

FirmUx

User Guide

For v1.11.0 firmwares

This user's guide and the software described in it are copyrighted with all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of 8devices

Notice

8devices reserves the right to change specifications without prior notice. While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. 8devices shall be liable only to the degree specified in the terms of sale and delivery. The reproduction and distribution of the documentation and software supplied with this product and the use of its contents are subject to written authorization from 8devices.

Trademarks

8devices logo is a trademark of 8devices. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

Table Of Contents

About This Guide	4	WireGuard® configuration	29
Purpose	4	OpenVPN® configuration	31
Definitions, acronyms, and abbreviations	4	ZeroTier® configuration	32
		Wireless radio configuration	33
Abbreviation list	5	Wireless network configuration	34
		Wireless network security options	36
8devices Firmux boards	6	Access point wireless mode	36
		Station wireless mode	37
Flashing Firmux firmware	6	System configuration	39
Flashing the bootloader	6	Country and time settings	39
Flashing the firmware	6	Device name, location and hostname	39
		Automatic update checker	41
Device Access	7	Physical reset button	42
First connection via Ethernet	7	Services configuration	42
Windows OS	8	Remote management	42
MAC OS	9	HTTP	42
First access to the web management interface	9	SSH	43
		Telnet	44
General Device Options	12	NTP	45
Applying and saving configuration changes	12	Device discovery	45
Navigating across the control settings	12	SNMP and SNMP traps	46
Device information pages	13	SNMP	46
Cards and Tabs	13	SNMP traps	47
Site Dashboard	14	Remote syslog	48
Interfaces	15	Ping Watchdog	49
Network	15	Web Shell	50
Clients	17	User configuration	50
Activity	18		
Maintenance	18	Tools	51
		Device discovery	51
Device Configuration	20	Site survey	51
Network configuration page	20	Ping	51
WAN configuration	21	Traceroute	52
DHCP client mode	21	View log	53
Static IP mode	21	Spectral scan	53
LAN configuration	22	Speedtest	54
Secondary IP	24	Web Shell	54
DHCP server	24		
VLAN configuration	25		
Ethernet configuration	26		
Hosts configuration	27		
Local DNS hosts	27		
DNS Blackhole	27		
Ad Block	27		
Static routes configuration	28		
Port forwarding configuration	28		
VPN configuration	29		

About This Guide

Purpose

This document provides information and procedures on setup, configuration, and management of the Firmux system.

Definitions, acronyms, and abbreviations

The following typographic conventions are used throughout this document:



Additional information that may be helpful but which is not required.



Important information that should be observed.

Abbreviation list

The following list of abbreviations are used throughout the document

Abbreviation	Description
AP	Access Point
DHCP	Dynamic Host Control Protocol
GHz	GigaHertz
GUI	Graphical User Interface
LAN	Local Area Network
LTE	Long Term Evolution
MAC	Media Access Control
MCS	Modulation Coding Scheme
MHz	MegaHertz
Mbps	Megabits per second
NAT	Network Address Translation
NTP	Network Time Protocol
HTTP	HyperText Transfer Protocol
PC	Personal Computer
PSK	Pre-Shared Key
RSSI	Received Signal Strength Indication
RX	Receive
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Service Set Identifier
TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WDS	Wireless Distribution System
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access 2

8devices Firmux boards

Single-band SOMs

Carambola 2, Centipede, Lima, Kinkan

Dual-band SOMs

Rambutan, Jalapeno, Komikan, Habanero, Mango

Flashing Firmux firmware

Flashing the bootloader

Carambola 2: <https://www.8devices.com/wiki/carambola2:uboot>

Centipede: <https://www.8devices.com/wiki/centipede:uboot>

Lima: <https://www.8devices.com/wiki/lima:uboot>

Jalapeno: <https://www.8devices.com/wiki/jalapeno:uboot>

Habanero: <https://www.8devices.com/wiki/habanero:uboot>

Rambutan: <https://www.8devices.com/wiki/rambutan:uboot>

After the new bootloader is flashed successfully, the bootloader environment needs to be reset. This step is different for each SOM. Execute these commands in the bootloader shell:

For Jalapeno, Habanero or Rambutan:

```
env default -f
```

For Lima:

```
sf erase 0x40000 0x40000
```

For Carambola 2 or Centipede:

```
erase 9f040000 +10000
```

After the environment is reset, save it and reboot the board:

```
env save
```

```
reset
```

Flashing the firmware

If you are flashing Firmux firmware on a SOM that previously had OpenWRT firmware, please follow the firmware recovery procedure described in the 8devices online wiki:

Carambola 2: <https://www.8devices.com/wiki/carambola2:recover>

Centipede: <https://www.8devices.com/wiki/centipede:recover>

Lima: <https://www.8devices.com/wiki/lima:recover>

Jalapeno: <https://www.8devices.com/wiki/jalapeno:recover>

Habanero: <https://www.8devices.com/wiki/habanero:recover>

Rambutan: <https://www.8devices.com/wiki/rambutan:recover>

If your board already has Firmux firmware, you can still flash it using the recovery procedure, although it is not required.

Device Access

First connection via Ethernet



Most Firmux boards have at least 2 ethernet ports. In default configuration one of those ports is configured for Internet connection (WAN port), the other port is configured for local network access (LAN port).

If you connect the Internet cable that was provided to you by your Internet Service Provider (ISP) to the WAN port, then Firmux device will automatically obtain its IP address from the DHCP server of your ISP. If you connect an ethernet cable between your computer and the Firmux board's LAN port, then your computer will automatically obtain an IP address from the DHCP server running on Firmux board.

If you would connect both ethernet cables at once (Internet cable to WAN port and a cable between your computer and the LAN port), then Firmux board would start sharing the internet to your computer as well. This should work automatically, assuming that both your computer's connection is set for automatic DHCP configuration, and that your ISP also provides DHCP service for automatic configuration of most important network parameters.

The default configuration of Firmux devices also has a Wireless network already set up.

WiFi network name: firmux

Authentication password: passphrase

After connecting to WiFi network, your device would be able to access Firmux board's configuration web interface (GUI). If Firmux board is connected to the Internet (via WAN ethernet port), then the internet connection would be shared to WiFi clients as well.

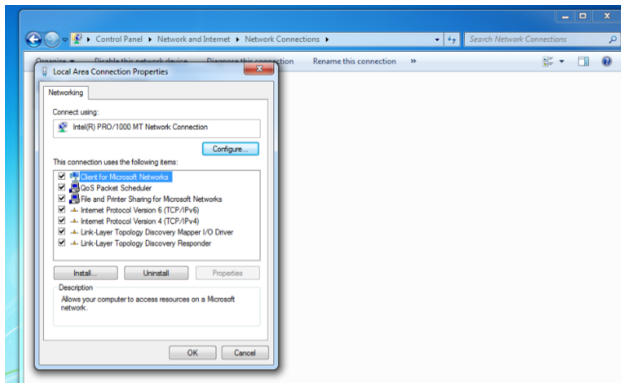
By default, devices connected to WiFi are on the same local network as devices connected by LAN ethernet port - so those devices can access each other easier.

Follow the steps to access device on different OS: In case the Firmux device is unable to obtain an IP address from a DHCP server, it fallback to the default static IP 192.168.1.1 (WAN).

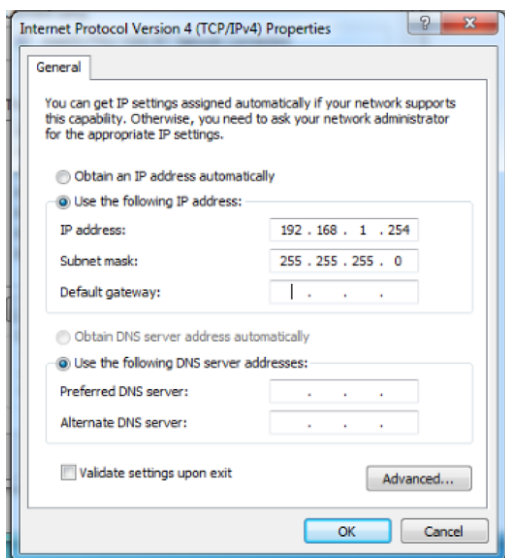
Windows OS

Step 1: Connect your PC directly to the device via Ethernet

Step 2: Open Windows Explorer, navigate to Network Connections ▶ Adapter Settings



Step 3: Set your PC ethernet interface to **192.168.1.254** as displayed below

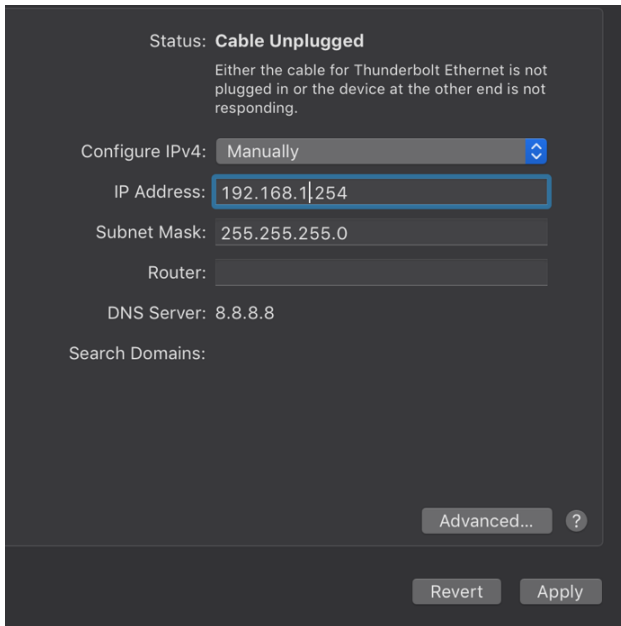


Step 4: Access device UI via <http://192.168.1.1> on WAN

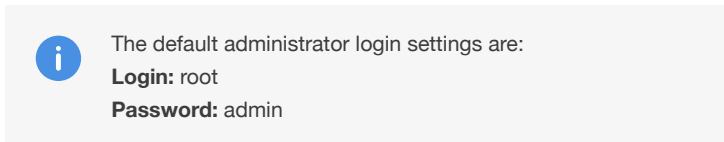
MAC OS

Step 1: Connect your PC to the device via Ethernet.

Step 2: Set your PC ethernet interface to 192.168.1.254 as displayed below



Step 3: Access device UI via <http://192.168.1.1> on WAN



First access to the web management interface

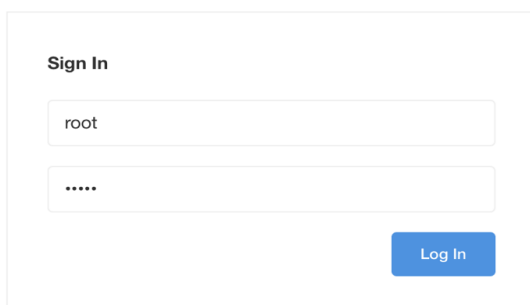
Follow the steps for the first connection to the device web management interface:

Step 1: Start your Web browser.

Step 2: Enter the device IP address in the web browser's address field and enter default login credentials.

FIGURE 1 – LOGIN SCREEN

FIRMUX



Step 2.1: When logging in for the first time, you will be greeted by a setup wizard and suggested to change your username and password.

FIGURE 2 – UPDATE YOUR CREDENTIALS

FIRMUX :

The screenshot shows a web interface for updating credentials. At the top, it says "Step 1: Credentials Change". Below that, the heading "Update your credentials" is followed by a note: "For security reasons we suggest you to update your username and password". There are three input fields: "root" in the first, "Password" in the second, and "Repeat Password" in the third. Each password field has a small eye icon to toggle visibility. At the bottom, there are three buttons: "Skip" (grey), "Back" (white), and "Next" (blue).

Step 2.2: After updating your credentials you can choose an operation mode scenario.

FIGURE 3 – OPERATION MODE SELECTION

FIRMUX :

The screenshot shows a web interface for selecting an operation mode. It says "Step 2 of 4: Operation Mode". Under the heading "Scenarios", there are three radio button options: "Wireless router mode" (which is selected), "Wireless router with wireguard VPN", and "Wireless (WDS) bridge". At the bottom, there are three buttons: "Skip" (grey), "Back" (white), and "Next" (blue).

Step 2.3: After completing the scenario steps you will see the setup wizard summary page, where you can review and confirm the changes.

