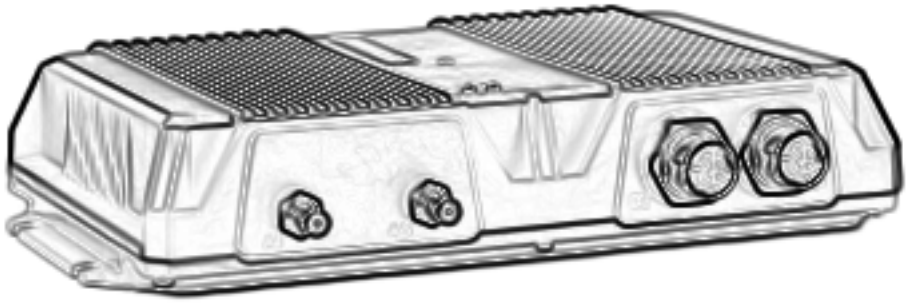
NetModule Wireless Access Point AP3400

User Manual for Software Version 99.99



Manual Version 1.9.3

NetModule AG, Switzerland

June 19, 2023

NetModule Wireless Access Point AP3400

This manual covers all variants of the *AP3400* product type.

The specifications and information regarding the products in this manual are subject to change without notice. We would like to point out that NetModule makes no representation or warranties with respect to the contents herein and shall not be responsible for any loss or damage caused to the user by the direct or indirect use of this information This document may contain information about third party products or processes. Such third party information is generally out of influence of NetModule and therefore NetModule shall not be responsible for the correctness or legitimacy of this information. Users must take full responsibility for their application of any products.

Copyright ©2023 NetModule AG, Switzerland All rights reserved

This document contains proprietary information of NetModule. No parts of the work described herein may be reproduced. Reverse engineering of the hardware or software is prohibited and protected by patent law. This material or any portion of it may not be copied in any form or by any means, stored in a retrieval system, adopted or transmitted in any form or by any means (electronic, mechanical, photographic, graphic, optic or otherwise), or translated in any language or computer language without the prior written permission of NetModule.

A large amount of the source code to this product is available under licenses which are both free and open source. Most of it is covered by the GNU General Public License which can be obtained from www.gnu.org. The remainder of the open source software which is not under the GPL, is usually available under one of a variety of more permissive licenses. A detailed license information for a particular software package can be provided on request.

All other products or company names mentioned herein are used for identification purposes only and may be trademarks or registered trademarks of their respective owners. The following description of software, hardware or process of NetModule or other third party provider may be included with your product and will be subject to the software, hardware or other license agreements.

Contact

https://support.netmodule.com

NetModule AG	Tel +41 31 985 25 10
Maulbeerstrasse 10	Fax +41 31 985 25 11
CH-3011 Bern	info@netmodule.com
Switzerland	https://www.netmodule.com

Contents

1. Welcome to NetModule . . . 7
2. Conformity . . . 8
   2.1. Safety Instructions . . . 8
   2.2. Declaration of Conformity . . . 12
   2.3. Waste Disposal . . . 13
   2.4. National Restrictions . . . 13
   2.5. Open Source Software . . . 14
3. Specifications . . . 15
   3.1. Appearance . . . 15
   3.2. Features . . . 15
   3.3. Environmental Conditions . . . 16
   3.4. Interfaces . . . 17
      3.4.1. Overview . . . 17
      3.4.2. Default LED Indicators . . . 17
      3.4.3. Reset . . . 18
      3.4.4. WLAN . . . 18
      3.4.5. M12 Ethernet Connectors . . . 19
      3.4.6. Power Supply . . . 21
4. Installation . . . 22
   4.1. Installation of the WLAN Antennas . . . 22
   4.2. Installation of the Local Area Network . . . 23
   4.3. Installation of the Power Supply . . . 23
   4.4. REST API . . . 23
5. Configuration . . . 24
   5.1. General Website Options . . . 24
      5.1.1. Device Access . . . 24
      5.1.2. Web Interface access . . . 25
      5.1.3. General Device Options . . . 26
      5.1.4. Navigating . . . 28
      5.1.5. Device information page . . . 28
      5.1.6. Maintenace . . . 32
   5.2. Device Website Configuration . . . 33
      5.2.1. Network Settings . . . 33
      5.2.2. Wireless Configuration . . . 40
      5.2.3. Services Configuration . . . 46
      5.2.4. System Configuration . . . 53
      5.2.5. User Configuration . . . 55
   5.3. Tools . . . 57
      5.3.1. Device Discovery . . . 57
      5.3.2. Site survey . . . 57
      5.3.3. Ping . . . 58
      5.3.4. Traceroute . . . 58
      5.3.5. Device log . . . 59
      5.3.6. Speedtest . . . 60
A. Appendix . . . 61
   A.1. Abbrevations . . . 61

List of Figures

3.1. AP3400 Outline . . . 15
3.2. AP3400 Interfaces . . . 17

5.1. AP3400 Web User Interface . . . 24
5.2. First login screen . . . 25
5.3. Update credentials screen . . . 25
5.4. AP3400 Web User Interface . . . 26
5.5. Save button . . . 26
5.6. Save configuration error button . . . 26
5.7. Search bar . . . 28
5.8. Dashboard navigation . . . 28
5.9. Cards and tabs . . . 29
5.10. Dashboard . . . 29
5.11. Network information page . . . 30
5.12. Interfaces information page . . . 31
5.13. Clients information page . . . 31
5.14. Activity page . . . 32
5.15. Maintenance tab . . . 32
5.16. Settings navigation tab . . . 33
5.17. Zone settings tab . . . 34
5.18. Ethernet settings tab . . . 36
5.19. Static route settings tab . . . 36
5.20. Port forwarding settings tab . . . 37
5.21. Wireguard server settings tab . . . 38
5.22. Wireguard client settings tab . . . 39
5.23. Wireless settings tab . . . 40
5.24. Access point settings tab . . . 41
5.25. Station settings tab . . . 42
5.26. Scan result tab . . . 43
5.27. SSID tab . . . 45
5.28. SSID Security tab . . . 46
5.29. Web service tab . . . 47
5.30. SSH service tab . . . 47
5.31. Telnet service tab . . . 48
5.32. NTP service tab . . . 48
5.33. Device discovery tab . . . 49
5.34. SNMP service tab . . . 50
5.35. SNMP Traps . . . 51
5.36. Remote Syslog . . . 52
5.37. Ping Watchdog Settings . . . 53
5.38. System Configuration Settings . . . 53
5.39. Automatic Updater Settings . . . 54
5.40. Firmware Updater Notification . . . 55
5.41. Physical Reset Button . . . 55
5.42. User Configuration . . . 55
5.43. Tools Menu . . . 57
5.44. Device discovery . . . 57
5.45. Site Survey Scan results . . . 58

5.46. Ping results 58
5.47. Traceroute results 59
5.48. Device log 59
5.49. Speedtest results 60

List of Tables

2.1. Antenna Information Detail 12

3.1. Environmental Conditions 16
3.2. AP3400 Interfaces 17
3.3. AP3400 Status Indicators 17
3.4. IEEE 802.11 2.4GHz Standards 18
3.5. IEEE 802.11 5GHz Standards 18
3.6. WLAN Antenna Port Specification 19
3.7. Ethernet Port Specification 19
3.8. Pin Assignments of 8 Poles Ethernet Connectors 20
3.9. Power Input Specifications 21
3.10. Pin Assignments of 8 Poles Ethernet Connectors 21

4.1. WLAN antenna port types 22

A.1. Abbreviations 63

1. Welcome to NetModule

Thank you for purchasing a NetModule product. This document should give you an introduction to the device and its features. The following chapters describe any aspects of commissioning the device, installation procedure and provide helpful information towards configuration and maintenance.

Please find further information such as sample SDK scripts or configuration samples in our wiki on https://wiki.netmodule.com.

2. Conformity

This chapter provides general information for putting the wireless access point into operation.

2.1. Safety Instructions

Please carefully observe all safety instructions in the manual that are marked with the symbol ⚠.

Compliance information: The NetModule wireless access points must be used in compliance with any and all applicable national and international laws and with any special restrictions regulating the utilization of the communication module in prescribed applications and environments.

Information about the accessories / changes to the device:

- Please only use original accessories to prevent injuries and health risks.
- Changes made to the device or the use of non-authorized accessories will render the warranty null and void and potentially invalidate the operating license.
- NetModule wireless access points must not be opened.

Information about the device interfaces:

- All systems that are connected to the NetModule wireless access point interfaces must meet the requirements for SELV (Safety Extra Low Voltage) systems.
- Interconnections must not leave the building nor penetrate the body shell of a vehicle.
- Connections for antennas may only exit the building or the vehicle hull if transient overvoltages (according to IEC 62368-1) are limited by external protection circuits down to 1 500 V_{peak}. All other connections must remain within the building or the vehicle hull.
- Always keep a distance of more than 40 cm from the antenna in order to reduce exposure to electromagnetic fields below the legal limits.
- Gardez toujours une distance de plus de 40 cm de l' antenne afin de reduire l' exposition aux champs electromagnetiques en dessous des limites legales
- Wireless access points may be operated only with applicable Regulatory Domain configured. Special attention must be paid to country, number of antennas and the antenna gain. WLAN antennas with a higher amplification may be used with a NetModule router including the "Enhanced-RF-Configuration" software license. The antenna gain and cable attenuation has to be correctly configured by certified specialized personnel. A misconfiguration will lead to loss of the approval.
- The maximum gain of an antenna (incl. the attenuation of the connection cables) must not exceed the following values in the corresponding frequency range:
  - WiFi (2.4GHz .. 2.5GHz) < 8.4dBi
  - WiFi (5.1GHz .. 5.9GHz) < 9.1dBi
- Only CE-compliant power supplies with a current-limited SELV output voltage range may be used with the NetModule wireless access points.

