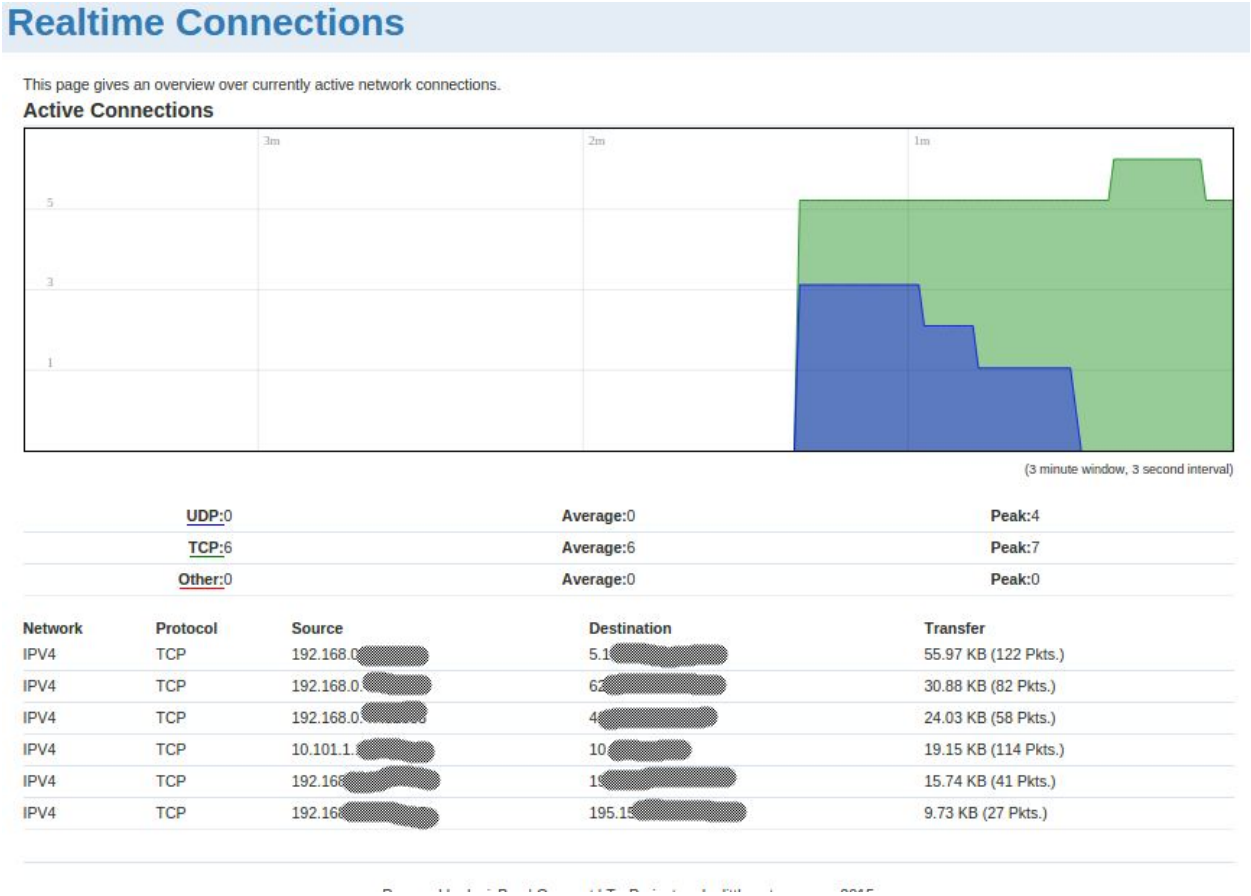
The Wireless section show the realtime graphs for Signal, Noise and Physical Rate.

Realtime Wireless



Connections

This section gives an overview of all the currently active connections on the router both source and destination.



Realtime Connections

This page gives an overview over currently active network connections.