FIGURE 4 – WIZARD SUMMARY PAGE

FIRMUX :

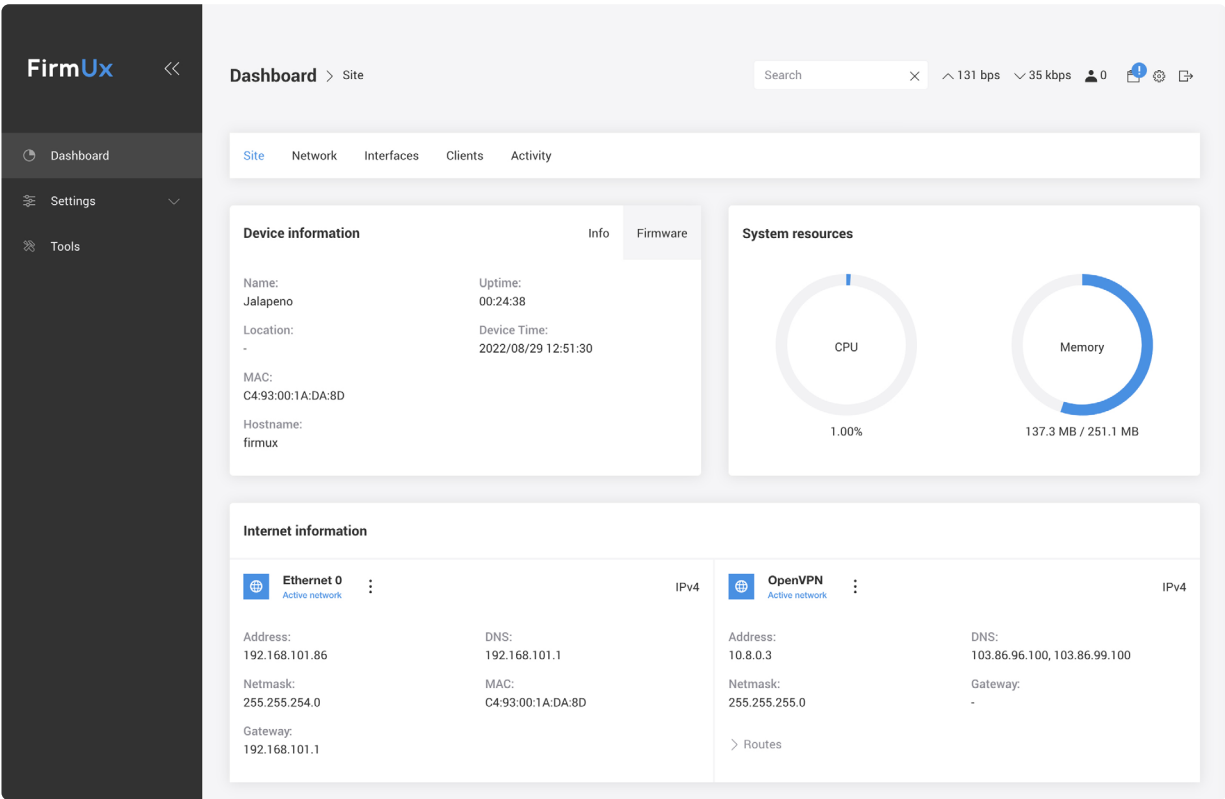
The screenshot shows a summary table for the setup wizard. It says "Step 4 of 4: Summary". The table lists the following settings:

Operation mode	Wireless router
Credentials > Username	root
Credentials > Password	*****
Credentials > Repeat Password	*****
Wireless Settings > SSID	firmux
Wireless Settings > Security mode	wpa2psk
Wireless Settings > Passphrase	*****

At the bottom, there are three buttons: "Skip" (grey), "Back" (white), and "Save" (blue).

Step 3: After a successful initial wizard setup you will see the Dashboard - main page of the device Web management interface. The device now is ready for usage and further configuration..

Figure 5 – the Default device dashboard



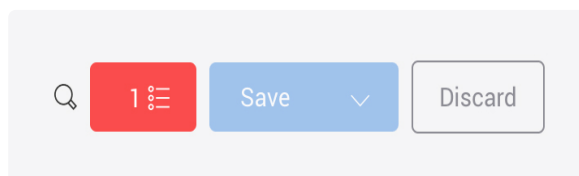
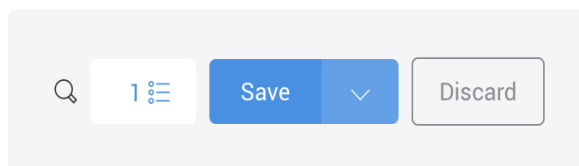
General Device Options

Applying and saving configuration changes

Whenever you make any configuration changes, the Save and Discard buttons will appear in the top right corner of the screen..

You can also view a list of changes before saving, test configuration before accepting it, or discard changes without saving them.

In case your current configuration is invalid (contains some errors, or some required fields are left empty), then the Save button will be disabled and you will be able to view a list of errors. Clicking on the error will take you to the specified error.



Save – if pressed, new configuration settings are applied and written to the permanent device config block.

Discard – if pressed, configuration changes are discarded.

Test changes – after clicking the arrow next to the Save button, Test changes button will appear. By clicking it, you are able to test changes before confirming or aborting them. You will have 3 minutes to check whether the new configuration is operational. If the Confirm button is not clicked during that time, then the new configuration will be discarded and device will return to its previous configuration.

Configuration changes list – the button left of the Save button expands a list of configuration changes you've made.

Configuration errors list – the red button left of the Save button expands a list of errors in the new configuration. The button is only visible if the new configuration is invalid.



It is not required to press Save changes in every Web GUI tab. The device tracks all changes made in every page and when the Save button is pressed, all changes will be applied.

It is very useful to Test changes before accepting them. If device were to become unreachable due to a new configuration, then device would return to its previous configuration after a 3 minute period.

Navigating across the control settings



In order to quickly navigate between different setting pages, use the navigation bar on the left.

Device information pages

The Dashboard of the device WEB interface has multiple pages that displays current configuration information, as well as stats for the device:

Site - the most commonly used basic information of the device.

Network - displays the information for all the networks (zones) that are created on the device, as well as Adblock, ARP and DHCP active leases table.

Interfaces - displays information about device physical interfaces.

Clients - shows WiFi clients that are connected to the board's network.

Activity - displays the log of most important events that occurred since the device was powered on or rebooted.

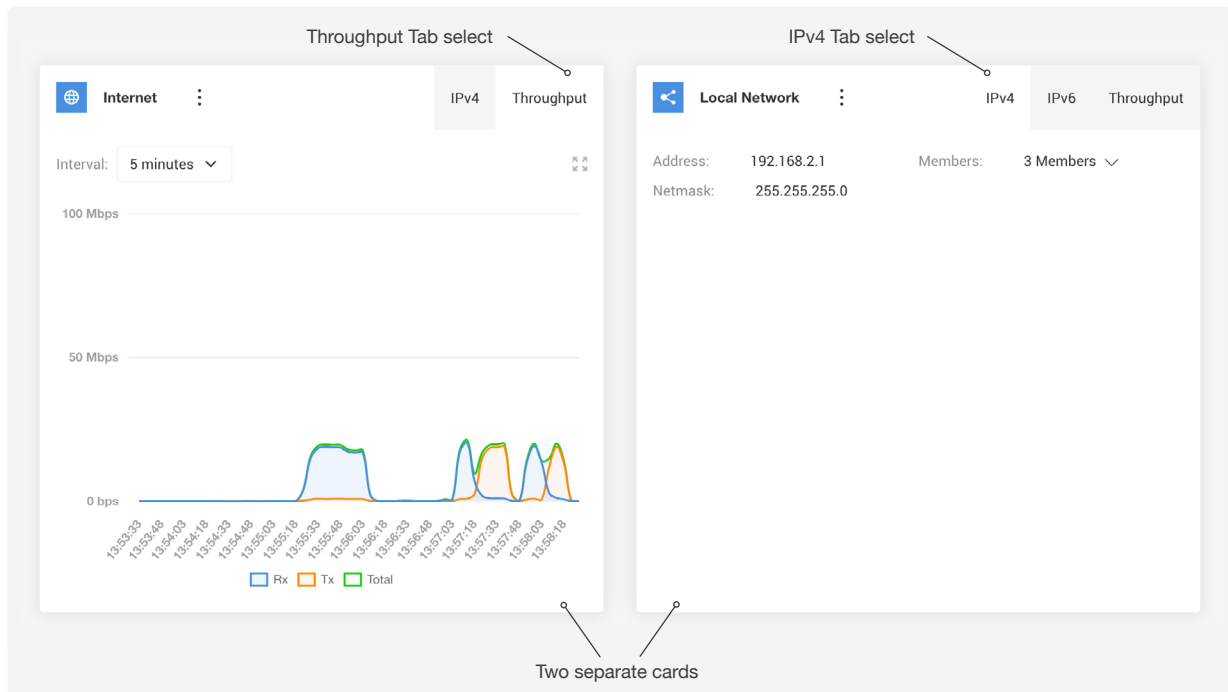
All these pages can be reached through the navigation bar at the top of the dashboard.

Cards and Tabs

Information in WEB GUI pages is separated into **Cards** - a block of information relating to one specific object, like Ethernet or Wireless interface; or Local Network; or WAN Network (internet).

Some Cards have additional information that is separated into Tabs. **Tabs** allow you to select what information should be displayed - like IPv4 or IPv6 network address information; or Throughput graph instead of textual information.

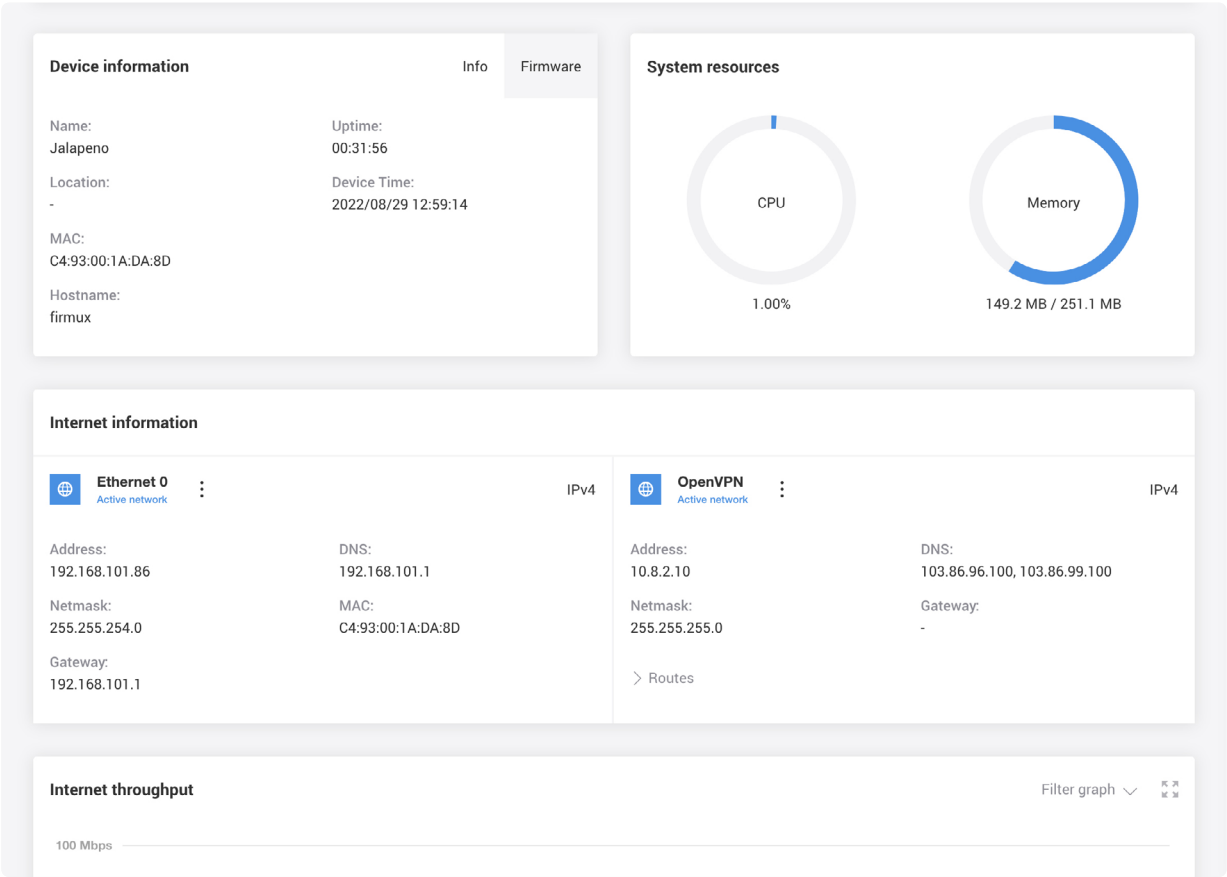
Figure 6 - Cards and Tabs



Site Dashboard

After logging in, WEB GUI displays the Site Dashboard page - main device information page. The site page displays the most important basic information about the device: WAN (internet) connection information, Firmware version, Uptime, CPU load, Network throughput graph, and Wireless client stats.

Figure 7 - Web Management Interface (Site Dashboard)

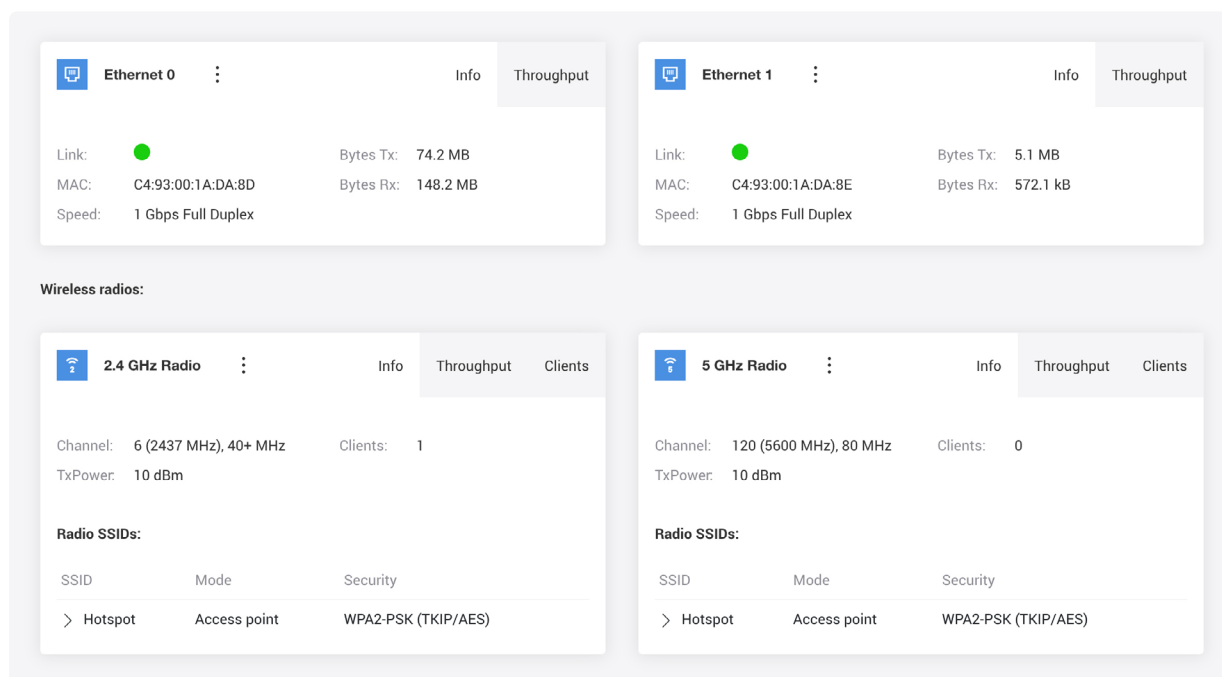


Interfaces

The Interfaces page displays information for Ethernet ports and Wireless radios. In case of device having LTE support, the LTE radio information will also be displayed on the Interfaces page.