FCC Warning:

- Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
- (1) This device may not cause harmful interference , and
- (2) this device must accept any interference received , including interference that may cause undesired operation.

- Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver .
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected .
- Consult the dealer or an experienced radio / TV technician for help.
- FCC Radiation Exposure Statement: This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipment should be installed and operated with minimum distance 40 cm between the radiator and your body.

IC Warning:

- This device complies with Innovation, Science and Economic Development Canada licence-exempt RSS standard (s). Operation is subject to the following two conditions:
- (1) this device may not cause interference, and
- (2) this device must accept any interference, including interference that may cause undesired operation of the device.
- Cet appareil est conforme aux CNR d' l'innovation, la science et le developpement economique Canada licables aux appareil radio exempts de licence. L'exploitation est autorisee aux deux conditions suivantes:
- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioelectrique subi, onj si le brouillage est susceptible d'en compromettre le fonctionnement.
- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Tous les changements ou modifications non expressement approuvee par le responsible de la conformitÃľ pourrait vider l'utilisateur est habilite a exploiter l'equipement.

- IC exposition aux radiations: This equipment complies with ISEDC RF radiation exposure limits set forth for an uncontrolled environment. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. This equipement should be isntalled and operated with minimum distance 40 cm between the radiator and your body
- IC exposition aux radiations: Cet equipement est conforme avec ISEDC les limites d' exposition aux rayonnements definies pour un controle environnement. Cet emetteur ne doit pas etre co-localises ou fonctionner en conjonction avec une autre antenne ou emetteur. Cet equipement doit etre installe et utilise avecune distance minimale 40 cm between le radiator et votre corps
- This radio transmitter [IC: 11468A-AP3] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed in in below table or Chapter 3.4.4, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.
- Cet emetteur radio [IC: 11468A-AP3] a ete approuvee par innovation, science et developpement economique Canada pour fonctionner avec les types d' antennes enumere ci-dessous et pour afficher le gain maximale admissible. Le gain du type d'antenne non inclus cette liste ici ou dans chapitre 3.4.4 est superier au gain maximal d' un des types enumeres et ne doit pas etre utilise avec cet equipement.

IC: The Antenna Information Detail:

Feature	Specification
Antenna Chain	Chain 0 and 1
Manufacturer	Antenna-Railway-Indoor-01-2WJq (Antonics)
Antenna Type	Patch
Input Impedance	50 Ohm
Frequency Range / Antenna Gain	2400-2500 MHz / 8.4 dBi
Frequency Range / Antenna Gain	5150-5250 MHz / 9.1 dBi
Frequency Range / Antenna Gain	5250-5350 MHz / 9.1 dBi
Frequency Range / Antenna Gain	5470-5725 MHz / 9.1 dBi
Frequency Range / Antenna Gain	5725-5850 MHz / 9.1 dBi

Table 2.1.: Antenna Information Detail

General safety instructions:

- Observe the usage limitations of radio units at filling stations, in chemical plants, in systems with explosives or potentially explosive locations.
- The devices may not be used in airplanes.
- Exercise particular caution near personal medical aids, such as pacemakers and hearing aids.
- The NetModule wireless access points may also cause interference in the nearer distance of TV sets, radio receivers and personal computers.
- Never perform work on the antenna system during a thunderstorm.
- The devices are generally designed for normal indoor use. Do not expose the devices to extraordinary environmental conditions worse than IP40.
- Protect them against aggressive chemical atmospheres and humidity or temperatures outside specifications.
- We highly recommended creating a copy of a working system configuration. It can be easily applied to a newer software release afterwards.

2.2. Declaration of Conformity

NetModule hereby declares that under our own responsibility that the wireless access points comply with the relevant standards following the provisions of the *RED Directive 2014/53/EU*. The signed version of the *Declaration of Conformity* can be obtained from `https://www.netmodule.com/downloads`

Operating frequency bands and related maximum radio frequency power transmitted is shown below,

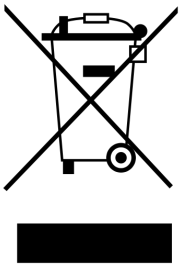
according to RED Directive 2014/53/EU, Article 10 (8a, 8b).

WLAN maximum output power

IEE 802.11b/g/n/ax
Operation frequency range: 2412-2472 MHz (13 channels)
Maximum output power: 20 dBm EIRP average (on antenna port)

IEE 802.11a/n/ac/ax
Operation frequency range: 5180-5350 MHz / 5470-5700 MHz (19 channels)
Maximum output power: 27 dBm EIRP average (on antenna port)

2.3. Waste Disposal



In accordance with the requirements of the *Council Directive 2012/19/EU* regarding Waste Electrical and Electronic Equipment (WEEE), you are urged to ensure that this product will be segregated from other waste at end-of-life and delivered to the WEEE collection system in your country for proper recycling.

2.4. National Restrictions

This product may be generally used in all EU countries (and other countries following the *RED Directive 2014/53/EU*, *FCC* or *ISED*) without any limitation. Please refer to our WLAN Regulatory Database for getting further national radio interface regulations and requirements for a particular country.

2.5. Open Source Software

We inform you that NetModule products may contain in part open-source software. We are distributing such open-source software to you under the terms of GNU General Public License (GPL)[1], GNU Lesser General Public License (LGPL)[2] or other open-source licenses[3]. These licenses allow you to run, copy, distribute, study, change and improve any software covered by GPL, Lesser GPL, or other open-source licenses without any restrictions from us or our end user license agreement on what you may do with that software. Unless required by applicable law or agreed to in writing, software distributed under open-source licenses is distributed on an "AS IS" basis, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

To obtain the corresponding open source codes covered by these licenses, please contact our technical support at router@support.netmodule.com.

[1] Please find the GPL text under http://www.gnu.org/licenses/gpl-2.0.txt
[2] Please find the LGPL text under http://www.gnu.org/licenses/lgpl.txt
[3] Please find the license texts of OSI licenses (ISC License, MIT License, PHP License v3.0, zlib License) under http://opensource.org/licenses

3. Specifications

3.1. Appearance

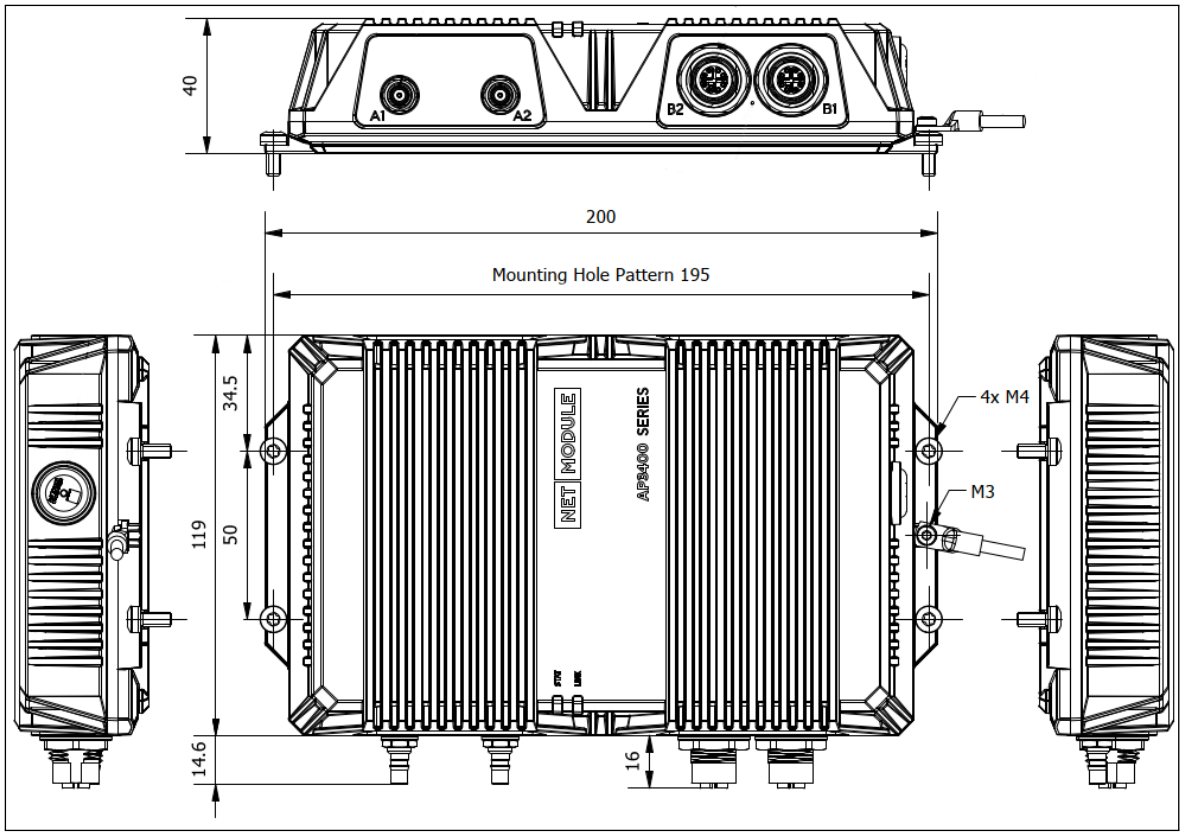


Figure 3.1.: AP3400 Outline

3.2. Features

All models of AP3400 have the following standard functionalities:

- 2x 2.5 Gbit Ethernet ports 802.3bz (M12, x-coded)
- PoE+ IEEE 802.3at (B1)
- 2x WLAN IEEE 802.11a/b/g/n/ac/ax

Due to its modular approach, the AP3400 and its hardware components can be arbitrarily assembled according to its indented usage or application. Please contact us in case of special project requirements.

