



---

# InvizBox User Guide

---



# Table of contents

[Table of contents](#)

[Introduction](#)

[Hardware](#)

[Quick Setup](#)

[Six Easy Steps](#)

[Overview](#)

[General Status](#)

[Admin](#)

[Password & Language](#)

[DropBear SSH](#)

[Network](#)

[Wifi](#)

[Customizing Wifi](#)

[Device Configuration](#)

[Interface Configuration](#)

[Network](#)

[Tor](#)

[Tor Status](#)

[Bridge Configuration](#)

[Proxy Configuration](#)

[Country Configuration](#)

[Tor Advanced Configuration](#)

[Realtime graphs](#)

[Load](#)

[Traffic](#)

[Wireless](#)

[Connections](#)

[Flash](#)

[Reboot](#)

[Logout](#)

[Troubleshooting](#)

[Reset](#)

[Misc Recommendations](#)



## 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



INVIZBOX PRIVACY MADE EASY

[Overview](#)
[Network](#)
[Admin](#)
[Tor](#)
[Realtime Graphs](#)
[Flash](#)
[Reboot](#)
[Logout](#)

---

## Status

### Tor Status

Tor Status	Connected to the Tor network
Tor Version	0.2.7.6 : recommended

### System

Hostname	InvizBox
Model	InvizBox : V1.3.0
Local Time	Mon Apr 11 20:19:18 2016
Uptime	3d 10h 44m 39s
Load Average	0.02, 0.59, 0.54
Memory	34704 kB / 61528 kB (56%)

### Network

IPv4 WAN Status	Type: dhcp Address: 192.168.0.103 Netmask: 255.255.255.0 Gateway: 192.168.0.254 DNS 1: [REDACTED] DNS 2: [REDACTED] Connected: 4h 22m 35s
Active Connections	7 / 3844 (0%)

### DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
[REDACTED]	10.101.0.96	[REDACTED]	20h 1m 54s

### Wireless

Generic 802.11bgn Wireless Controller (radio0)	SSID: [REDACTED] Mode: Master Channel: 11 (2.462 GHz) Bitrate: 72.2 Mbit/s BSSID: [REDACTED] Encryption: mixed WPA/WPA2 PSK (CCMP)
--	---

### Connected Clients

MAC-Address	Network	Signal	Noise	RX Rate	TX Rate
[REDACTED]	Master [REDACTED]	-70 dBm	0 dBm	72.2 Mbit/s, MCS 7, 20MHz	72.2 Mbit/s, MCS 7, 20MHz

Powered by InvizBox | Openwrt | TorProject and a little extra sauce. 2015

# Admin

## Password & Language

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



## Router Password

Changes the administrator password for accessing the device

### System Properties

#### Language

#### Password

#### Confirmation

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.

## SSH Access

Dropbear offers [SSH](#) network shell access and an integrated [SCP](#) server

### Dropbear Instance

*This section contains no values yet*

**Add**

### SSH-Keys

Here you can paste public SSH-Keys (one per line) for SSH public-key authentication.

**Save & Apply**

**Save**

**Reset**

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



## SSH Access

Dropbear offers [SSH](#) network shell access and an integrated [SCP](#) server

### Dropbear Instance

Port

Specifies the listening port of this *Dropbear* instance

Password authentication

Allow [SSH](#) password authentication

Allow root logins with password

Allow the *root* user to login with password

### SSH-Keys

Here you can paste public SSH-Keys (one per line) for SSH public-key authentication.

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.






## Wireless Overview

 **Generic MAC80211 802.11bgn (radio0)**  
Channel: 11 (2.462 GHz) | Bitrate: ? Mbit/s

---

 **SSID:** InvizBox | **Mode:** Master  
0% **BSSID:** 2[REDACTED] | **Encryption:** mixed WPA/WPA2 PSK (CCMP)

## Connected Clients

SSID	MAC-Address	IPv4-Address	Signal	Noise	RX Rate	TX Rate
No information available						

Powered by InvizBox | Openwrt | TorProject and a little extra sauce. 2015

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 brings you to a more detailed section which allows 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:** 20:00:00:00:00:00 | **Encryption:** mixed WPA/WPA2 PSK (CCMP)  
**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