The page also contains throughput information for every interface. Throughput graphs are accessible via the “Throughput” tab in every interface card.

Figure 8 – Interfaces information page



Network

The Network page displays information for all the networks (network zones) that are created on the device. By default there are two networks created on a fresh configuration - Internet and Local network.

Internet - the main Wide Area Network (WAN), through which Firmux device is connected to the internet.

Local network - a Local Area Network (LAN), that contains all the local devices in your home or organization which are connected to a Firmux board. The devices on your local network share the same Internet connection. Local networks also provide easier connection between your devices, like sharing a printer, files or connecting to your smart TV or other smart devices.

Network cards display information such as IP addresses, gateways, netmasks and members - the interfaces that belong to that network. IPv4 and IPv6 information, whenever applicable, is displayed in separate tabs, as well as throughput graphs for that network.

The **Members** section in cards shows interfaces that are added to the network (zone). Only the networks that have at least one interface added to them will be active and displayed.

ARP entries (Address Resolution Protocol) and **DHCP active leases** (Dynamic Host Configuration Protocol) tables are also displayed in the page.

Figure 9 – Network information page

Network information:

Internet IPv4 Throughput

Address: 192.168.101.86 Gateway: 192.168.101.1

Netmask: 255.255.254.0 Members: 1 Member ▼

Local Network IPv4 IPv6 Throughput

Address: 192.168.2.1 Members: 3 Members ▼

Netmask: 255.255.255.0

OpenVPN IPv4 Throughput Logs

Address: 10.8.2.10 Gateway: -

Netmask: 255.255.255.0

ARP entries:

Items per page: 10 Search ×

IP address ⌵	MAC address ⌵	Interface ⌵
192.168.101.1	E4:8D:8C:25:51:02	Ethernet 0
192.168.2.236	BE:22:58:D8:69:F6 ⓘ	Local Network
192.168.2.5	00:E0:4C:68:A8:62	Local Network

Total entries: 3 ⏪ < 1 > ⏩

DHCP active leases:

Items per page: 10 Search ×

IP address ⌵	MAC address ⌵	Hostname ⌵	Time left ⌵	Interface ⌵
192.168.2.236	BE:22:58:D8:69:F6 ⓘ	OnePlus-8T	23:51:31	Local Network

Total entries: 1 ⏪ < 1 > ⏩

Clients

The **Clients** information page displays general information about the newly connected clients. The Clients information page lists all the clients that are currently connected to your wireless network through an **Access point**.



Clients are all the devices that are connected to the board's wireless network (WiFi). Examples of WiFi clients can be smartphones, laptops, smart TVs, wireless speakers, printers and other smart devices.

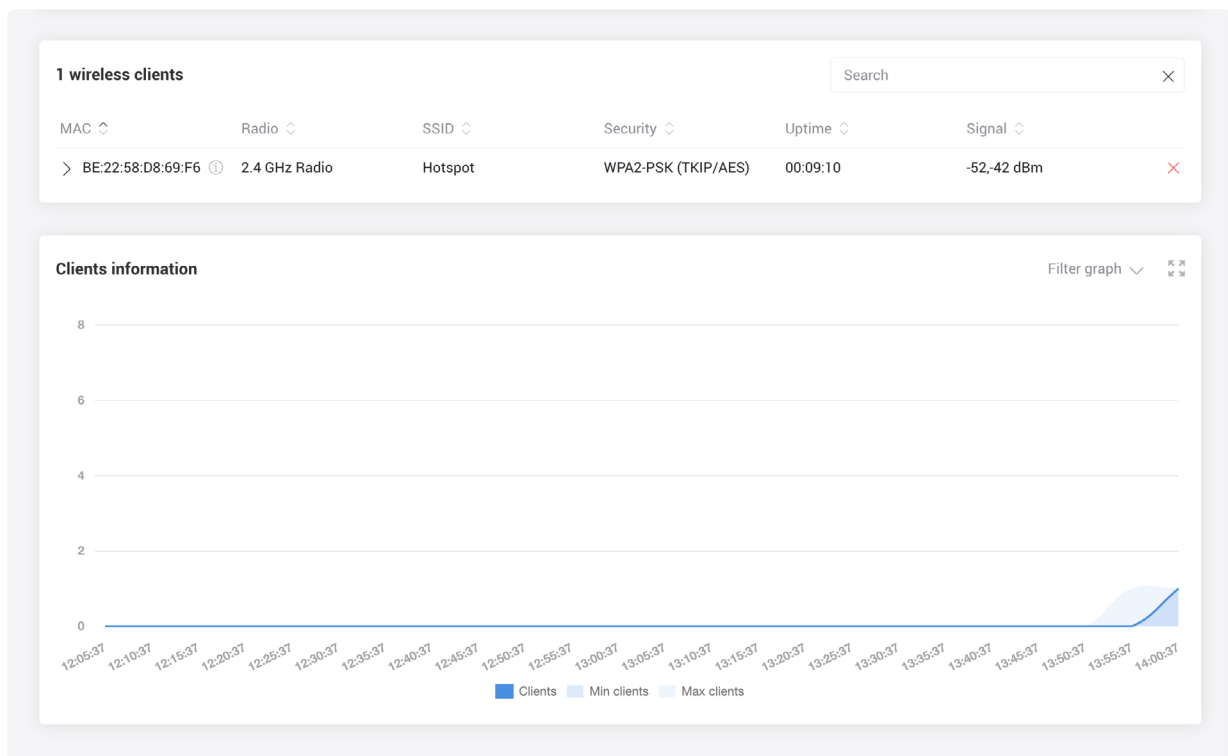
The Clients information page shows a list of all currently connected clients and their stats such as MAC address, uptime, signal strength, SSID, wireless radio frequency and security mode. Your Firmux board can have multiple WiFi networks created. Those networks usually have different network names (SSIDs) and passwords.

SSID (Service Set Identifier) is commonly referred to as a **wireless network name**. When you search for available WiFi networks on your computer or smartphone, you can see the list of nearby WiFi network names (SSIDs).



Each LAN network can have multiple SSIDs assigned (e.g. you can have a main WiFi network and a guest WiFi network in your home, with a different password and different wireless network name (SSID)).

Figure 10 – Clients information page

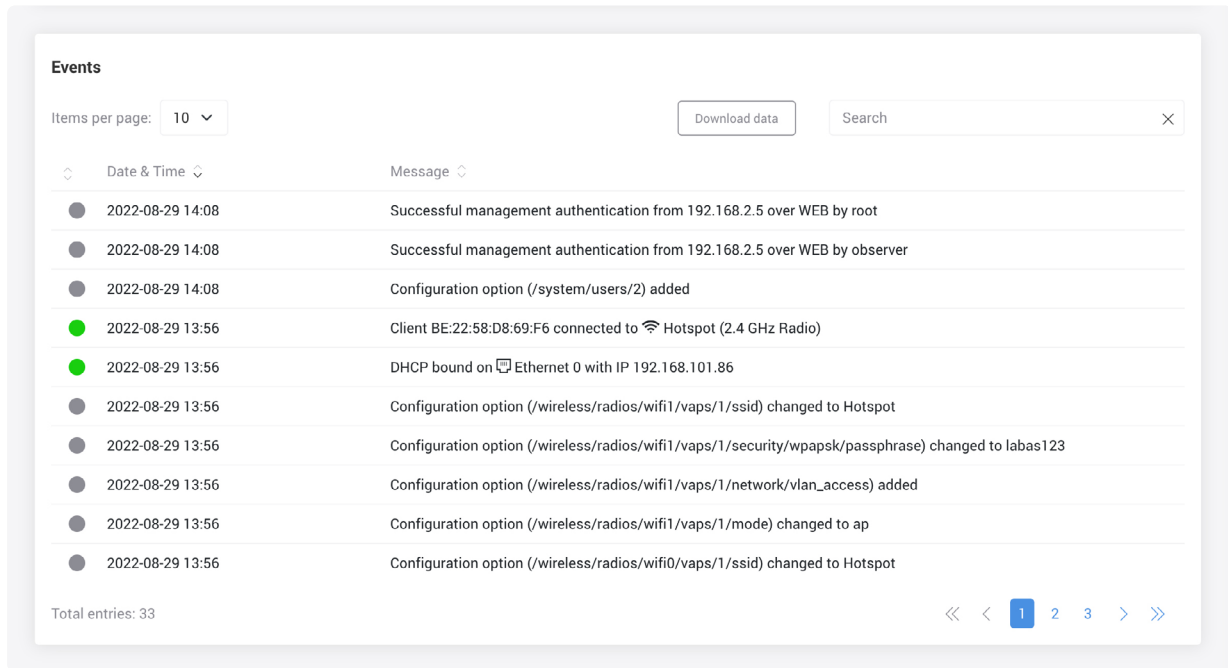


Advanced. Firmux boards allow you to create multiple WiFi networks, and those multiple WiFi networks can be added as interfaces to one or more LAN or WAN networks.

Activity

The Activity page provides a list of the most important device events that have happened since the Firmux device was started.

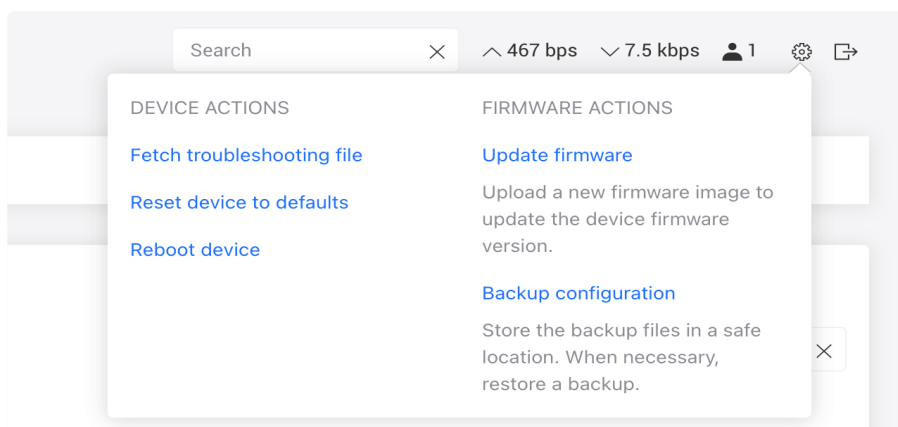
Figure 11 – Activity page



Maintenance

The maintenance menu can be accessed by clicking on the gear icon in the top right corner of the screen. The maintenance menu allows you to perform main system actions (reboot, restore configuration, etc.).

Figure 12 – Maintenance submenu



Upgrade firmware - allows you to upload a new firmware binary image file to upgrade firmware.

Backup configuration - allows you to download the current device configuration file or to upload a configuration file and thus restore device parameters to those saved in configuration file. The saved configuration file is useful to restore a configuration in case of device misconfiguration or to upload a standard configuration to multiple devices without the need manually configuring each device through the web interface.

Fetch troubleshooting file - allows you to download extensive device diagnostic (troubleshooting) file (diagnose_*.tar.gz archive), which may be useful when trying to find the cause of possible errors or malfunctions.

Reboot - reboot device with the last saved configuration.

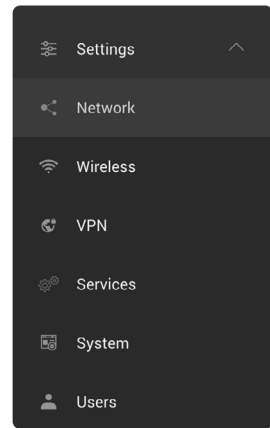
Reset device - click to restore the configuration of the device to default settings. This only restores the configuration of the device, but does not restore the firmware to previous versions.



Resetting the device is an irreversible process. The current configuration and the administrator name/password will be set back to the factory default.

Device Configuration

The device configuration settings are accessible by selecting **Settings** in the sidebar menu. Device configuration options are grouped into seven main categories (Network, Wireless, VPN, Mobile broadband, Services, System and Users), which are accessible via sidebar navigation menu. Each configuration page contains multiple options grouped by cards and tabs.



Network configuration page

Network configuration page allows you to configure, add or remove **LAN** and **WAN** networks. More advanced options allow you to configure **Ethernet ports**, **Static routes**, **Port forwarding rules**.