3.3. Environmental Conditions

Parameter	Rating
Input Voltage	PoE+ (IEEE 802.3at)
Operating Temperature Range	EN50155 OT4 + ST0 ($-40\,°C$ bis $+70\,°C$)
Storage Temperature Range	$-40\,°C$ to $+85\,°C$
Humidity	0 to 95% (non-condensing)
Altitude (Variant Pa)	up to 4000m
Over-Voltage Category	I
Pollution Degree	2
Ingress Protection Rating	IP40

Table 3.1.: Environmental Conditions

3.4. Interfaces

3.4.1. Overview

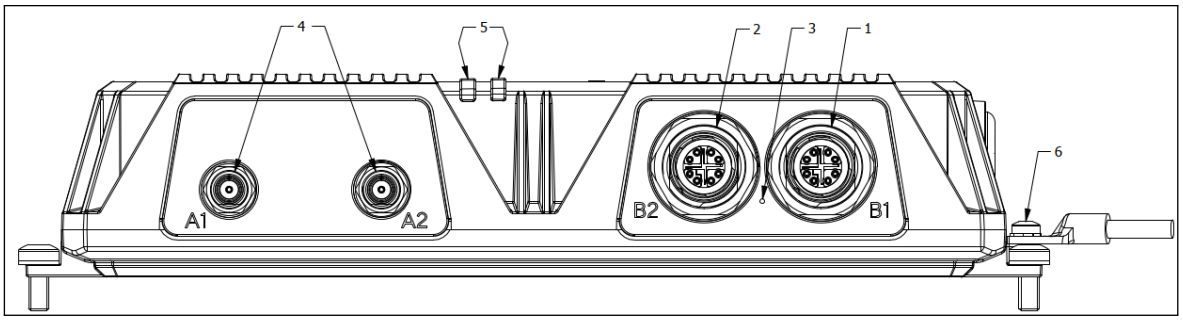


Figure 3.2.: AP3400 Interfaces

Nr.	Label	Function
1	ETH1 B1	2.5 Gbit Ethernet, can be used as LAN or WAN interface. PoE Port
2	ETH2 B2	2.5 Gbit Ethernet, can be used as LAN or WAN interface.
3	Reset	Reboot and factory reset button
4	WLAN A1 / A2	QLS female connectors for MIMO WLAN antenna, both are main antennas
5	LED Indicators	LED Indicators for Status and Link
6	⏚	M3 earth protection connector, connected to the system ground. Galavnic isolated to power supply

Table 3.2.: AP3400 Interfaces

3.4.2. Default LED Indicators

Status LEDs

The following table describes the AP3400 status indicators.

Label	Color	State	Function
STAT	🟢	on	The device is ready.
	🔴	on	System boot failure: recovery mode
	🟡	on	The device is busy due to startup
Link	🟢	on	One Wi-Fi radio module is up and has at least 1 client associated
	🔴	on	Failure on WLAN operation

Table 3.3.: AP3400 Status Indicators

3.4.3. Reset

The reset button has two functions:

1. Reboot the system:
   Press at least 3 seconds to trigger a system reboot.
2. Factory reset:
   Press at least 10 seconds to trigger a factory reset.

3.4.4. WLAN

The AP3400 supports one Wi-Fi 6 802.11 b/g/n/ax 2.4 GHz module with 2x2 MU-MiMo.

Standard	Frequencies	Bandwidth	Data Rate
802.11b	2.4 GHz	20 MHz	11 Mbit/s
802.11g	2.4 GHz	20 MHz	54 Mbit/s
802.11n	2.4 GHz	20/40 MHz	300 Mbit/s
802.11ax	2,4 GHz	20/40 MHz	573.5 Mbit/s

Table 3.4.: IEEE 802.11 2.4GHz Standards

The AP3400 supports one Wi-Fi 6 802.11 a/n/ac/ax 5 GHz module with 2x2 MU-MiMo.

Standard	Frequencies	Bandwidth	Data Rate
802.11a	5 GHz	20 MHz	54 Mbit/s
802.11n	5 GHz	20/40 MHz	300 Mbit/s
802.11ac	5 GHz	20/40/80 MHz	866.7 Mbit/s
802.11ax	5 GHz	20/40/80 MHz	1201 Mbit/s

Table 3.5.: IEEE 802.11 5GHz Standards

The WLAN antenna ports have the following specification:

Feature	Specification
Max. allowed cable length	30 m
Max. allowed antenna gain including cable attenuation	8.4 dBi (2.4GHz) resp. 9.1dBi (5GHz) [1]
Anntenna used for compliance: RED, FCC und IC	Antenna-Railway-Indoor-01-2WJq (Antenna Typ Patch, Manuf. Antonics)
Min. distance between collocated radio transmitter antennas	20 cm
Min. distance between people and antenna	40 cm
Connector type	QLS (QMA)

Table 3.6.: WLAN Antenna Port Specification

3.4.5. M12 Ethernet Connectors

Specification

Feature	Specification
Isolation to enclosure	1500 V_{DC}
Speed	100/1000/2500 Mbit/s
Mode	Half- & Full-Duplex
Crossover	Automatic MDI/MDI-X
Max. cable length	100 m
Cable type	CAT5e or better
Cable shield	mandatory
Connector type	M12 x-coded

Table 3.7.: Ethernet Port Specification

[1] **Note:** WLAN antennas with a higher amplification may be used with the NetModule router "Enhanced-RF-Configuration" software license and the antenna gain and cable attenuation that have been correctly configured by certified specialized personnel.

Pin Assignment on M12, 8 poles, X-coded female

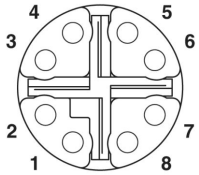
Pin	Signal	Pinning
1	M1+ / DA+	
2	M1− / DA−	
3	M0+ / DB+	
4	M0− / DB−	
5	M2+ / DD+	
6	M2− / DD−	
7	M3− / DC−	
8	M3+ / DC+	

Table 3.8.: Pin Assignments of 8 Poles Ethernet Connectors

3.4.6. Power Supply

Specification

The power input has the following specifications:

Feature	Specification
Power supply	PoE+ (IEEE 802.3at) or passive PoE with 48V [2]
Max. power consumption	15 W
Max. cable length	100m
Cable shield	mandatory
Galvanic isolation	yes, 1500 V_{DC} (according to EN 50155 & EN 62368-1)
Connector type	M12, X-coded, Ethernet 1 (B1)

Table 3.9.: Power Input Specifications

Pin Assignment on M12, 8 poles, X-coded female

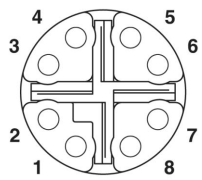
Pin	Signal	Pinning
1	0 V_{DC}	
2	0 V_{DC}	
3	48 V_{DC}	
4	48 V_{DC}	
5	-	
6	-	
7	-	
8	-	

Table 3.10.: Pin Assignments of 8 Poles Ethernet Connectors

[2] **Note:** An ES1(Energy class according to EN 62368-1) power supply must be used

4. Installation

The AP3400 is designed for mounting it on a worktop or wall. Please consider the safety instructions in chapter 2, the environmental conditions in chapter 3.3 and the installation instruction document.

The following precautions must be taken before installing a AP3400 wireless access point:

- Avoid direct solar radiation
- Protect the device from humidity, steam and aggressive fluids
- Guarantee sufficient circulation of air around the device
- The device is for indoor use only

Attention: NetModule wireless access point are not intended for the end consumer market. The device must be installed and commissioned by a certified expert.

4.1. Installation of the WLAN Antennas

The following table shows how to connect the WLAN antennas.