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

**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

#### Device Configuration

General Setup
Advanced Settings

**Status**

Mode: Master | SSID: InvizBox  
 BSSID: 20:28:18:A0:BC:5E | Encryption: mixed WPA/WPA2 PSK (CCMP)  
 Channel: 11 (2.462 GHz) | Tx-Power: 20 dBm  
 Signal: -58 dBm | Noise: 0 dBm  
 Bitrate: 48.0 Mbit/s | Country: 00

---

Wireless network is enabled

Disable

**Channel**

11 (2.462 GHz)
▼

**Transmit Power**

20 dBm (100 mW)
▼

### 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



## Device Configuration

### Band

2.4GHz (802.11g+n) ▼

### HT mode (802.11n)

20MHz ▼

### Country Code

00 - World ▼

Use ISO/IEC 3166 alpha2 country codes.

### Distance Optimization

Distance to farthest network member in meters.

### Fragmentation Threshold

### RTS/CTS Threshold

## Interface Configuration

## 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.



### Interface Configuration

General Setup | **Wireless Security** | MAC-Filter

**ESSID**  
InvizBox

**Mode**  
Access Point ▼

**Network**

- lan: \*\*\*
- tor: \*\*\*
- wan: \*\*\*
- wifi: \*\*\*
- 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**

### Wireless Security

In this section you can edit the following :

- Encryption
- Cipher
- Key

### Interface Configuration

General Setup | **Wireless Security** | MAC-Filter

**Encryption**  
WPA-PSK/WPA2-PSK Mixed Mode ▼

**Cipher**  
auto ▼

**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

### Interface Configuration

General Setup
Wireless Security
MAC-Filter

**MAC-Address Filter**

Allow listed only ▼

**MAC-List**

▼

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.

### Interfaces

**Interface Overview**

Network	Status	Actions
<b>LAN</b> <small>لوز (22.00)</small> br-lan	Uptime: 3d 22h 24m 51s MAC-Address: ██████████ RX: 14.15 MB (53578 Pkts.) TX: 24.09 MB (48454 Pkts.) IPv4: 10.101.0.1/24	<span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;">Connect</span> <span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;">Stop</span> <span style="border: 1px solid #ccc; padding: 2px 10px;">Edit</span>
<b>TOR</b> <small>تور</small> eth0.3	Uptime: 3d 22h 24m 51s MAC-Address: ██████████ RX: 0.00 B (0 Pkts.) TX: 0.00 B (0 Pkts.) IPv4: 172.16.1.1/24	<span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;">Connect</span> <span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;">Stop</span> <span style="border: 1px solid #ccc; padding: 2px 10px;">Edit</span>
<b>WAN</b> <small>وان</small> eth0.2	Uptime: 16h 3m 10s MAC-Address: ██████████ RX: 66.86 MB (111684 Pkts.) TX: 18.47 MB (32147 Pkts.) IPv4: 192.168.0.103/24	<span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;">Connect</span> <span style="border: 1px solid #ccc; padding: 2px 10px; margin-right: 5px;">Stop</span> <span style="border: 1px solid #ccc; padding: 2px 10px;">Edit</span>

Add new interface...

Powered by InvizBox | Openwrt | TorProject and a little extra sauce. 2015

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.

### Tor Status and Configuration

Tor Status
Bridge Configuration
Proxy Configuration
Country Options

Restart Tor
New Identity
Refresh

**Tor Connection Status**

Connected to the Tor network

**Tor Version**

0.2.7.6 : recommended

**Tor Circuit Status**

```

39 BUILT $9CAE650EB7B479B3ED7C4A9C0FDB4265745BDC0F~Unnamed,$397136F37F5EFCADB6371318839B875140E439B~coolmike,$276E109C584D98CAC7813185F217...
444 BUILT $9CAE650EB7B479B3ED7C4A9C0FDB4265745BDC0F~Unnamed,$B9F3623690227FCFDB0D7D63AA1B6E3CC4A74338~asuka,$31D01A8CD3799E0CB6A56D8F1498...
446 BUILT $9CAE650EB7B479B3ED7C4A9C0FDB4265745BDC0F~Unnamed,$30973217E70AF00EBE51797FF6D9AA720A902EAA~youlooksuspcious,$D52CD431CEF28E01B11...
                    
```

Save & Apply
Save
Reset

Powered by InvizBox | Openwrt | TorProject and a little extra sauce. 2015

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](#).