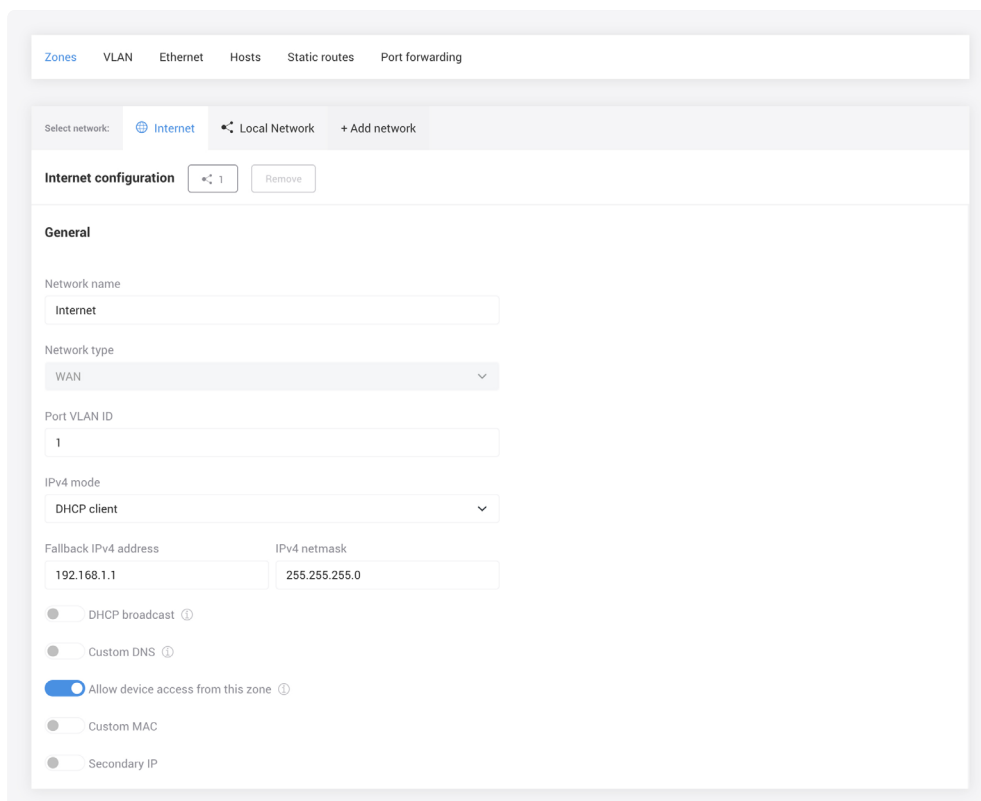
Two networks are created on Firmux boards by default - Internet and Local network:

Internet - the main **Wide Area Network (WAN)**, through which Firmux device is connected to the internet.

Local network - a **Local Area Network (LAN)**, that contains all the local devices in your home or organization which are connected to the Firmux board. The devices on your local network share the same Internet connection. Local networks also provide easier connection between your devices, like sharing a printer, files or connecting to your smart TV or other smart devices.

The two default LAN and WAN networks cannot be removed, but you can change their names and parameters. For more advanced configuration, you can create more additional LAN or WAN networks by clicking the “Add network” button and then selecting LAN or WAN **Network type**.

Figure 13 – Internet (WAN) settings



WAN configuration

Allows you to change and configure WAN network parameters. If DHCP client IPv4 mode is selected then the Firmux board will automatically configure itself with parameters provided by your Internet Service Provider (ISP).



Your Firmux board has one interface added to the default WAN network - Ethernet 0 port (which for simplicity we call WAN port). If the board has LTE support, then an additional WAN network would be present, containing the LTE interface.

IPv4 mode – specify whether the device will be manually configured (Static mode) or dynamically configured by the DHCP server of your ISP.

IP addresses can either be retrieved from a DHCP server of your ISP or configured manually:

- **Static IP** mode – the IP address, netmask and gateway must be specified manually.
- **DHCP client** mode – DHCP server dynamically assigns an IP address and other network configuration parameters. Internet service providers usually support DHCP configuration for simplicity sake, so plugging ethernet cable to the board's WAN port would automatically set up all the necessary parameters.

Allow device access from WAN – when this option is selected, device WEB GUI and SSH would be accessible from both the internet and from LAN network by using its WAN IP address. If this option is not selected, then the WEB GUI and SSH would only be accessible from the LAN network. In order to reach Firmux GUI from the internet, you must have a **public IP address** provided by your ISP.

Default route metric – this option is only available when **multiple WAN networks** are created. The route metric allows you to prioritize WAN networks, where 0 is the highest priority. When multiple WAN networks are Active (connected and configured), then the one with highest priority would be considered the mainnetwork, while the other networks would be classed as backup.

DHCP client mode

In **DHCP client mode**, the IP address for this device will be assigned from the DHCP server. You can access WEB GUI (Graphical User Interface) by typing that IP address into the web browser's address bar.

If a DHCP server is not available, or the board fails to receive dynamic IP from the DHCP server, the **Fallback IP** address will be used. You can access the board's WEB GUI by using this address. By default, Fallback IP is **192.168.1.1**. To access the board by this address, connect your computer via ethernet cable to the board's WAN port, and manually configure your computer to use **192.168.1.254** IP address on its ethernet port.

Static IP mode

Static IP mode can be selected when the DHCP server is not available, or when you need a more advanced WAN configuration. In this case you have to manually enter the main network parameters, which would normally be assigned by the DHCP server.

IP address – specify an IP address for the device.

Netmask – specify a subnet mask for the device.

Gateway – specify a gateway address for the device.

DNS servers – specify one or two DNS addresses.

Secondary IPs – specify IPv4 and IPv6 secondary IP addresses.

Figure 14 – Static IP mode of WAN network

The screenshot displays the configuration page for a WAN network. At the top, 'Network type' is set to 'WAN'. Below it, 'Port VLAN ID' is set to '1'. The 'IPv4 mode' is set to 'Static'. There is an unchecked 'Custom MAC' option. The 'IPv4' section is enabled and contains the following fields: IP address (192.168.1.1), Netmask (255.255.255.0), Gateway (192.168.1.254), and two empty DNS servers fields. A 'Secondary IP' option is also present and unchecked. The 'IPv6' section is disabled.

LAN configuration

By default Firmux boards have one Local Area Network (LAN) created. The default LAN network has a name “Local Network”, which you can change. This network cannot be removed, but its parameters can be changed.

By definition a local area network (LAN) is a computer network that interconnects computers in one physical location such as a building, office or home.



Firmux boards have two or three interfaces added to the default LAN network - Ethernet 1 port (which we call LAN port) and a wireless radio interface, or two radio interfaces if the board supports dual-band wireless operation (2.4 GHz and 5 GHz).



Advanced. Wireless radio interfaces cannot be directly added to networks – rather they are added by creating SSIDs – WiFi networks with separate names and passwords – and then selecting which LAN or WAN network that SSID will be added to.

For more advanced configuration, you can create more LAN networks by clicking “Add network” button and then selecting the LAN **network type**.

Figure 15 – LAN network configuration

Local Network configuration ◀ 3 Remove

General

Network name
Local Network

Network type
LAN

Port VLAN ID
1

Custom MAC

Isolate network

IPv4

Enabled

IP address: 192.168.2.1 Netmask: 255.255.255.0

DHCP server

IP range from: 192.168.2.2 IP range to: 192.168.2.254

DHCP lease time: 1 day

Secondary IP

IPv6

Enabled

IP address: 2001::3 Prefix: 64

Secondary IP

Static DHCP leases + Add

Name	IP address	MAC	Status
No static leases configured			

The default local network has 192.168.2.1 IP address configured on the board.

This network has Ethernet 1 port interface added by default. A WiFi network with default SSID name “firmux” is also selected as an interface to this network zone.

If you connect your computer via ethernet cable to this Ethernet 1 port, or if you connect to “firmux” WiFi network, then you can reach WEB GUI by typing **192.168.2.1** into the address bar of your web browser.

The default password of this WiFi “firmux” network is “**passphrase**”. You can change this wireless network name and password as explained in the SSID section of this user guide. This LAN network has a DHCP server running on board, so whenever you connect your computer or another smart device to this network (by Ethernet 1 port or WiFi network), that device will receive a dynamic IP address in range 192.168.2.2–192.168.2.254.

- **IP address** – device IP address in LAN network (**default 192.168.2.1**).
- **DHCP server** – enable a built-in DHCP server, that provides an IP addresses for your devices connected over Wireless and Wired interfaces via LAN (interface).
- **IP address from** – specify the starting IP address of the DHCP address pool.
- **IP address to** – specify the ending IP address of the DHCP address pool.
- **Lease time** – specify the expiration time for the IP address assigned by the DHCP server.



Click **Add** to add additional LAN networks, each of the networks must have a different IP address range.

Secondary IP

The secondary IP is available in static and DHCP modes. Secondary IP is used when we want to add additional IP addresses to the same zone. In order to use it you will have to enable it by switching Secondary IP toggle.

Figure 16 – Secondary address

Secondary IPv4 addresses + Add

IP address	Netmask	
192.168.3.1	255.255.255.0	✕
192.168.4.1	255.255.255.0	✕



Click **Add** to add secondary IP and then enter IP address and netmask.

DHCP server

The Dynamic Host Configuration Protocol (DHCP) server dynamically assigns an IP address and other network configuration parameters to each device (client) on the network, so they can communicate with each other, and with other IP networks.



This LAN network has a **DHCP** server running on board, so whenever your computer or another smart device connects to this network via ethernet cable or WiFi, that **device will receive a dynamic IP address in range 192.168.2.2–192.168.2.254**.

For this to work your smart devices must have the "Automatic DHCP" IP method selected. This is usually the default option, especially when connecting to a WiFi network.

Static DHCP lease – if you want your smart device (client) to have the same IP address assigned every time it connects to this LAN network, then you can add a Static DHCP lease. For this you must know a MAC address of your device – a unique hardware identifier, that all network devices have.

Figure 17 – Static DHCP leases

Static DHCP leases + Add

Name	IP address	MAC	Status
Laptop	192.168.2.2	1C:1B:B5:41:B5:FE	<input checked="" type="checkbox"/> ✕
Smartphone	192.168.2.3	C4:93:00:1D:B6:09	<input checked="" type="checkbox"/> ✕

You can usually find your smart devices **MAC** address in the **Network information page** of Firmux WEB GUI. The “DHCP active leases” table shows IP addresses assigned to all currently connected devices as well as their unique MAC addresses.

VLAN configuration

VLANs allow network administrators to group hosts together even if the hosts are not directly connected to the same network switch. Because VLAN membership can be configured through software, this can greatly simplify network design and deployment. Without VLANs, grouping hosts according to their resource needs the labor of relocating nodes or rewiring data links.

Figure 18 – VLAN configuration

Select VLAN: IPTV + Add VLAN

IPTV configuration Remove

General

Name: IPTV

VLAN ID: 6

Management

Enabled

Access interfaces must be removed before enabling management

Interfaces Edit

Interface	Mode	Type
firmux	Trunk	Wireless
AP	Access	Wireless

The **VLAN configuration** page lets you assign VLAN IDs to a trunk and access interfaces (ethernet and wireless) by clicking on the Interface edit button, then selected interfaces are represented on the table.

Figure 19 – Management VLAN configuration

Management

Enabled

Use address: IPv4 IPv6

IPv4 address: 192.168.12.1

IPv4 netmask: 255.255.255.0

IPv6 address: 2001:4860:4860::8888

IPv6 Prefix: 64

You can also set up management VLAN by specifying IPv4 - IPv6 addresses

Ethernet configuration

Figure 20 – Ethernet port configuration

Ethernet configuration

Ethernet 0

Enabled

Auto-negotiation

Network zone

Internet ▼

VLAN

VLAN pass-through

Access VLAN

None ▼

Trunk VLAN

✓ IPTV (6)

Ethernet 1

Enabled

Auto-negotiation

Network zone

Local Network ▼

VLAN

VLAN pass-through

The **Ethernet configuration** page lets you assign ethernet interfaces to specific LAN or WAN networks. You can also assign a trunk and access VLANs or you can enable VLAN pass-through.



Trunk and access VLANs can also be selected in the VLAN page.

Default ethernet port settings

Interface	Ethernet 0	Ethernet 1
Network name	Internet	Local Network
Network type	WAN	LAN



Disabling Ethernet ports or changing networks to which ethernet interfaces are added may leave your Firmux board inaccessible for administration.

Auto-negotiation – when switched on (default), the board will automatically recognize ethernet line speed and duplex mode.

Fixed speed – parameter is available when auto-negotiation is off. Allows you to select the preferred line speed and duplex mode.

Hosts configuration

Local DNS hosts

This feature allows users to configure and create custom names for local network hosts, so that they could be accessed with the specified host name.

Figure 21 – LocalDNS hosts

Local DNS hosts

This feature allows to configure and create custom names for local network hosts, so that they could be accessed by using a domain name.

Enabled

Host name	IP address
<input type="text" value="firmux.com"/>	<input type="text" value="192.168.2.1"/> <input type="button" value="X"/>

DNS Blackhole

DNS blackhole is used to spoof DNS servers to prevent resolving hostnames of specified URLs.

Figure 22 – DNS blackhole

DNS Blackhole

DNS blackhole is used to spoof DNS servers to prevent resolving hostnames of specified URLs.

Enabled

Blocked host

<input type="text" value="google.com"/> <input type="button" value="X"/>
--

Ad Block

Ad block is used to block ads, malicious websites, websites that are not suitable for specific audiences (eg. schools, organizations).