Antenna Port	Type
WLAN A1	Main
WLAN A2	Main

Table 4.1.: WLAN antenna port types

Attention:
When installing the antenna be sure to observe chapter 2

4.2. Installation of the Local Area Network

Up to two 100/1000/2500 Mbps Ethernet devices can be directly connected to the wireless access point, further devices can be attached via an additional Ethernet switch. Please ensure that the connector has been plugged in properly to B1 respectively B2 and remains in a fixed state, you might otherwise experience sporadical link loss during operation. By default, the wireless access point is configured as a DHCP client, with fallback adress 192.168.1.200

Attention:
Only a shielded Ethernet cable may be used.

4.3. Installation of the Power Supply

The wireless access point can be powered with an PoE+ supply. It works with active and passive PoE. If passive PoE is used 48 V_{DC} is necessary. The wireless access point is now ready for getting engaged.

Attention: Only CE-compliant PoE power supply may be used with the NetModule wireless access point

4.4. REST API

The AP3400 is configured with REST API from a NetModule router. Refer to the corresponding router manual for information about how to configure.
The REST API is documented with Swagger and the corresponding JSON schema which can be found here:
Status
Config
Reset
Alternatively the AP3400 can be configured with the WebGUI. See next chapters.

Note:
- Either REST API or GUI may be used, not both together.
- If the Access Point AP3400 is being managed by Netmodule Connectivity-Suite (CS), config changes, Firmware updates should no longer be done directly on the device but on CS only.

5. Configuration

5.1. General Website Options

This chapter will be about general graphical user interface options.

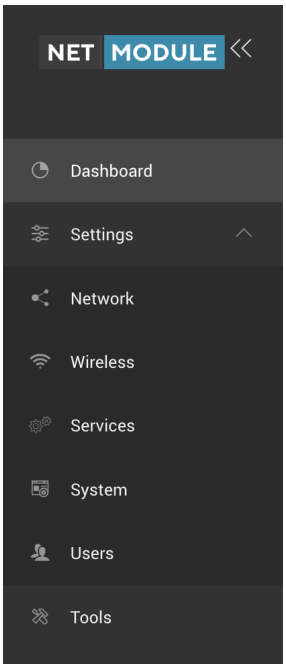


Figure 5.1.: AP3400 Web User Interface

5.1.1. Device Access

By default, the wireless access point is configured as DHCP client. After 10 seconds AP3400 has an IP address of **192.168.1.200**.

5.1.2. Web Interface access

The default administrator login settings are:
Login: **root**
Password: **admin**

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

1. Start your Web browser.
2. Enter the device IP address in the web browser‘s address field and specify default login settings.

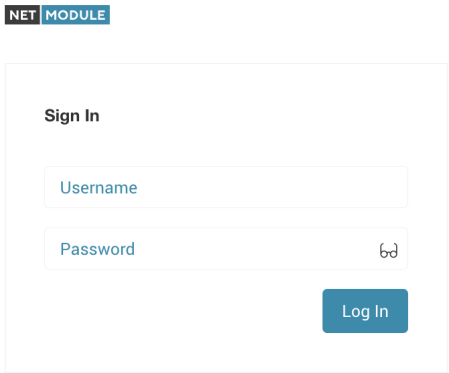


Figure 5.2.: First login screen

3. When logging in for the first time, you will be suggested to change your username and password.

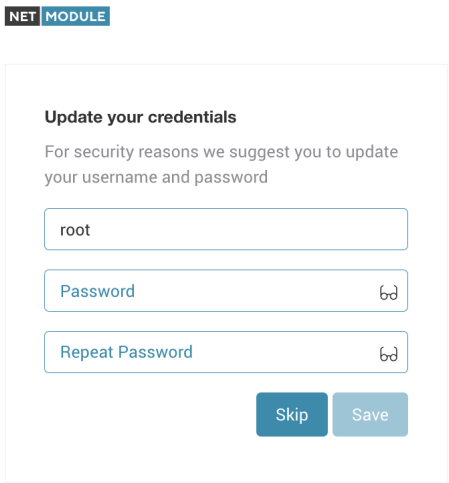


Figure 5.3.: Update credentials screen

4. After successful administrator login you will see the Dashboard - main page of the device Web

management interface. The device now is ready for configuration.

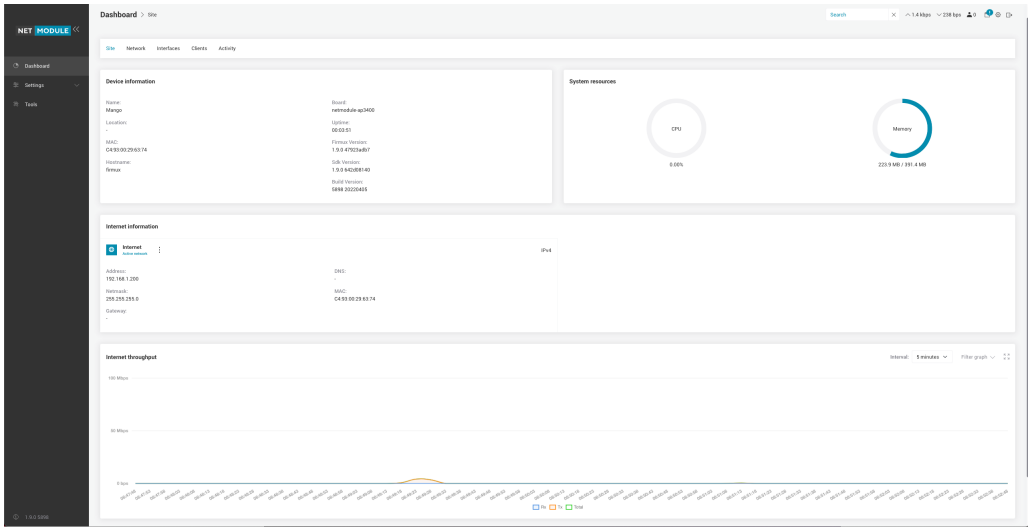


Figure 5.4.: AP3400 Web User Interface

5.1.3. General Device Options

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

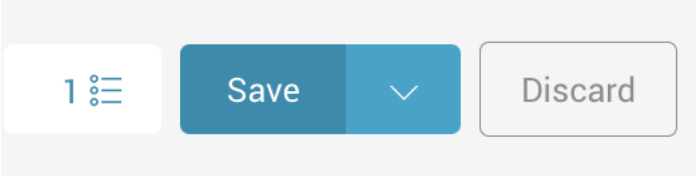


Figure 5.5.: Save button

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, but you will be able to view a list of errors.

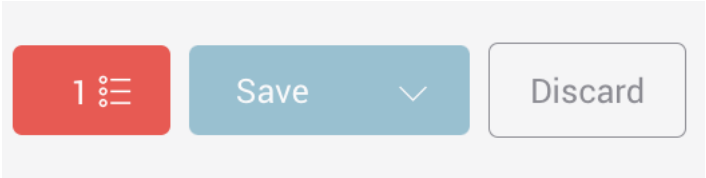


Figure 5.6.: Save configuration error button

- **Save** - if pressed new configuration settings are applied instantly and written to the permanent device config block.
- **Discard** - if pressed configuration changes are discarded.

- **Test changes** - click arrow icon next to Save button and 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 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 remembers all changes made in every tab and 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 3 minute time.

5.1.4. Navigating

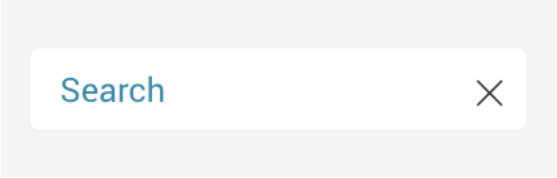


Figure 5.7.: Search bar

In order to quickly navigate between different setting pages, use a search icon, that will redirect to the relevant configuration section.

5.1.5. Device information page

- **Site** - the most important basic information of the device.
- **Network** - displays the information for all the Networks (zones) that are created on the device, as well as ARP table and DHCP active leases table.
- **Interfaces** - displays information for the physical interfaces of the device.
- **Clients** - shows WiFi clients that are connected to the boards network.
- **Activity** - displays the log of most important events that occurred since the device was powered on or rebooted.

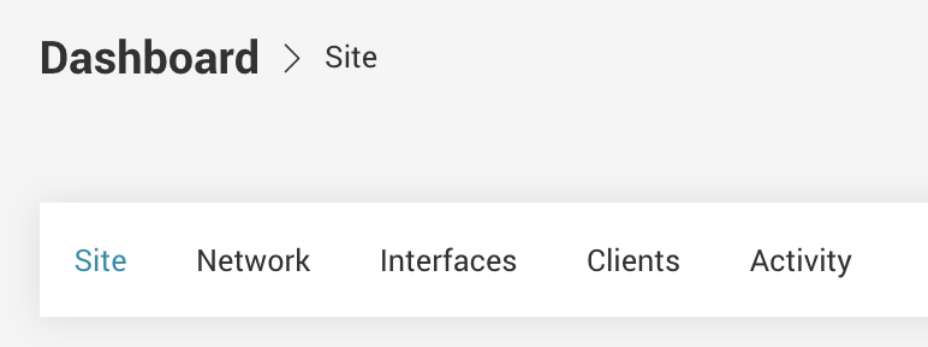


Figure 5.8.: Dashboard navigation

Cards and Tabs

Information in WEB GUI pages are generally 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.