Active Connections

(3 minute window, 3 second interval)

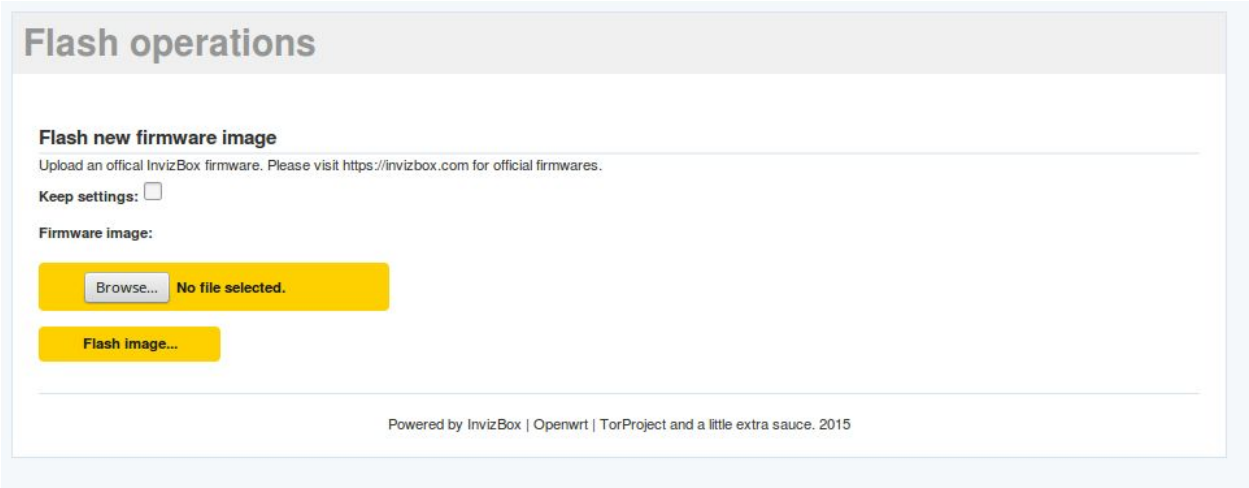
UDP:0	Average:0	Peak:4
TCP:6	Average:6	Peak:7
Other:0	Average:0	Peak:0

Network	Protocol	Source	Destination	Transfer
IPV4	TCP	192.168.0[redacted]	5.1[redacted]	55.97 KB (122 Pkts.)
IPV4	TCP	192.168.0.[redacted]	62[redacted]	30.88 KB (82 Pkts.)
IPV4	TCP	192.168.0[redacted]	4[redacted]	24.03 KB (58 Pkts.)
IPV4	TCP	10.101.1.[redacted]	10[redacted]	19.15 KB (114 Pkts.)
IPV4	TCP	192.16[redacted]	1[redacted]	15.74 KB (41 Pkts.)
IPV4	TCP	192.16[redacted]	195.1[redacted]	9.73 KB (27 Pkts.)

Flash

Periodically InvizBox will release a new firmware. This is the section where you upload and apply that firmware. Only ever flash official InvizBox firmware. We can't assist if you start tinkering with other firmwares.

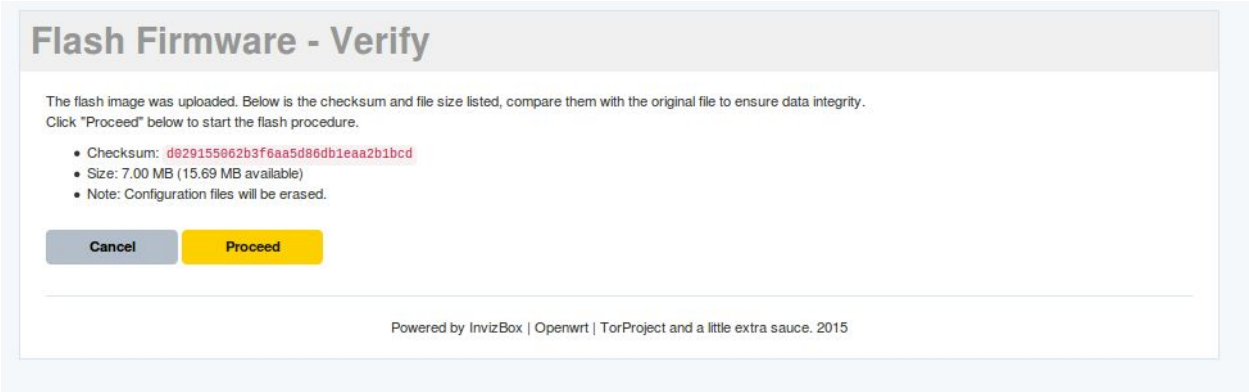
Dont worry the flash procedure is pretty straightforward.