### Tor Status and Configuration

Tor Status | Bridge Configuration | Proxy Configuration | Country Options

#### Bridge Configuration

ⓘ Please enter in the bridges you want Tor to use, one per line.  
The format is : "ip:port [fingerprint]" where fingerprint is optional. e.g. 121.101.27.4:443 4352e58420e68f5e40ade74faddcccd9d1349413.  
To get bridge information, see the Tor bridges page.

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.

[Save & Apply](#) [Save](#) [Reset](#)

Powered by InvizBox | Openwrt | TorProject and a little extra sauce. 2015

## 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 a valid proxy of type HTTPS, SOCKS4, or SOCKS5. (To clarify, an HTTPS proxy is an HTTP proxy that also supports CONNECT requests.)

### Tor Status and Configuration

Tor Status
Bridge Configuration
Proxy Configuration
Country Options

**Proxy Type**

**Proxy IP Address**

**Port**

**Username**

**Password**

Save & Apply
Save
Reset

Powered by InvizBox | Openwrt | TorProject and a little extra sauce. 2015

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**

### Tor Status and Configuration

Tor Status

Bridge Configuration

Proxy Configuration

Country Options

**Country Config**

Use any exit node (default)

**Countries: (hold ctrl to select multiple)**

Anonymous Proxies  
 Argentina  
 Asia/Pacific Region  
 Australia  
 Austria  
 Belarus  
 Belgium  
 Brazil  
 Bulgaria  
 Cambodia  
 Canada  
 Chile  
 Colombia  
 Costa Rica  
 Croatia

Save & Apply

Save

Reset

Powered by InvizBox | Openwrt | TorProject and a little extra sauce. 2015

**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](#)



INVIZBOX PRIVACY MADE EASY

[Overview](#)
[Network](#)
[Admin](#)
[Tor](#)
[Realtime Graphs](#)
[Flash](#)
[Reboot](#)
[Logout](#)

---

## Tor Advanced Configuration

**Torrc Configuration**

```

## Configuration file for a typical Tor user
## Last updated 9 October 2013 for Tor 0.2.5.2-alpha.
## (may or may not work for much older or much newer versions of Tor.)
##
## Lines that begin with "## " try to explain what's going on. Lines
## that begin with just "#" are disabled commands: you can enable them
## by removing the "#" symbol.
##
## See 'man tor', or https://www.torproject.org/docs/tor-manual.html,
## for more options you can use in this file.
##
## Tor will look for this file in various places based on your platform:
## https://www.torproject.org/docs/faq#torrc

## Tor opens a socks proxy on port 9050 by default -- even if you don't
## configure one below. Set "SocksPort 0" if you plan to run Tor only
## as a relay, and not make any local application connections yourself.
#SocksPort 9050 # Default: Bind to localhost:9050 for local connections.
#SocksPort 192.168.0.1:9100 # Bind to this address:port too.

## Entry policies to allow/deny SOCKS requests based on IP address.
## First entry that matches wins. If no SocksPolicy is set, we accept
## all (and only) requests that reach a SocksPort. Untrusted users who
## can access your SocksPort may be able to learn about the connections
## you make.
#SocksPolicy accept 192.168.0.0/16
#SocksPolicy reject *

## Logs go to stdout at level "notice" unless redirected by something
## else, like one of the below lines. You can have as many Log lines as
## you want.
                
```

Advanced configuration of the Tor configuration. Be very careful, here be dragons. Touch at your own peril