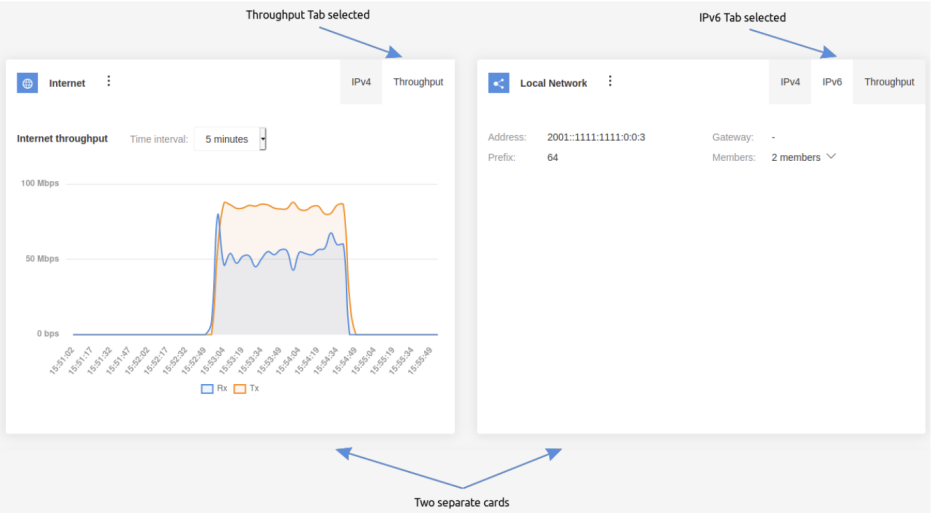


Figure 5.9.: Cards and tabs

Dashboard

After logging in, the WEB GUI displays the Dashboard page - main device information page. The dashboard 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.

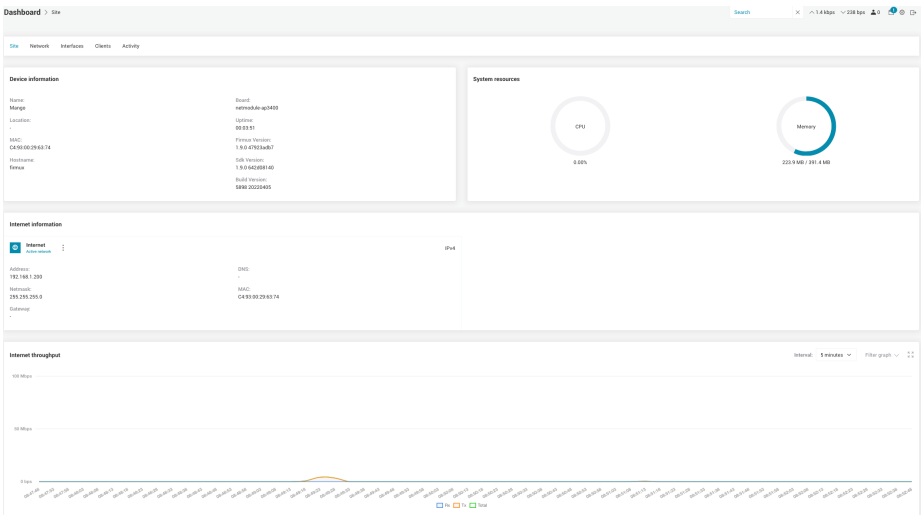


Figure 5.10.: Dashboard

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 new AP3400 devices - Internet and Local network.

- **Internet** -he main Wide Area Network (WAN), through which AP3400 device is connected to the internet.
- **Local network** - a Local Area Network (LAN), that contains all the local devices in your home or organisation connected to AP3400 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.
- **Members** - shows interfaces that are added to the network (zone). Only the networks that have at least one interface added to them will be displayed.
- **ARP entries and DHCP active leases**

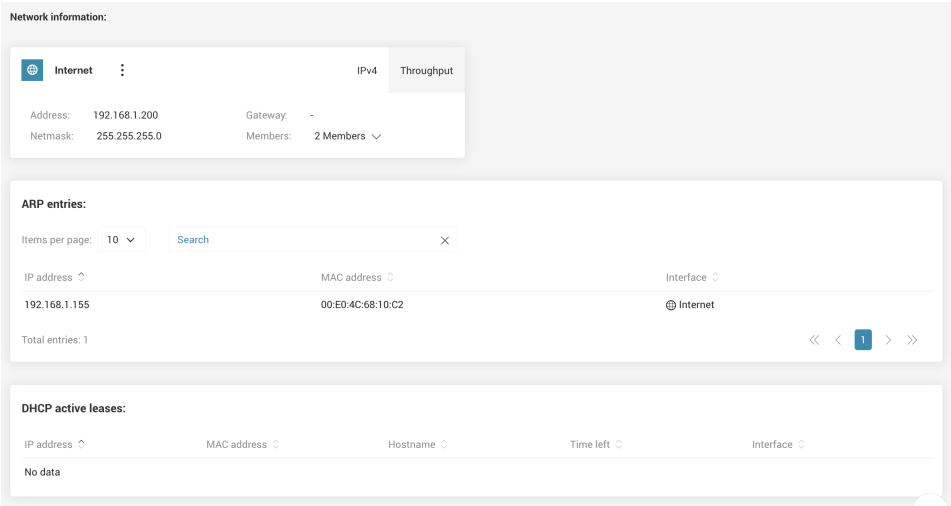


Figure 5.11.: Network information page

Interfaces

The Interfaces page display information for Ethernet ports and Wireless radios.
The page also contains throughput information for every interface. Throughput graphs are accessible via the "Throughput" tab in every interface card.

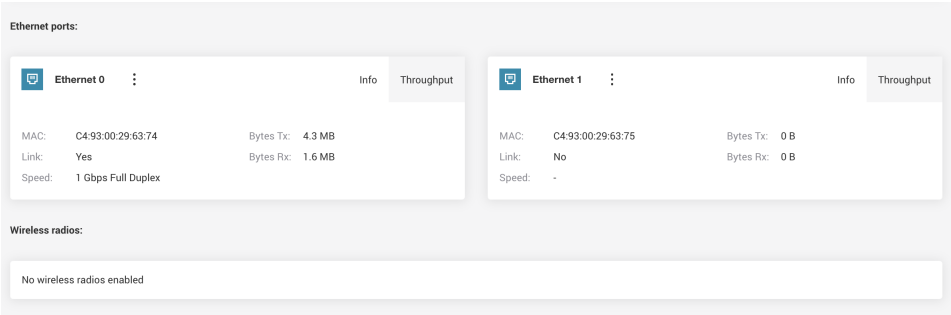


Figure 5.12.: Interfaces information page

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 addresses, uptime, signal strength, SSID, wireless radio frequency and security mode. Your AP3400 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 different password and different wireless network name (SSID).

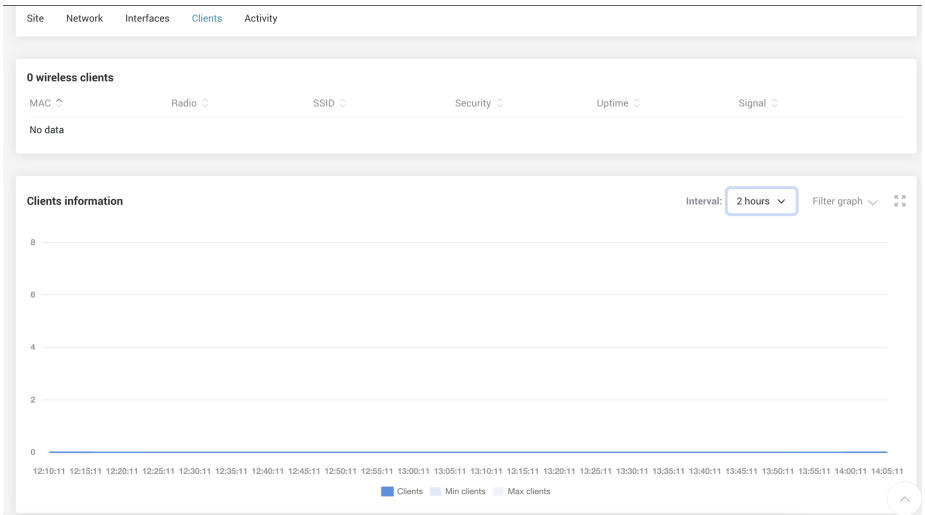


Figure 5.13.: Clients information page

Activity

The Activity page provides a list of most important device events that have happened since the AP3400 device was started.

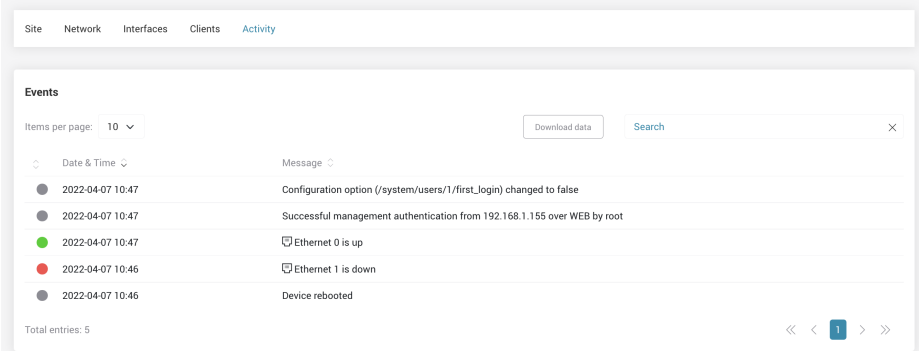


Figure 5.14.: Activity page

5.1.6. Maintenace

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.).