To install a new firmware follow these simple steps

1. Download official firmware from [our firmware page](#).
2. Take note of the listed "Checksum" on the InvizBox website.
3. On the InvizBox router, in the Flash section click "Choose File" and select the official firmware that you downloaded.
4. Click "Flash Image".

Wait a few second whilst the firmware is uploaded to the InvizBox. A page similar to the below should appear.

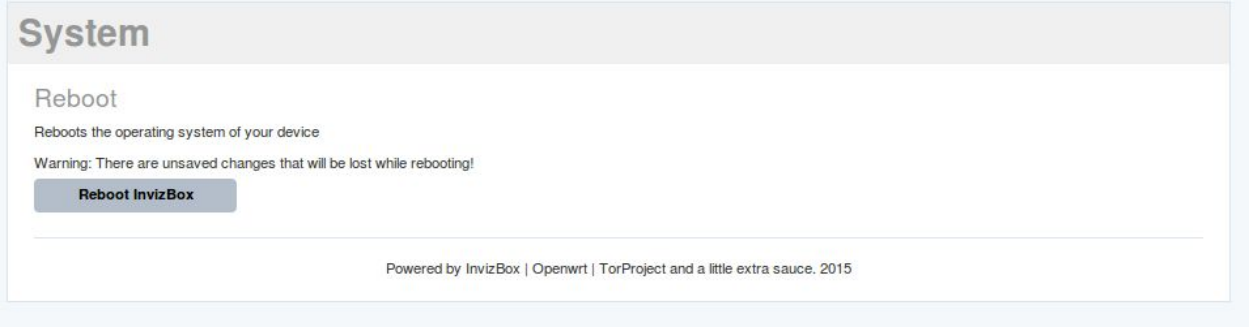


Verify that the “Checksum” displayed matches the corresponding one on the firmware download page that you took note of earlier. **If they do not match click “Cancel”.** If everything matches then go ahead and click “Proceed”. Wait Approx 120 seconds for the flash to complete and for the InvizBox to reboot. That’s it.

Note: *All settings and any password changes will be erased / reset by flashing. Please use the password supplied with the InvizBox to connect to both Wifi and Administration UI.*

Reboot

To reboot the InvizBox. Click “Reboot InvizBox”. Yes its that simple.



The follow page will be displayed showing you everything is in order.

Logout

As simple as it sounds. If you wish to Logout. Click “Logout”

Troubleshooting

Reset

Reserved for those moments when something bad has happened and you can't figure it out. You've tried turning it off and on again. Hair is beginning to get pulled. Hard Reset is your friend.

To perform a Hard Reset:

1. Power Off the Invizbox.
2. On the rear of the InvizBox there is a Reset button. (Use a paperclip or similar to push the button)
3. Hold the Reset button and Power on the InvizBox, Keep holding the Reset button for 30 seconds.
4. Thats it. You're back to how the InvizBox was when it first arrived.

Misc Recommendations

Please consider using the following plugins:

- HTTPS everywhere
- Privacy Badger
- uBlock

Also please look into disabling WebRTC. This is an issue in both Firefox and Chrome which can lead to IP address exposure. There are firewall rules in place in the latest InvizBox firmware to help protect you.

To disable WebRTC in Firefox, enter about:config into the address bar, then set media.peerconnection.enabled to false (double click works).

Alternatively you can install the NoScript add on.

In Chrome / Chromium the add on available is called WebRTC block. You can alternatively install ScriptSafe. Both are available in the Chrome store.