Save & Apply
Save
Reset

---

Powered by InvizBox | Openwrt | TorProject and a little extra sauce. 2015

**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.

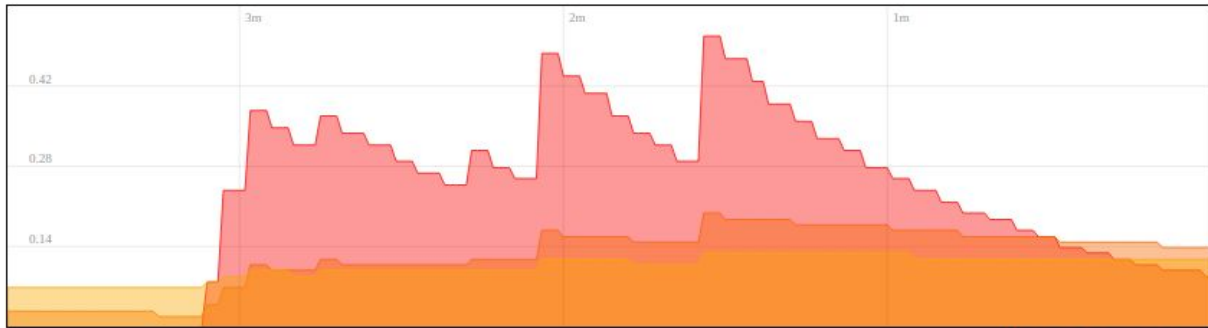
## Realtime graphs

### 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)

<b>1 Minute Load:</b> 0.09	<b>Average:</b> 0.10	<b>Peak:</b> 0.51
<b>5 Minute Load:</b> 0.14	<b>Average:</b> 0.14	<b>Peak:</b> 0.20
<b>15 Minute Load:</b> 0.12	<b>Average:</b> 0.12	<b>Peak:</b> 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.

### Realtime Traffic

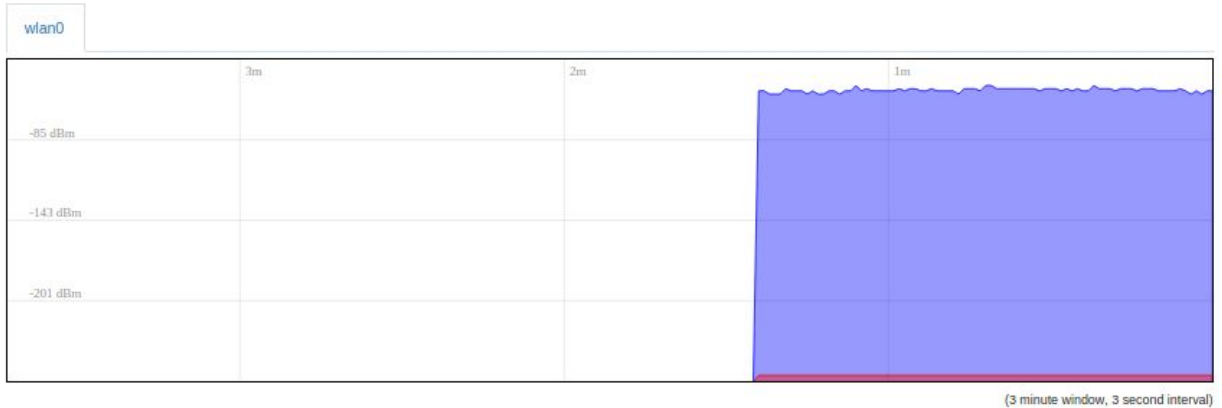




## Wireless

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

### Realtime Wireless



**Signal:** -53 dBm (SNR 202 dBm)

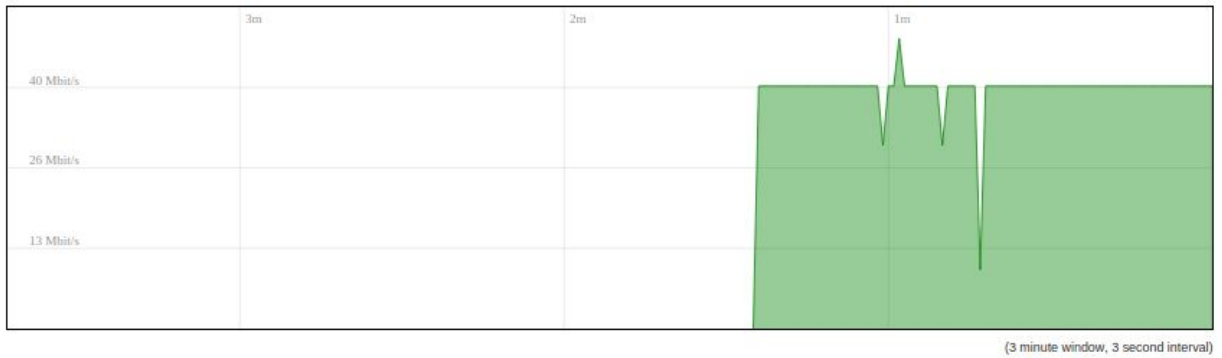
**Average:** -53 dBm (SNR 201 dBm)