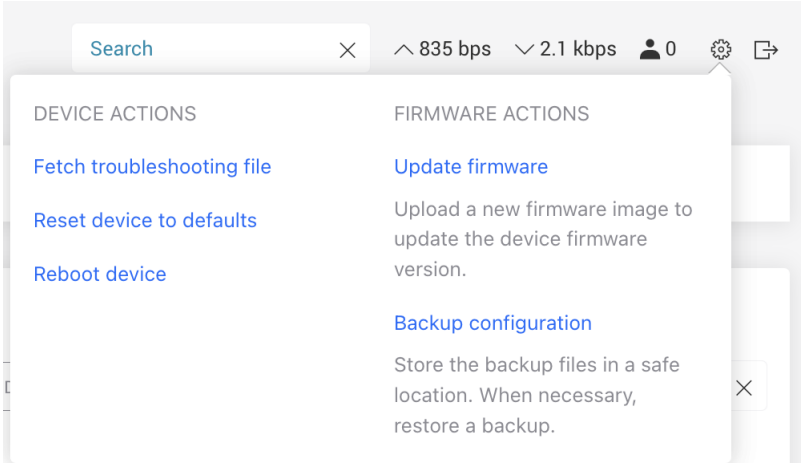


Figure 5.15.: Maintenance tab

- **Update firmware** - allows you to upload new firmware binary image file to upgrade firmware.
- **Backup configuration** - allows you to download current device configuration file or to upload 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 a device misconfiguration or to upload a standard configuration to multiple devices without the need to manually configure 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 device** - reboot device with the last saved configuration.

5.2. Device Website Configuration

The device configuration settings are accessible by selecting **Settings -> Configuration** in the side-bar menu. Device configuration options are grouped into five main categories (Network, Wireless, Services, System and Users), which are accessible by horizontal navigation menu. Each configuration page contains multiple options grouped by cards and tabs.

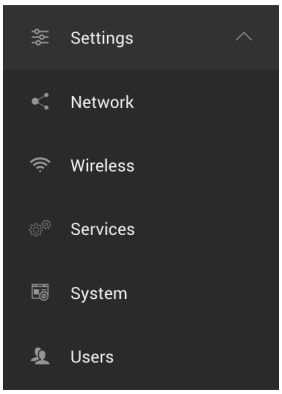


Figure 5.16.: Settings navigation tab

5.2.1. Network Settings

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

Two networks are created on AP3400 boards by default - Internet and Local network:

Internet - the main Wide Area Network (WAN), through which AP3400 device is connected to the internet. Local network - a Local Area Network (LAN), that contains all the local devices in your home or organisation connected to AP3400 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.

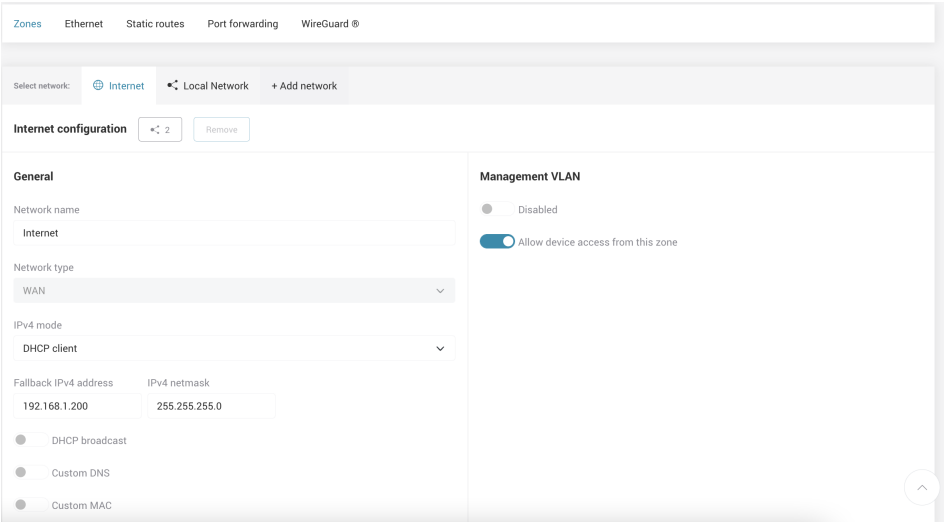


Figure 5.17.: Zone settings tab

WAN Configuration

Allows you to change and configure WAN network parameters. If DHCP client IPv4 mode is selected, then AP3400 board would automatically configure itself with parameters provided by your Internet Service Provider (ISP).

Your AP3400 board has two interfaces added to the default WAN network - Ethernet 0 port and Ethernet 1.

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. Your internet service provider most likely supports DHCP configuration, 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 AP3400 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 "Main" network, and the other networks would be "Backup".

DHCP Client 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, then the Fallback IP address will be used. You can access the board's WEB GUI by using this address. By default, Fallback IP is 192.168.1.200. 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 a DHCP server is not available, or when you need a more advanced WAN configuration. In this case you must 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.

LAN Configuration

By default AP3400 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.

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

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 IP address for devices connected over Wireless and Wired interfaces on LAN side (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.

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.

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.

You can usually find your smart devices MAC address in the Network information page of AP3400

WEB GUI. The "DHCP active leases" table shows IP addresses assigned to all currently connected devices as well as their unique MAC addresses.

Ethernet Configuration

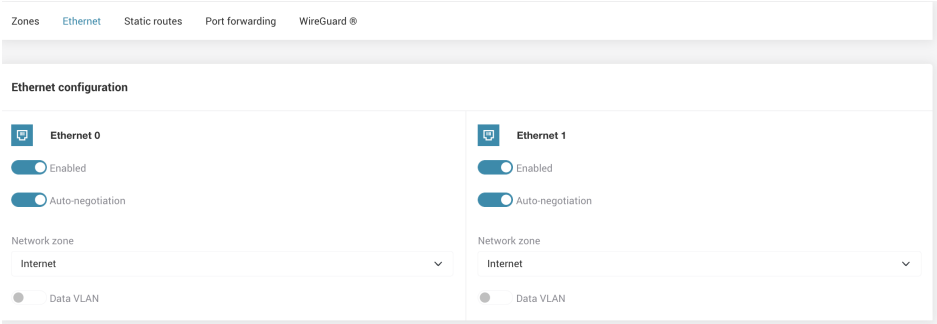


Figure 5.18.: Ethernet settings tab

The Ethernet configuration page lets you assign ethernet interfaces to specific LAN or WAN networks. By default there is one WAN network created on the AP3400 board, and one LAN network. The WAN network has an "Internet" name and Ethernet 0 and Ethernet 1 Interface added to it. The LAN network has "Local Network" name and no interfaces added to it.

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.

Static routes

Static routing is a form of manual configuration of routing entries, telling each IP network what is the next hop that the traffic should be delivered to.

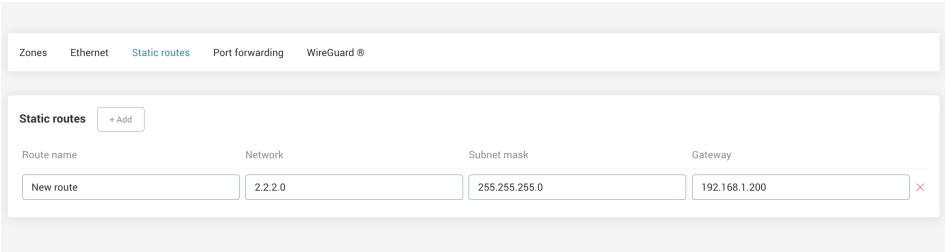


Figure 5.19.: Static route settings tab

Route Name - Give a name for a route for readability.
Network and Subnet Mask - A range of IP addresses that will be routed .
Gateway - Next hop for which the range of IP addresses will take.

Port forwarding

Port forwarding is an application of network address translation (NAT) that redirects the communication request from IP address with a port, to another.

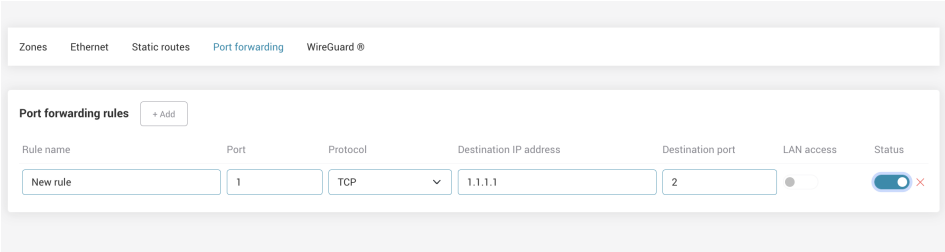


Figure 5.20.: Port forwarding settings tab

Rule Name - Give a name for readability.
Port - Port that is going to be receiving packets.
Protocol - Protocol that is going to be used forwarding the packet.
Destination IP address - IP address that is going to be receiving packets.
Destination Port - Port that is being forwarded the packets.