In order to use Ad block you need to add a block list URL.

Figure 23 – Ad Block

Ad Block

Host-based ad blocking via DNS

Enabled

Status	List URL
<input checked="" type="checkbox"/>	<input type="text" value="https://raw.githubusercontent.com/kboghady/youTube_ads_4_pi-hole/master/youtubelist.txt"/> <input type="button" value="X"/>
<input checked="" type="checkbox"/>	<input type="text" value="https://raw.githubusercontent.com/oneoffdallas/dohservers/master/list.txt"/> <input type="button" value="X"/>
<input checked="" type="checkbox"/>	<input type="text" value="https://raw.githubusercontent.com/Sekhan/TheGreatWall/master/TheGreatWall.txt"/> <input type="button" value="X"/>

Static routes configuration

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from dynamic routing traffic. Static routes are manually configured by adding entries into a routing table. Unlike dynamic routing, static routes are fixed and do not change if the network is changed or reconfigured. Static routing and dynamic routing are not mutually exclusive. Both dynamic routing and static routing are usually used on a router to maximize routing efficiency and to provide backups in case dynamic routing information fails to be exchanged. Static routing can also be used in stub networks, or to provide a gateway of last resort.

You can add a static route by clicking the “+ Add” button and then entering all required fields.

Figure 24 – Static routes

Route name	Network	Subnet mask	Gateway	
New route	2.2.2.0	255.255.255.0	1.1.1.1	✕
New route 1	2.2.3.0	255.255.255.0	1.1.1.1	✕

Port forwarding configuration

Port forwarding or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway. This technique is most commonly used to make services on a host residing on a protected or masqueraded (internal) network available to hosts on the opposite side of the gateway (external network), by remapping the destination IP address and port number of the communication to an internal host.

Figure 25 – Static routes

Rule name	Port	Protocol	Destination IP address	Destination port	LAN access	Status
New rule	25	TCP	192.168.101.51	2	<input type="checkbox"/>	<input checked="" type="checkbox"/> ✕
New rule 1	50	TCP	192.168.61.1	2	<input type="checkbox"/>	<input checked="" type="checkbox"/> ✕

VPN configuration

WireGuard® configuration

WireGuard® is a free and open-source software application and communication protocol that implements virtual private network (VPN) techniques to create secure point-to-point connections in routed or bridged configurations.

Figure 26 – WireGuard® Server mode configuration

The screenshot shows the WireGuard configuration interface. It is divided into three main sections: General, Interface, and Peers. The General section includes fields for Network name (Wireguard), Mode (Server), Port (51820), Private key (with a generate button), and Public key (gPrxPRDZdrjDFMwW5daWBj+YDI5PNE9gyInuvX2f6HA=). The Interface section includes IP address (192.168.200.1), Netmask (255.255.255.0), NAT (checked), WAN (checked), Gateway (192.168.200.254), and Default route metric (1). The Peers section has a table with columns for Public key, Persistent keepalive, and Allowed IP, and a '+ Add' button. One peer is listed with Public key KjaAbfPPfxLZDvWx785iE3GL1I8zSda2iO1kDinW3ks=, Persistent keepalive 0, and Allowed IP 192.168.200.5.

Server mode – server must have a public IP address (or an IP address otherwise reachable by the client).

- Network name - A given name for this particular WireGuard® configuration.
- Port – specify the port on which the WireGuard® connection will work (default 51820).
- Public and private key – click the generate button next to the private key field to generate both private and public keys.
 - Private key – should be kept secret, it is used for public key generation.
 - Public key – you will need to enter this public key in the WireGuard® configuration on the client side. Click a “generate” button next to the private key field to generate both keys.
- IP address – specify the WireGuard® IP address of the server. Server and client WireGuard® IP addresses must be on the same network.
- Netmask – specify the netmask that determines the size of the WireGuard® network.
- NAT - Used to enable NAT on the WireGuard® network.
- WAN - Used to treat the WireGuard® network as a WAN zone (eg. can be used to route a LAN zone through WireGuard® configuration).
 - Gateway - specify a gateway address.
 - Default Route Metric - set the priority of this WAN network for the device.
- WireGuard® peers – enter the peer (client) details for every client you want to be able to use the WireGuard® protocol.
 - Public key – specify the peer public key, which is generated on the client side.
 - Persistent keepalive – when enabled, a keepalive packet is sent to the client with specified interval in seconds. Setting it to 0 turns the feature off (default).
 - Allowed IP – specifies the IP address that this client is allowed to use.

Figure 27 – WireGuard® Client mode configuration

The screenshot shows the WireGuard configuration interface with the following fields and values:

- General:**
 - Network name: Wireguard
 - Mode: Client
 - Port: 51820
 - Private key: [Redacted]
 - Public key: BmfG+Qsl3pjNl8Sr1ATV02M2QkbiaG4pLmaS4NAsIRM=
- Interface:**
 - IP address: 192.168.200.1
 - Netmask: 255.255.255.0
 - NAT:
 - WAN:
- Server:**
 - Address: 192.168.4.1
 - Port: 51820
 - Public key: JRmws0ZW8Ext6skUgxfokhyPeCSP4s0mUFYhz
 - Persistent keepalive: 0

Client mode – client uses a WireGuard® server to establish and maintain the secure connection.

- Network name - A given name for this particular WireGuard® configuration.
- Port – specify the port on which the WireGuard® connection will work (default 51820).
- Public and private key – click the generate button next to the private key field to generate both private and public keys.
 - Private key – should be kept secret, it is used by the WireGuard® to generate a public key.
 - Public key – you will need to enter this public key in the WireGuard® server configuration. This key allows the WireGuard® to encrypt and decrypt information on the client-server connection. Click a “generate” button next to the private key field to generate both keys.
- Server address – enter the **public IP address** of the server (this public IP address is not the same as WireGuard® IP address; public IP address is the actual IP address by which server is reachable by the client).
- Server port – enter the same port as is configured on the server side (default 51820).
- Public key – specify the server public key, which is generated on the server side.
- Persistent keepalive – when enabled, a keepalive packet is sent to the server with a specified interval in seconds. Setting it to 0 turns the feature off (default)
- IP address – specify the WireGuard® IP address of the client. Client WireGuard® IP addresses must be on the same network as the server WireGuard® IP.
- Netmask – specify the netmask that determines the size of the WireGuard® network.
- NAT - Used to enable NAT on the WireGuard® network.
- WAN - Used to treat the WireGuard® network as a WAN zone (eg. can be used to route a LAN zone through WireGuard® configuration).
 - Gateway - specify a gateway address.
 - Default Route Metric - set the priority of this WAN network for the device

ZeroTier® configuration¹

ZeroTier® is a popular VPN platform for creating secure private networks. It helps safely connect to your machines from anywhere in the world and safely access servers in the cloud. It enables intranet applications for external users.

Figure 29 ZeroTier® configuration page

ZeroTier®
Creates secure, manageable networks and treat connected devices as though they're in the same physical location. Enabled

Port
9993

Networks

	Network ID	Comment
<input checked="" type="checkbox"/>	sssi7hihb73121	

- Port - select the port to use this service on (default 9993).
- Networks - ZeroTier® networks that this device is apart of.
 - Network ID - Specify the ID that is given by the ZeroTier® network management platform.
 - Comment - an optional comment regarding the specific network.

¹ This feature only works on Mango based boards.

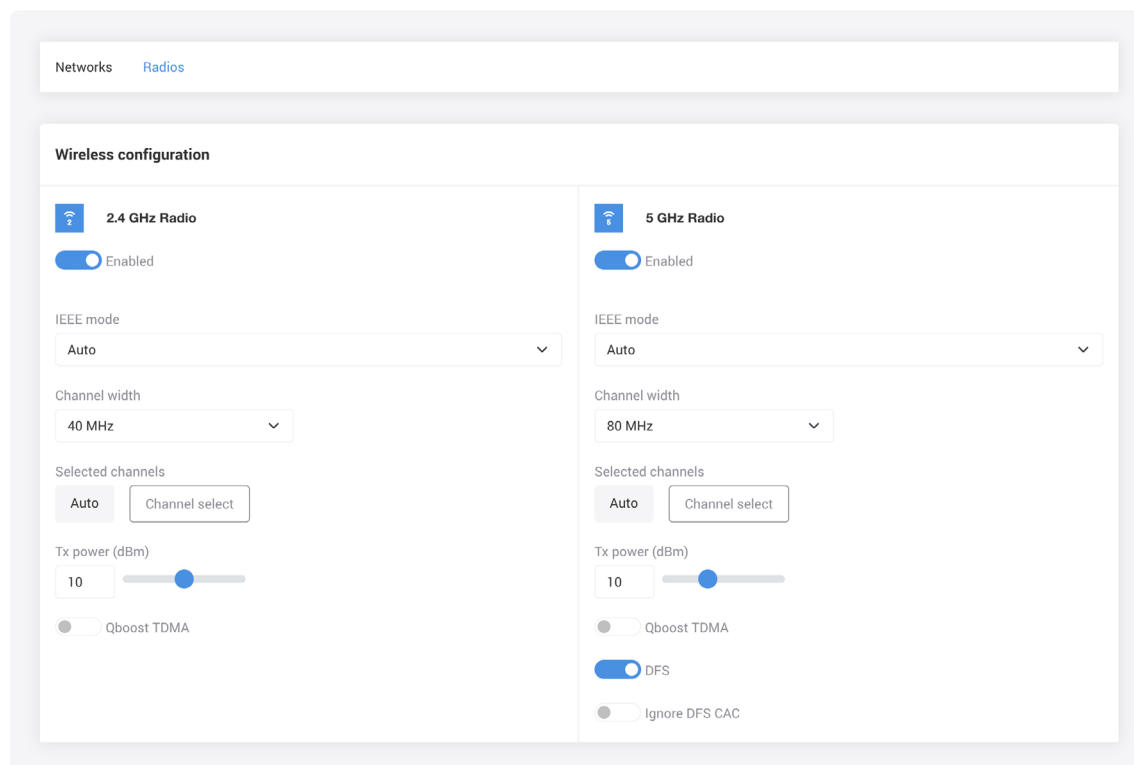
Wireless radio configuration

The **Radio tab** in the **Wireless configuration** page allows the user to control the wireless interfaces of the device. Depending on the device module, there might be one or more wireless radio interfaces.



Single-band boards have a 2.4 GHz wireless interface. Dual-band boards have 2.4 GHz, 5 GHz and or 60 GHz radio interfaces. Some non-concurrent boards have a joint 2.4 / 5 GHz wireless interface. If your board has LTE support, then it will also have a LTE interface under wireless settings.

Figure 30 – Wireless configuration page



Every radio has a toggle **On/Off** switch that enables or disables specific radio.

Channel width – select the maximum width of the operating radio channel. The device 5 GHz radio device typically supports channel widths of 20 MHz, 40 MHz and 80 MHz; the 2.4 GHz radio typically supports channel widths of 20 MHz and 40 MHz. When you select higher channel width, the device will be able to overlap its channels – this may increase the data transfer rate.

Channel – select the channel at which the access point will be operating. Auto channel selection is the default option. When automatic channel selection is enabled, the board will attempt to choose the best channel, based on the surrounding network usage and interference. Channel selection can influence the WiFi coverage and performance. You can also select multiple channels on which the board will operate.



Some boards have a **Spectral scan** tool, which allows you to diagnose what radio frequencies are used the most in the surrounding area. This may be usable when deciding which wireless channel to select. Spectral scan tool is available in **Settings -> Tools -> Spectral scan**.

Tx power (dBm) – the unit’s transmitting power at which the device will transmit the data. Changing this option will affect the strength of the signal that radio produces during transmission. The higher Tx power may extend the operation range of the wireless network, but lowering Tx power reduces interferences, especially when other wireless devices operate nearby. The maximum transmit power permitted varies by country in which the device is operating.

Qboost TDMA – proprietary Qualcomm wireless communication protocol that leverages Time Division Multiple Access (TDMA) to improve link performance. All connected peers must support Qboost and it must be enabled for it to work correctly.

DFS – Dynamic Frequency Selection (DFS) is a channel allocation scheme designed to prevent electromagnetic interference with other critical infrastructure (such as radars). Enabling this feature will allow your Firmux board to dynamically select and use those reserved channels whenever there is no activity at that frequency.

Wireless network configuration



SSID (Service Set Identifier) is commonly referred to as a **wireless network name**. When you search for available WiFi networks on your computer or smartphone, you can see the list of nearby WiFi network names (SSIDs).

Whenever you want to create a WiFi network you must take three main steps:

1. Create a LAN or WAN network (*Settings -> Network*).
2. Enable a wireless radio (*Settings -> Wireless -> Radios*).
3. Add that radio interface to a LAN or WAN network by creating a SSID and selecting to which LAN or WAN network this interface will be added (*Settings -> Wireless -> Networks*).

Figure 31 – Wireless network configuration page

AP (Hotspot) configuration Remove

General

Mode
Access point

SSID
Hotspot

Hide SSID
 SSID is shown

Network zone
Local Network

VLAN
 VLAN pass-through

Access VLAN
None

Trunk VLAN
IPTV (6)

Enable on radio
 5 GHz Radio
 2.4 GHz Radio

Access Control List
 Disabled

Security

Mode
WPA2 personal

Passphrase
.....

Wireless networks can be set into either Access point or Station mode:

- **Access point (AP)** wireless mode allows you to create WiFi networks, to which other network devices – **clients** – can connect.
- **Station wireless mode** – when this mode is selected, the Firmux board itself will act as a wireless client, so it can connect other wireless networks (access points).