**Peak:** -49 dBm (SNR 206 dBm)

**Noise:** -255 dBm

**Average:** -255 dBm

**Peak:** -255 dBm



**Phy Rate:** 41 Mbit/s

**Average:** 40 Mbit/s

**Peak:** 49 Mbit/s



## 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)

<u>UDP</u> :0	Average:0	Peak:4
<u>TCP</u> :6	Average:6	Peak:7
<u>Other</u> :0	Average:0	Peak:0

Network	Protocol	Source	Destination	Transfer
IPV4	TCP	192.168.0.1	5.1.1.1	55.97 KB (122 Pkts.)
IPV4	TCP	192.168.0.1	62.1.1.1	30.88 KB (82 Pkts.)
IPV4	TCP	192.168.0.1	4.1.1.1	24.03 KB (58 Pkts.)
IPV4	TCP	10.101.1.1	10.1.1.1	19.15 KB (114 Pkts.)
IPV4	TCP	192.168.0.1	1.1.1.1	15.74 KB (41 Pkts.)
IPV4	TCP	192.168.0.1	195.15.1.1	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.

### Flash operations

**Flash new firmware image**  
Upload an official InvizBox firmware. Please visit <https://invizbox.com> for official firmwares.

Keep settings:

Firmware image:

No file selected.

---

Powered by InvizBox | Openwrt | TorProject and a little extra sauce. 2015

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.

### Flash Firmware - Verify

The flash image was uploaded. Below is the checksum and file size listed, compare them with the original file to ensure data integrity.  
Click "Proceed" below to start the flash procedure.

- Checksum: `d029155962b3f6aa5d86db1eaa2b1bcd`
- Size: 7.00 MB (15.69 MB available)
- Note: Configuration files will be erased.

---

Powered by InvizBox | Openwrt | TorProject and a little extra sauce. 2015





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.

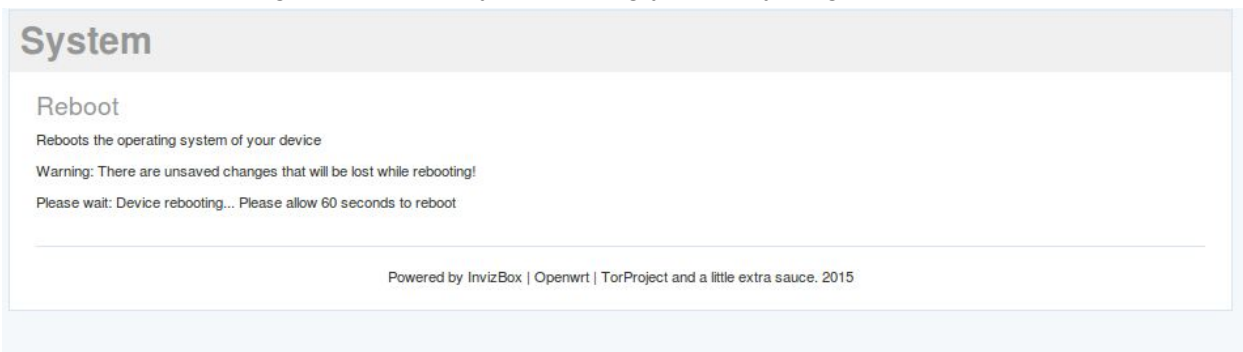
**Note:** *All settings and any password changes will be erased / reset by flashing. Please use the password supplied with the InvizBox to connect to both Wifi and Administration UI.*

## 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. That's 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.