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.

*Server Mode

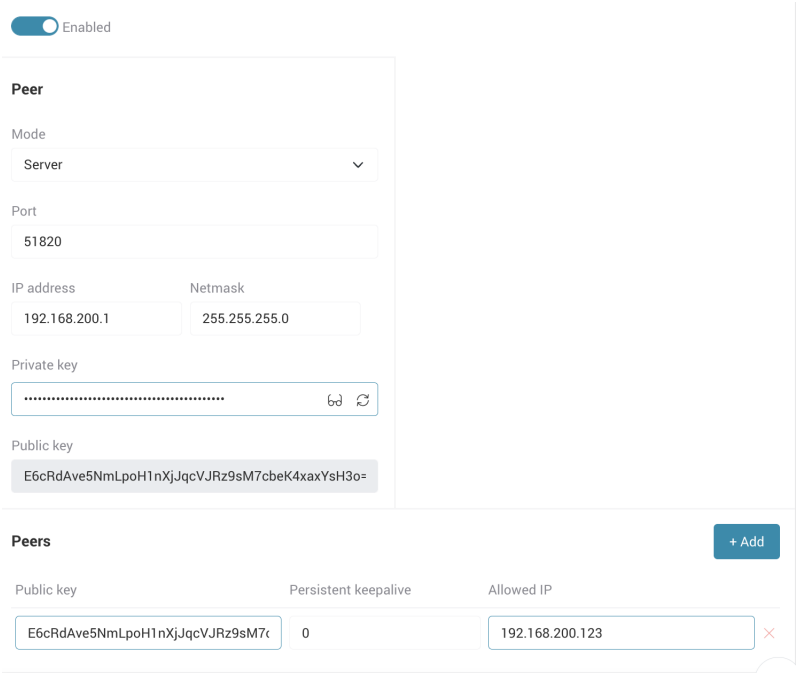


Figure 5.21.: Wireguard server settings tab

Server must have a public IP address (or an IP address otherwise reachable to client).

- Port - specify the port on which the wireguard connection will work (default 51820).
- 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.
- 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.
- 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).

***Client Mode**

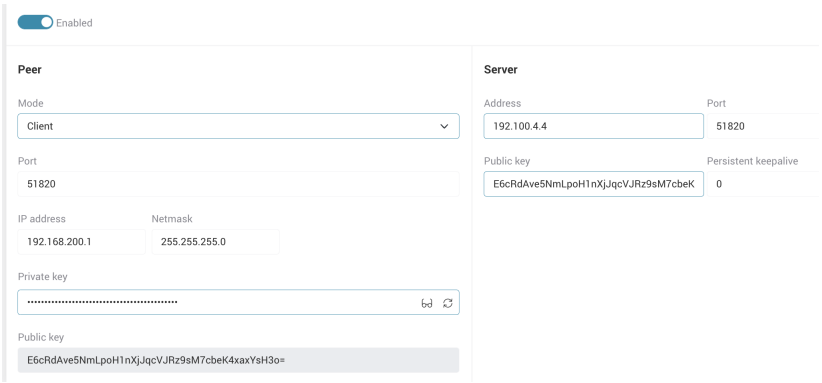


Figure 5.22.: Wireguard client settings tab

Client uses a wireguard server to establish and maintain the secure connection.

- Port - specify the port on which the wireguard connection will work (default 51820).
- 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.
- 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 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).

5.2.2. Wireless Configuration

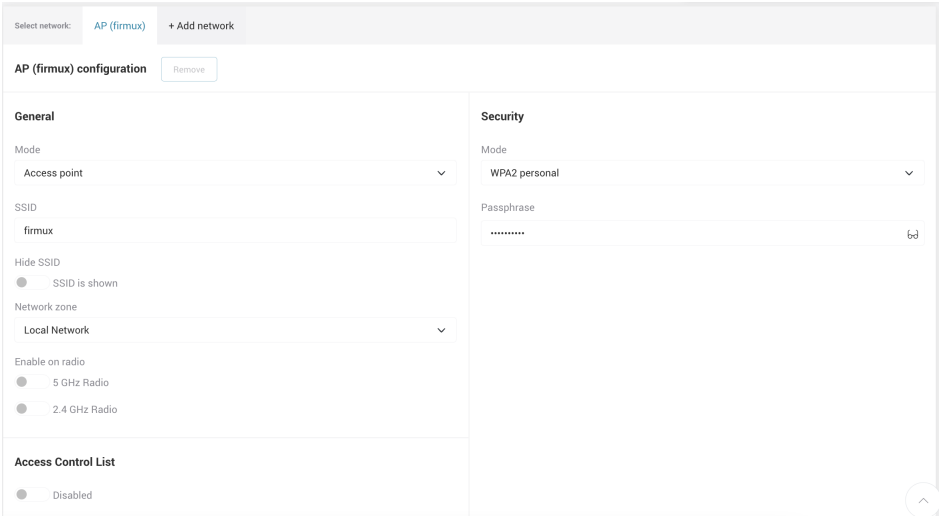


Figure 5.23.: Wireless settings tab

The Wireless configuration page allows the user to control the wireless interfaces of the device. *AP3400 boards have 2.4 GHz and 5 GHz radio interfaces.*

Every radio has a toggle On/Off switch that enables or disables specific radio. Wireless radios 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 AP3400 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).

Radio controls

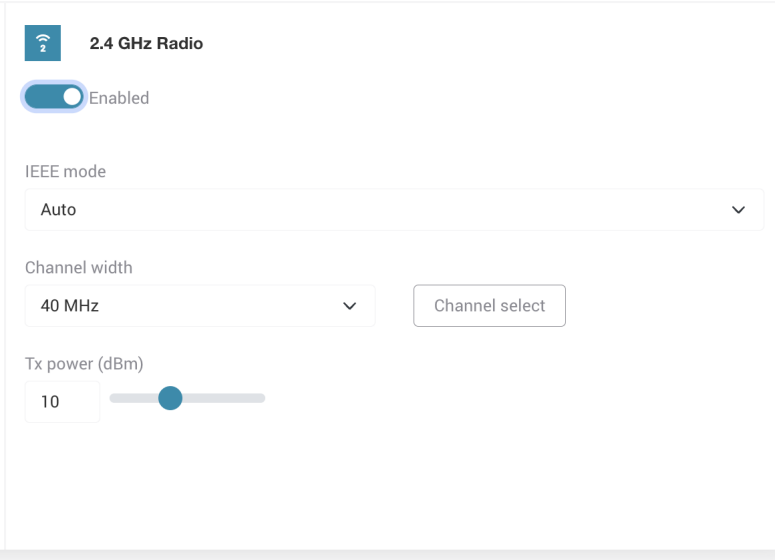


Figure 5.24.: Access point settings tab

IEEE modes - Different IEEE 802 modes for different types of area networks.

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.

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.

Station mode

When you select a Station wireless mode, your board itself can act as a wireless client, so it can connect to other wireless network SSIDs (access points).
The Station wireless radio interface must be added as a member to one of the networks created on this AP3400 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 a 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).

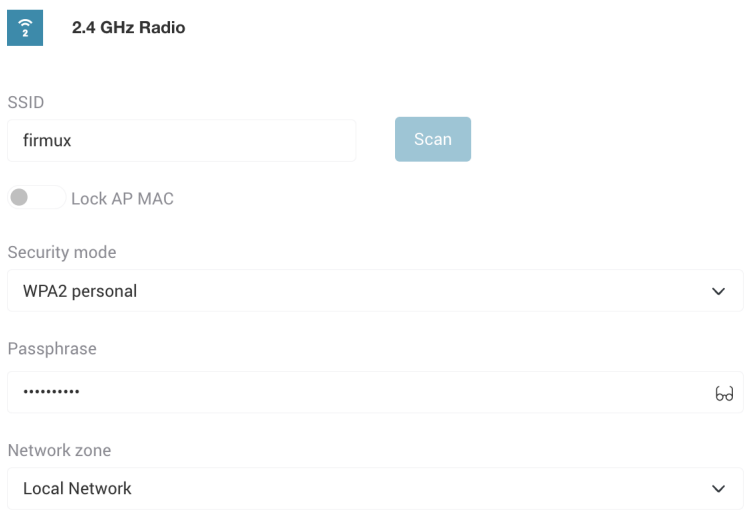


Figure 5.25.: Station settings tab

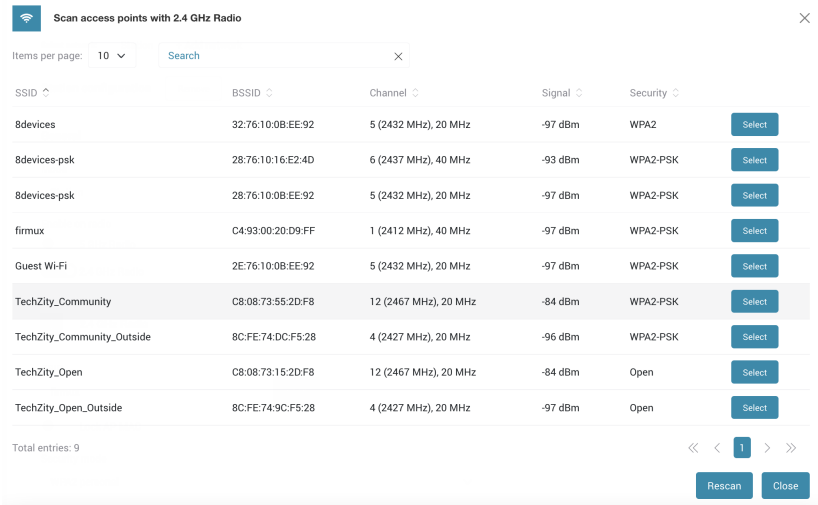
Dual-band concurrent AP3400 boards can have one radio frequency operating in Station mode, and the other frequency operating in Access point wireless mode. This allows your board to wirelessly connect to an internet source, and at the same time share network and internet to multiple WiFi client devices.