Clients are all the network devices that are connected to the board's wireless network (WiFi).

In the wireless network configuration page you also have the following options:

- **SSID** – the name of your WiFi network, that clients will be able to see and connect to.
- **Enable on radio** – select at least one radio frequency, and that radio frequency will be added to the WiFi network.
 - Multiple frequency options are available on dual-band concurrent Firmux boards.
 - Only the radios that are in Access point mode will be available.
- **Network zone** – select to which network that radio interface will be added.
 - If you select a **LAN network**, the clients connected to the WiFi network will be on that local network, and they will receive an IP address assigned by a DHCP server operating on the Firmux board (this option is recommended).
 - If DHCP service is disabled in LAN configuration, then the device will not be automatically assigned an IP address. In such a case, you must manually configure an IP address on your client device, and that IP must be on the same network.
 - All the client devices on the same LAN network will be able to communicate with each other easier.
 - If you select a **WAN network**, the clients will receive an IP address assigned by your ISP (internet service provider).
 - This option will only work if your ISP provides multiple IP addresses for you. Contact your ISP to ask if this option is available.
 - The client devices on the WAN network will have a restricted access to devices on your LAN networks.
 - Also you can assign a trunk and access VLANs or you can enable VLAN pass-through.



Trunk and access VLANs can also be selected in the VLAN page.



Firmux boards allow you to have multiple SSIDs added to the same LAN network, or to separate LAN networks. If you plan to create a **Guest WiFi network**, you should always create a separate LAN network for security purposes. That way guest clients will have restricted access to the main LAN network devices.

Wireless network security options

When creating a new wireless network, you must select one of the available security modes for your access point:

- **Open** – the WiFi network will not require any authentication. The data transferred will not be encrypted – anyone within the range of a signal will be able to connect to a network. The data transferred wirelessly could be captured and read by third parties.
- **WPA2 or WPA3 personal** – the network will be protected by a password (passphrase). Other users will need to know this password in order to join the network. The data transferred will be encrypted and much more difficult to access by third parties. This security mode is also known as **WPA2-PSK (WPA3-PSK)** (pre-shared key).
- **WPA2 or WPA3 enterprise** – this is an advanced security mode, mainly used in enterprise networks. This security mode requires the use of authentication servers to ensure advanced protection of the data and network. This security mode is also known as **WPA2 (WPA3)**.

Access point wireless mode

When your Firmux board is in **Access point** (AP) wireless mode, you can create multiple WiFi networks, and wireless clients can connect to those networks.

One firmux board can have multiple WiFi networks created. This is done by creating SSIDs. For simplicity reasons, the term “**wireless network name**” is often used instead of the SSID term.

SSID stands for “Service Set Identifier” and is a unique identifier of any WiFi network. This allows wireless devices to uniquely identify each other.

You create a custom name for your WiFi network and that name will be visible to other nearby WiFi devices. User-created wireless network names doesn’t have to be unique and can have duplications, but SSID ensures that all network devices can uniquely identify each other,

In other words, smartphone users scanning for available WiFi networks will simply see a list of network names, but their smartphones will also see unique BSSIDs for available WiFi networks.

Data packets transferred over a wireless network always include the SSIDs. This ensures that data sent over the air is received by the correct device.

Separate WiFi networks are created by choosing a unique network name (SSID) and assigning it to a LAN network, in most general cases.



LAN settings are described in the **Network configuration** section of this guide.

Station wireless mode

When you select a **Station** wireless mode, your Firmux board itself can act as a wireless client, so it can connect to other wireless network SSIDs (access points). Station mode can be enabled separately for each wireless radio.

The Station wireless radio **interface** must be added as a member to one of the networks created on this Firmux board, either LAN or WAN:

- If you add the Station interface to a WAN network, then it will act similarly to an ethernet cable connected to a WAN ethernet port – you can connect to other access points that are sharing an internet connection. You can use such connection instead of an ethernet cable, or you can create multiple WAN networks on the board and have them as main / backup internet sources.
- If you add the Station interface to a LAN network, it can extend the LAN network of the access point (of the device that your station is connected to).

Figure 32 – Station configuration

The screenshot shows the 'Station configuration' interface. At the top, there is a 'Station configuration' header with a 'Remove' button. Below this is the 'General' section, which includes a 'Mode' dropdown menu set to 'Station', and two toggle switches for 'Enable on radio' for '5 GHz Radio' and '2.4 GHz Radio', both of which are turned on. The interface is split into two columns for '5 GHz Radio' and '2.4 GHz Radio'. Each column contains fields for 'SSID' (with a 'Scan' button), a 'Lock AP MAC' toggle, 'Security mode' (set to 'WPA2 personal'), 'Passphrase' (masked with dots), and 'Network zone' (set to 'Local Network').



Dual-band concurrent Firmux boards can have one radio frequency operating in Station mode, and the other frequency operating in Access point wireless mode. This allows your board to wirelessly connect to an internet source, and at the same time share network and internet to multiple WiFi client devices.

SSID – specify the wireless network name of the access point you want to connect to. The easiest way to do so is by clicking the Scan button next to the SSID field and picking a desired WiFi network to which you want to connect.

Scan feature – allows you to easily choose an access point from the list of available WiFi networks. After clicking the Scan button, the Firmux board will start looking for advertised network SSIDs in the surrounding area. Click the Select button to choose a desired access point SSID.

The list of available access points is arranged by SSID / (wireless network name), but you can change the order by clicking on the header of a respective column, or by using the Search field to filter results:

- **SSID** – the name of the wireless network. SSIDs are not always unique.
- **BSSID** – usually a unique network identifier that generally matches the **MAC address** of the access point radio.
- **Channel** – displays current channel of access point, its frequency and channel width.
- **Signal** – received signal strength (in dBm – decibels relative to a milliwatt). Numbers closer to zero mean the signal is stronger, that is **-40 dBm is better than -60 dBm**.
- **Security** – displays the **security mode** of available access points:
 - **Open** – insecure network, the data transferred is not encrypted – anyone within range of a signal can connect to a network, the data transferred wirelessly can be captured and read by third parties.
 - **WPA2-PSK** (pre-shared key) – password-protected encrypted network – it can be accessed by anyone provided they know a pre-shared key and are within range of the signal. Data transferred is encrypted and cannot be read by third parties without a key. This security mode is also known as **WPA2 Personal**.
 - **WPA2** – this mode is designed for enterprise networks and uses authentication servers. This security mode is also known as **WPA2 Enterprise**.

Figure 33 – Scan access points feature

SSID	BSSID	Channel	Signal	Security	
TechZity_Open	C8:08:73:15:2A:28	11 (2462 MHz), 20 MHz	-2 dBm	Open	Select
OnePlus 8T	42:7E:82:D4:6C:55	11 (2462 MHz), 20 MHz	-47 dBm	WPA2-PSK	Select
8devices-psk	00:16:16:2B:94:FD	11 (2462 MHz), 40 MHz	-63 dBm	WPA2-PSK	Select
TechZity_Community	C8:08:73:55:2A:28	11 (2462 MHz), 20 MHz	-66 dBm	WPA2-PSK	Select
8devices-psk	C4:93:00:1D:B7:DD	1 (2412 MHz), 40 MHz	-86 dBm	WPA2-PSK	Select
4G-Gateway-942A66	D4:72:26:94:2A:66	6 (2437 MHz), 20 MHz	-89 dBm	WPA2-PSK	Select
8devices-psk	28:76:10:0B:EB:06	5 (2432 MHz), 40 MHz	-89 dBm	WPA2-PSK	Select
CGTrader	8C:FE:74:1D:C7:88	11 (2462 MHz), 20 MHz	-90 dBm	WPA2-PSK	Select
8devices-psk	28:76:10:0B:EE:92	5 (2432 MHz), 20 MHz	-90 dBm	WPA2-PSK	Select
8devices	CA:93:00:1D:B7:DD	1 (2412 MHz), 40 MHz	-92 dBm	WPA2	Select

Lock AP MAC – allows the Station to be locked to the specified Access Point (AP) MAC address (BSSID). The available SSIDs can sometimes be the same for multiple access points. This means that your board may connect to other WiFi networks with the same name if their signal strength is better. If you want to avoid this, you should enable the “Lock AP MAC” feature and specify the MAC address of the desired access point. This address will be automatically entered if you use the SSID Scan feature to select a network.

System configuration

The System configuration page allows you to manage the main settings like device location, device name, hostname, time and country.

Figure 34 – System configuration page

The screenshot shows the 'System configuration' page with the following sections:

- Device information:** Fields for Device name (Jalapeno), Device location (Office), Country (Lithuania), and Hostname (firmux).
- Time settings:** Time zone dropdown (UTC+2 Europe/Vilnius), Date selector (2022-08-25), and Time selector (18:15). A 'Set current time' button is also present.
- Automatic firmware update:** A toggle switch for 'Check for firmware updates' which is currently turned off.
- Other settings:** A toggle switch for 'Physical reset button' which is currently turned on.

Country and time settings

Country – select the country in which your Firmux device is located. Different countries / regions have **different regulations for wireless radio usage**. It is important to select your actual country, so your Firmux device will comply with those regulations.

You can click the **Set current time** button to automatically set the Time zone, Date and Time. Those parameters will be retrieved from the settings of your web browser.

If any of those fields are incorrect, you can select the actual values manually from the **Time zone** dropdown, and from the **Date** and **Time** selectors.

Device name, location and hostname

The information you enter in the three textual fields describing your Firmux board will be visible to you and to other connected network devices. Device discovery services, if enabled, broadcast those fields to other devices (*Settings -> Services -> Device discovery*). This information will also be visible to you in the device *Dashboard*, for easier identification.

Figure 35 – Device location, name and hostname fields

Device information

Device name

Device location

Country

Hostname

- Device name – specify a name that describes this device. This name will be visible in your browser's title when viewing WEB GUI. This name will also be broadcasted by Device discovery service (LLDP, CDP or MNDP).
- Hostname – specify unique identifier of the device, other devices may be able to see this information. This name will be visible when using SSH or serial connection to manage the device. You will also see hostnames of devices in the “*DHCP active leases*” table in the *Network information* page.
- Device location – specify the physical location of the device, this is useful when managing networks with multiple devices. This field will also be broadcasted by Device discovery service (LLDP, CDP or MNDP).

Figure 36 – Device information card in dashboard

Device information

Info **Firmware**

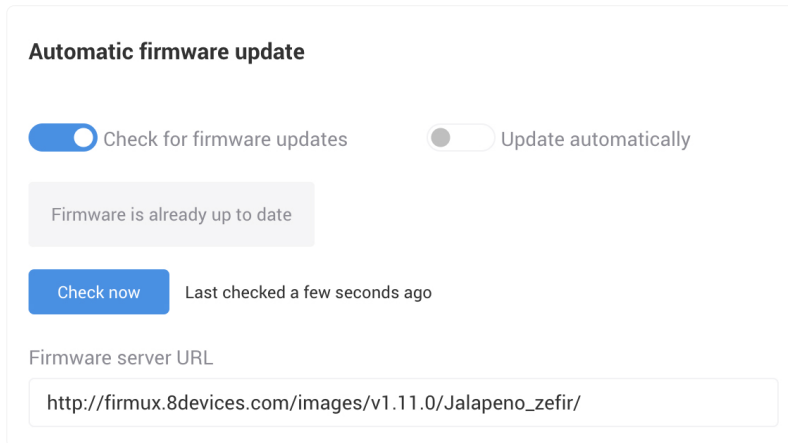
Name:	Uptime:
Jalapeno	00:03:31
Location:	Device Time:
Kitchen	2022/09/07 10:35:14
MAC:	
C4:93:00:1A:DA:8D	
Hostname:	
firmux	

Automatic update checker

With the automatic update functionality, your firmux board is able to periodically check for newer firmware versions. Whenever new firmware is available on the server, your firmux WEB GUI will display you a notification to update the firmware.

You will be able to choose to update immediately, postpone the notification or trigger the update manually.

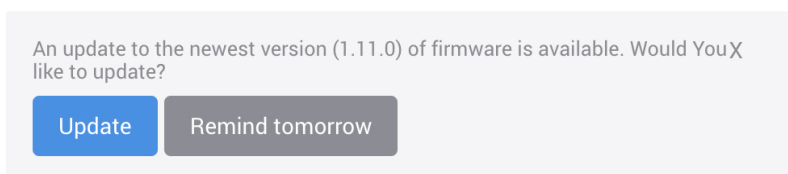
Figure 37 – Automatic update checker



To enable the automatic update checker, you must have a link to the update server. Server should contain the binary update files, and a textual firmwares.json file, which holds information about the most recent firmware version. Automatic update checker periodically compares your board's current firmware version with the one on the server, and informs you whenever a newer version is available.

- Check for firmware updates – enable if you want automatic update checks and notifications to be performed.
- Update automatically – when this is enabled, Firmux will automatically update (without notifying the user) when new firmware is available.
- “Check now” button – click if you want Firmux to check for an update at that moment.
- Firmware server URL – specify the server address where new firmware is published.
- Update button – this button will appear when a new update is available on the server.
 - You will be notified by a popover dialog about the option to update. You can either click the “Update” button in the popover, or update later in the *System configuration* page.

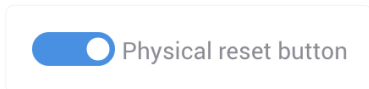
Figure 38 – Update notification dialog



Physical reset button

If your Firmux board has a physical reset button, there will be an option to enable or disable the functioning of this button.

Figure 39 – Physical reset button



Services configuration

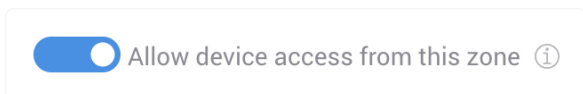
Remote management

Your Firmux board provides multiple management options: WEB GUI through HTTP service, console management via SSH or serial or Telnet connection.



If you want your device WEB GUI and SSH to be accessible by the WAN IP address, you must leave the “**Allow device access from WAN**” option enabled in the *Network configuration page* -> *WAN settings*. Otherwise the device will be accessible only by LAN IP address.

Figure 40 – Allow device access from WAN option in *Network configuration page*

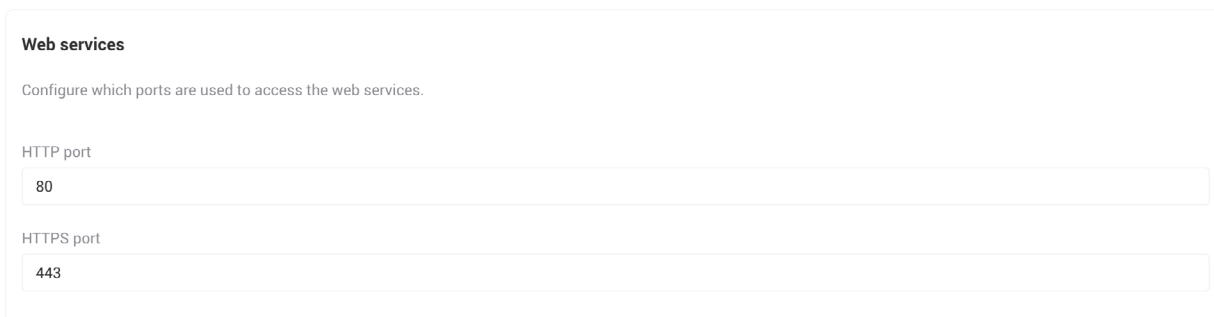


HTTP

HTTP management (WEB GUI) is always switched on. You can manage ports if needed.

- **HTTP port** – for HTTP connections web browsers use port 80 by default.
- **HTTPS port** – for secure HTTPS connections web browsers use port 443 by default.

Figure 41 – HTTP service configuration

A screenshot of a configuration page titled "Web services". It contains a sub-header "Web services" and a descriptive text: "Configure which ports are used to access the web services." Below this, there are two input fields: "HTTP port" with the value "80" and "HTTPS port" with the value "443".

Default HTTP options

Enabled	Yes (always)
Port	80
HTTPS port	443
Hostname	Device IP address

SSH

Secure Shell (**SSH**) is a cryptographic network protocol for administering network services securely over an otherwise unsecured network. This allows you to remotely manage and control your Firmux board using a shell (console).

Figure 42 – SSH service configuration

SSH

The Secure Shell Protocol (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network.

Enabled

Port

Password login ⓘ

To use SSH connection for device management, the Firmux board must be accessible by its IP address from the computer that you are using to connect to the board.

To connect via SSH you will either need to provide the username and password of an Admin level user, or add an SSH key in the Users configuration page. The Firmux by default has one Admin level user (“root”), and you can create more users in **Settings -> Users** configuration page. If the password login option is disabled, you can only access SSH by using an SSH key.

Default SSH options

Enabled	Yes (always)
Port	80
Password login	443

SSH connection parameters

Hostname	Device IP address (same that you use to access WEB GUI).
User (default)	root
Password (default)	admin
Console (command line) query	ssh [user@]hostname[:port]
Console (command line) query example	ssh root@192.168.2.1

You do not need to provide the port number, if the default port (22) is configured in your Firmux board. You will be asked to enter the password once

Graphical interface tools

If you are not used to the command line, you

PuTTY (<https://www.putty.org/>)

could install and use one of open source graphical SSH tools, such as PuTTY. The PuTTY helps you with connecting to the device, and can also be used for Telnet or Serial connections.

Telnet

Telnet is a network protocol that was built for interacting with remote devices and managing them. It provides a two-way text-based communication channel between two machines, similar to SSH, but less secure.

Figure 43 – Telnet service configuration

Telnet

Telnet is a network protocol used to virtually access a computer and to provide a two-way, collaborative and text-based communication channel between two machines.

Enabled

Port

Default Telnet options

Enabled	No
Port	23

SSH connection parameters

Hostname	Device IP address (same that you use to access WEB GUI).
User (default)	root
Password (default)	admin
Console (command line) query	telnet hostname port
Console (command line) query example	telnet 192.168.2.1

You do not need to provide the port number, if the default port (23) is configured in your Firmux board. You will be asked to enter the username and password once connection is established.

Graphical interface tools

As in SSH, you could install and use an open source graphical application PuTTY for easier connection to the device.

PuTTY (<https://www.putty.org/>)

NTP

The NTP (Network Time Protocol) service synchronizes the clock of the device with the defined online time server. Enable NTP service and enter the NTP server address in order to use the NTP service.

Figure 44 – NTP service configuration

NTP

Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network.

Enabled

Server addresses

- **Enable NTP** – select whether you want the NTP service enabled or disabled.
- **NTP Server address** – specify the trusted NTP server IP or hostname for time synchronization.

Default NTP options

Enabled	Yes
Server address 1	pool.ntp.org
Server address 2	-

Device discovery

Device discovery allows your Firmux board to advertise its capabilities, identity, and other information onto a LAN. Device discovery service also allows the Firmux board to receive such information from other devices on the network.



The information received about other devices is displayed in the Device discovery page under **Tools -> Device discovery**.

Figure 45 – Device discovery service configuration

Device discovery

This feature allows to find other devices compatible with the available discovery protocols, as well as to broadcast information to other devices.

Enabled

Discover nearby devices:

LLDP listener

Broadcast device info:

LLDP (Link Layer Discovery Protocol)

CDP (Cisco Discovery Protocol)

MNDP (MikroTik Neighbor Discovery Protocol)

Discover nearby devices service allows the Firmux board to learn information about other devices on its network links:

- LLDP server – Link Layer Discovery Protocol (LLDP) server – allows the Firmux board to learn information about other devices on its LAN network links. Such information, when available, is displayed under **Tools -> Device discovery**.

Broadcast device info allows your Firmux distribute (advertise) it's own information capabilities and other parameters to neighboring network devices:

- **LLDP** – Link Layer Discovery Protocol service.
- **CDP** – Cisco Discovery Protocol
- **MNDP** – MikroTik Neighbor Discovery Protocol

Device information can include information such as Chassis ID, Port ID, Management IPv4 address, Management IPv6 address, System name, System description and VLAN ID.

SNMP and SNMP traps

SNMP

Simple Network Management Protocol (SNMP) is a protocol for collecting and organizing information about managed devices on IP networks. SNMP service allows the SNMP manager to access the information collected on the device.

Figure 46 – SNMP service configuration

SNMP

Simple Network Management Protocol (SNMP) is an application-layer protocol for monitoring and managing network devices on a local area network (LAN) or wide area network (WAN). The purpose of SNMP is to provide network devices such as routers, servers and printers with a common language for sharing information with a network management system (NMS).

Enabled

Protocol
SNMPv2 + SNMPv3

Community
public

User
root

Password
.....

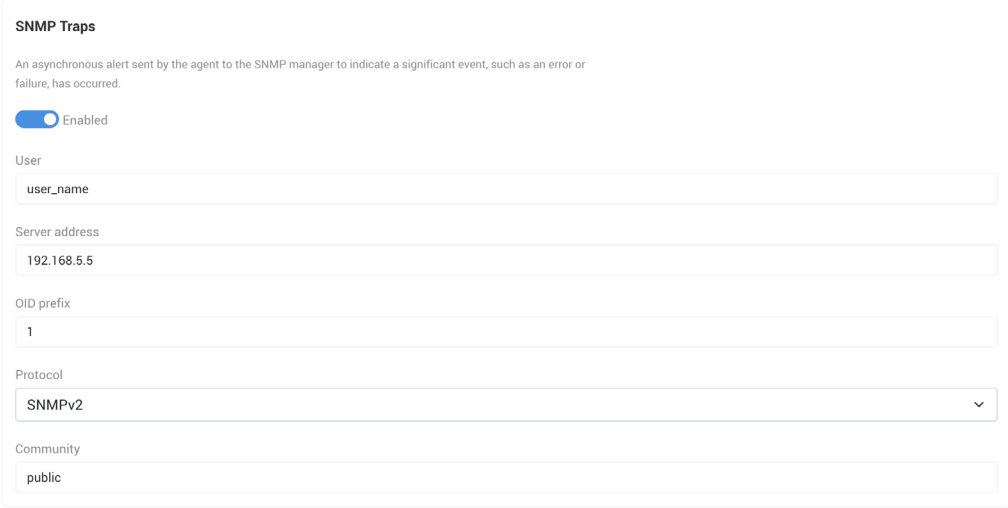
Firmux enables the use of SNMPv2 and SNMPv3 versions of the protocol.

- **SNMPv2**
 - Community – the SNMP community string is used as an authentication means for accessing the SNMP service on the board.
- **SNMPv3**
 - User and password – in SNMPv3 username and password are used to authenticate the remote access to the SNMP service on board.
- **SNMPv2 + SNMPv3**
 - If this protocol is chosen, both authentication methods will be used.

SNMP traps

SNMP traps allow the device to automatically send the collected information to the management server. Monitored device (SNMP agent) sends the messages in a form of traps to the destination (server).

Figure 47 – SNMP traps service configuration



SNMP Traps

An asynchronous alert sent by the agent to the SNMP manager to indicate a significant event, such as an error or failure, has occurred.

Enabled

User

user_name

Server address

192.168.5.5

OID prefix

1

Protocol

SNMPv2

Community

public

- User – specify the username for authentication.
- Server address – specify the SNMP trap destination server IP address or hostname.
- OID prefix – select the oid prefix. Object Identifier (OID) uniquely identifies the managed information object in the information hierarchy.
- SNMPv2 protocol
 - Community – the SNMP community string is used as an authentication means for accessing the SNMP service on the board.
- SNMPv3 protocol
 - Password – the password that will be used for the authentication.

Remote syslog

When remote syslog is enabled, the device will be collecting device log messages in a log file.

Figure 48 – Remote syslog service configuration - Periodic logging to file

Remote syslog

Syslog is a way for this network device to send event messages to a logging server or file.

Enabled

Mode

Periodic logging to file

Syslog is periodically written to /etc/logread.out file in the device flash memory. WARNING: the device has limited amount of flash memory

Period (minutes)

5

- Instant logging to file – the log file will be appended everytime new log messages are available. The log file will be saved on device flash memory. By a serial or SSH connection that file can be accessed in the “/etc/logread.out” location.
- Periodic logging to file – the log file will be appended every once in a specified period (in minutes).
- Remote server – the system log will be collected on a remote syslog server. Many open-source syslog server applications are available.
 - Protocol – TCP, UDP
 - Server address – the IP address or hostname of the remote syslog server.
 - Port – the port that will be used.
 - Log prefix – prefix used by syslog server to organize the information.

Local log file

Local log file can be accessed by serial or SSH connection.

Location	/etc/logread.out
Server address 2	-

Remote server

Syslog server using TCP or UDP protocol.

Port	514 (default)
-------------	---------------

Figure 49 – Remote syslog service configuration - Remote server

Remote syslog

Syslog is a way for this network device to send event messages to a logging server or file.

Enabled

Mode
Remote server

Protocol
TCP

Server address
192.168.1.16

Port
4444

Log prefix
nice_log!

Ping Watchdog

When the ping watchdog is enabled, the device will try to periodically ping selected IP addresses. When these addresses are unreachable, the device will be rebooted. This service is useful as a last resort mechanism that tries to recover the device when something unexpected happens in the network.

- Ping interval – the amount of time in seconds the service will try to ping selected IP addresses.
- Startup delay – the amount of time in seconds the service will wait after startup before starting the ping sequence. This is useful when network setup takes a while, for example when DHCP is enabled.
- Failure count – device will reboot after this amount of failures to ping.
- IP address to ping – these IP addresses will be pinged periodically. If multiple IPs are entered, the device will only reboot if all of them are unreachable.

Figure 50 – Ping Watchdog configuration

Ping Watchdog

The purpose of ping watchdog is to reboot the device when it cannot ping a particular IP address.

Enabled

Ping interval (s)
300

Startup delay (s)
300

Failure count
3

IP address to ping
192.168.1.1

Web Shell

Web shell lets you access device console via our graphical user interface. It can do most of the functions that you would normally do connecting to the device with other means such as SSH, serial, etc.. It works over WebSockets protocol.



The console is displayed in the Web Shell page under **Tools -> Web Shell**.

Figure 51 Web Shell configuration

Web Shell

This service enables device console inside the graphical user interface. When enabled, Web Shell can be accessed in Tools page.

Enabled

Port

7681

SSL

- Port - Set the port for Web Shell, default is 7681.
- SSL - Allow Web Shell tool to be accessed via HTTPS with SSL certificates.

User configuration

User configuration page lets you create users with different roles, add SSH keys for root users, remove them and modify their status.

Figure 52 User configuration

User configuration + Add

User name	Role	Status	Set new password
> root	Admin	<input checked="" type="checkbox"/>	
observer	Observer	<input checked="" type="checkbox"/>	
Installer	Installer	<input checked="" type="checkbox"/>	

- User name - set the user name for login purposes.
- Role - specify a role for the user. Different roles can see things in WEB GUI.
 - Admin - this role has all the privileges.
 - Installer - this role is similar to the Admin role, with a few less privileges, it is unable to see the users section in configuration and GUI, unable to reset the device and access Web Shell tool.
 - Observer- this role is only able to see statistics about the device (main dashboard page).
- Status - this option lets you disable or enable the user without deleting it.
- Set new password - this lets you update your existing password with a new one, clicking on the glasses icon will unhide the password.

Tools

Device discovery

Tool that lets you find nearby devices.

Figure 53 Device discovery tool

Chassis ID	Local Port	Remote Port	IPv4 address	IPv6 address	Name	VLAN
> 08:BD:43:6A:BD:58	eth2	-	10.0.12.4	-	SW 3	-
> 08:BD:43:6A:BD:58	eth2	-	10.0.12.4	-	SW 3	-
> 28:76:10:13:6A:93	eth3	-	192.168.201.1	-	AP 25	100

Site survey

Lets you find SSIDs by selected radio frequency.

Figure 54 Site survey tool

SSID	BSSID	Channel	Signal	Security
8devices	2E:76:10:00:00:01	5 (2432 MHz), 20 MHz	-78 dBm	WPA2
IgniteNet-Test-2G	32:76:10:00:00:01	5 (2432 MHz), 20 MHz	-78 dBm	WPA2-PSK
firmux-2G	C4:93:00:0F:30:42	11 (2462 MHz), 40 MHz	-85 dBm	Open
Jaunimas	54:E6:FC:DD:F5:34	6 (2437 MHz), 20 MHz	-90 dBm	WEP

Ping

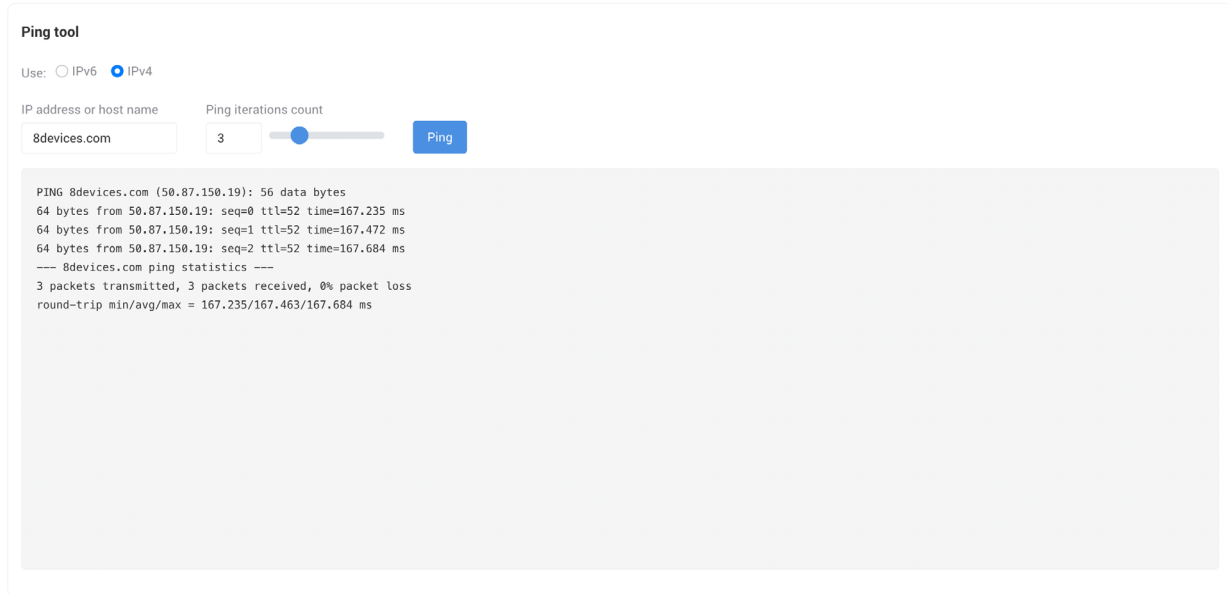
Ping measures the round-trip time for messages sent from the originating host to a destination computer that are echoed back to the source.

Most of the time ping is used to check if IP address is reachable.

You can ping hostnames or IP addresses and chose in what IP address you want to resolve it.

Also you can chose how many times you want to ping. After pressing “Ping” button you will see result in the bottom table.

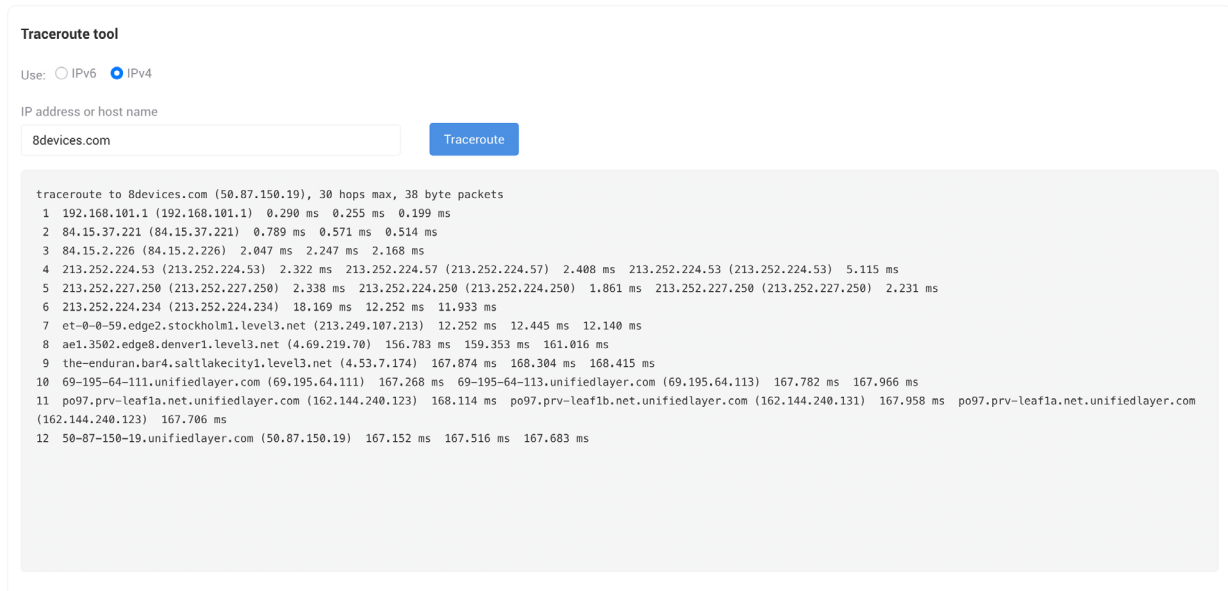
Figure 55 Ping tool



Traceroute

Traceroute is helpful for figuring out the routing hops data has to go through, as well as response delays as it travels across nodes, which are what send the data toward its destination. Traceroute also enables you to locate where the data was unable to be sent along, known as points of failure. Same as Ping you can ping hostnames or IP addresses and chose in what IP address you want to resolve it. After pressing “Traceroute” button you will see result in the bottom table.

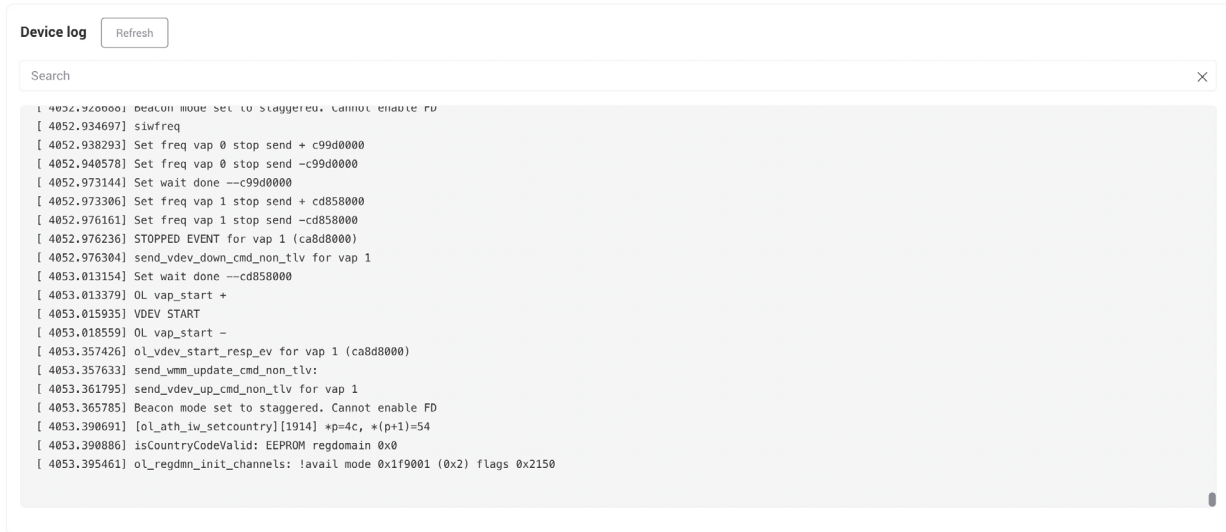
Figure 56 Traceroute tool



View log

Tool that lets you check device logs with searching capabilities.

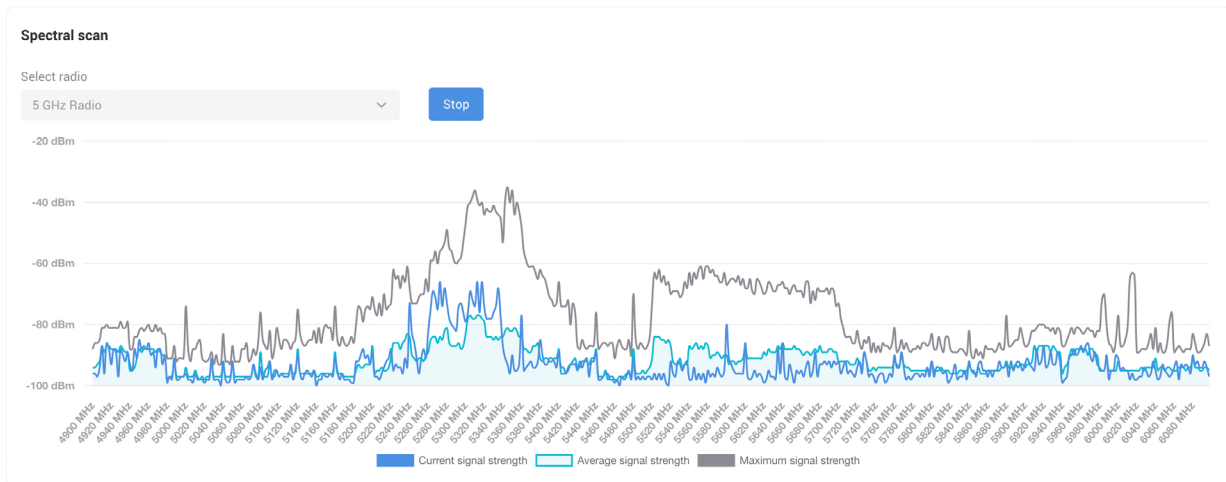
Figure 57 Device log tool



Spectral scan

Measures the magnitude of an input signal versus frequency within the full frequency range of the device. The primary use is to measure the power of the spectrum of known and unknown signals.

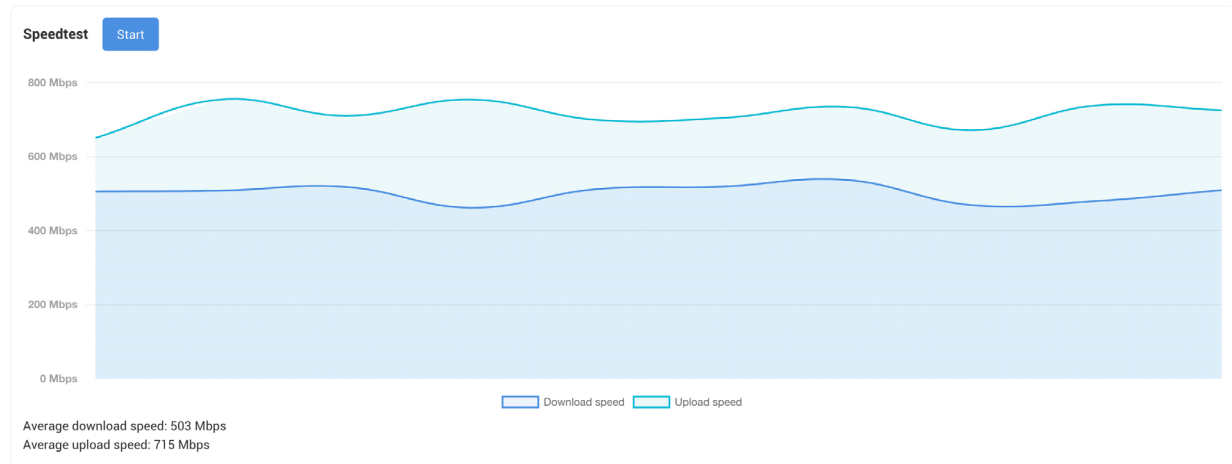
Figure 58 Spectral scan tool



Speedtest

Speedtest measures the speed between your device and a test server, using your device's internet connection.

Figure 59 Speedtest tool



Web Shell

This tool lets you use device terminal over the web.

Figure 60 Web Shell tool