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 pick 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 AP3400 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.
- 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.
  - OWE - Opportunistic Wireless Encryption, secure open network that everyone can connect,

but data transferred is individualized and encrypted.
- WPA personal - uses pre-shared key, most common and simple method used for wireless networks.
- WPA enterprise - commonly used simple method with RADIUS server.
- 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.
- WPA3 - more robust password based authentication.
- WPA3 enterprise - Built on a WPA2 foundation with more secure features.
- Mixed modes - Supports several named encryptions.



SSID	BSSID	Channel	Signal	Security	
8devices	32:76:10:0B:EE:92	5 (2432 MHz), 20 MHz	-97 dBm	WPA2	Select
8devices-psk	28:76:10:16:E2:4D	6 (2437 MHz), 40 MHz	-93 dBm	WPA2-PSK	Select
8devices-psk	28:76:10:0B:EE:92	5 (2432 MHz), 20 MHz	-97 dBm	WPA2-PSK	Select
firmux	C4:93:00:20:D9:FF	1 (2412 MHz), 40 MHz	-97 dBm	WPA2-PSK	Select
Guest Wi-Fi	2E:76:10:0B:EE:92	5 (2432 MHz), 20 MHz	-97 dBm	WPA2-PSK	Select
TechZity_Community	C8:08:73:55:2D:F8	12 (2467 MHz), 20 MHz	-84 dBm	WPA2-PSK	Select
TechZity_Community_Outside	8C:FE:74:DC:F5:28	4 (2427 MHz), 20 MHz	-96 dBm	WPA2-PSK	Select
TechZity_Open	C8:08:73:15:2D:F8	12 (2467 MHz), 20 MHz	-84 dBm	Open	Select
TechZity_Open_Outside	8C:FE:74:9C:F5:28	4 (2427 MHz), 20 MHz	-97 dBm	Open	Select

Figure 5.26.: Scan result tab

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 used the SSID Scan feature to select a network.

Security Mode - select the authentication mode for the access point:
- Open - network doesn't require authentication.
- Opportunistic Wireless Encryption - open network, with individualized encryption.
- WPA personal - uses Temporal Key Integrity Protocol for more secure encryption.
- WPA personal - wireless security protocol designed for enterprise wireless networks.
- WPA2 personal - network requires a pre-shared key (Passphrase).
- WPA2 enterprise - network uses advanced security measures. Requires you to enter authentication details that were provided to you by network administrators.
- WPA3 personal - brings better protections to individual users by providing more robust password-

based authentication.
- WPA3 enterprise - builds upon the foundation of WPA2-Enterprise with the additional requirement of using Protected Management Frames on all WPA3 connections.
- WPA2/WPA3 personal - supports both WPA2 and WPA3 personal modes.
- WPA/WPA2 personal - supports both WPA and WPA2 protocol.
- WPA2/WPA3 enterprise - supports both WPA3 and WPA2 enterprise security modes.

Network zone - allows you to add the Station interface to one one of the networks created on the board. Pick a WAN or LAN network from the list and the Station wireless interface will be added to that network. The list displays network names - those networks can be created and configured in the Network configuration page.

Access Point configuration

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

1. Create a LAN or WAN network (Configuration -> Network).
2. Enable a wireless radio in Access point mode (Configuration -> Wireless).
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 (Configuration -> SSID).

When your AP3400 board is in Access point (AP) wireless mode, you can create multiple WiFi networks, and wireless clients can connect to those networks.

One 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 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.

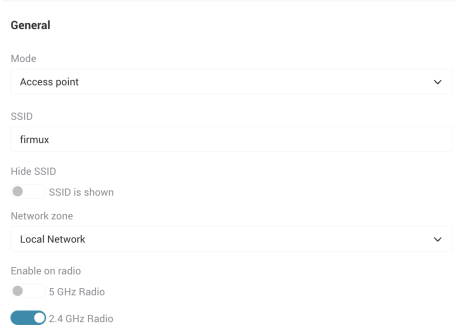


Figure 5.27.: SSID tab

In the SSID configuration page you 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.
- Network name - 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 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.

SSID Security options

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

- Open - network doesn't require authentication.
- WPA2 personal - network requires a pre-shared key (Passphrase).
- WPA2 enterprise - network uses advanced security measures. Requires you to enter authentication details that were provided to you by network administrators.
- WPA3 personal - brings better protections to individual users by providing more robust password-based authentication.
- WPA3 enterprise - builds upon the foundation of WPA2-Enterprise with the additional requirement of using Protected Management Frames on all WPA3 connections.
- WPA2/WPA3 personal - Supports both WPA2 and WPA3 personal modes.

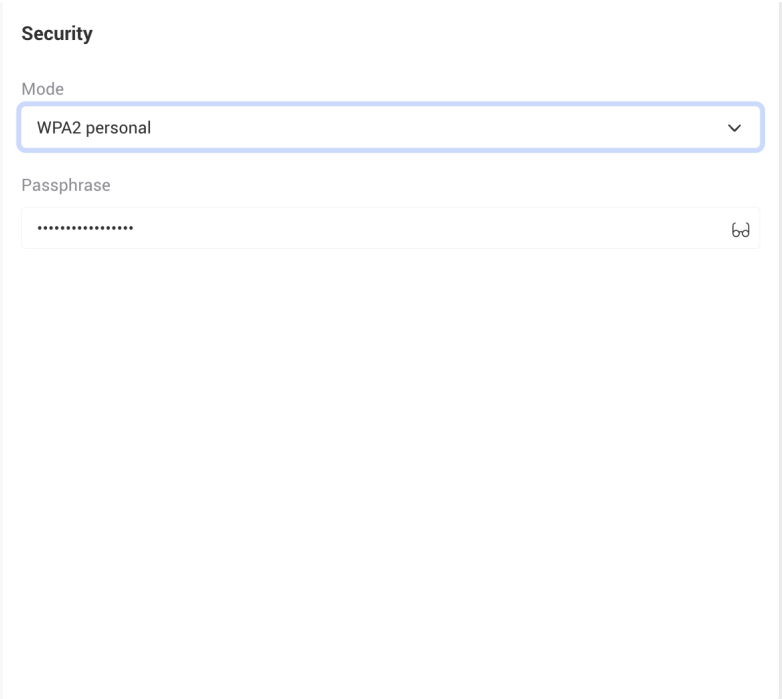


Figure 5.28.: SSID Security tab

Fast BSS

IEEE 802.11r feature that can be configured on AP3400 wireless access points to improve the efficiency of wireless networks. This feature helps to reduce the amount of time it takes for wireless clients to connect to the network and get an IP address.
Upon enabling it two fields appear:

- NAS Identifier - string for RADIUS messages. When used, this should be unique to the NAS within the scope of the RADIUS server. Please note that hostapd uses a separate RADIUS client for each BSS and as such, a unique Nas identifier value should be configured separately for each BSS. This is particularly important for cases where RADIUS accounting is used.

  When using IEEE 802.11r, NAS identifier must be set and must be between 1 and 48 octets long.
- Domain Address - used to indicate a group of APs (within an ESS, i.e., sharing the same SSID) between which a STA can use Fast BSS Transition. The domain identifier string has to match between different APs. 2-octet identifier as a hex string.

5.2.3. Services Configuration

Web Services

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.

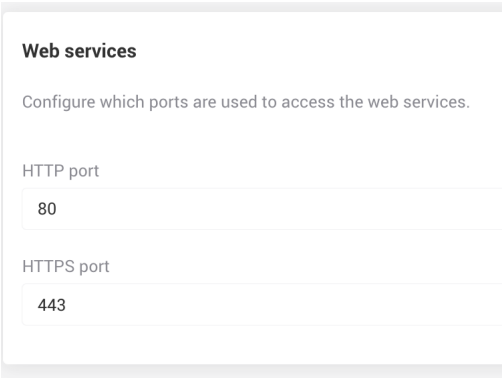


Figure 5.29.: Web service tab

SSH Services

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 AP3400 board using a shell (console).

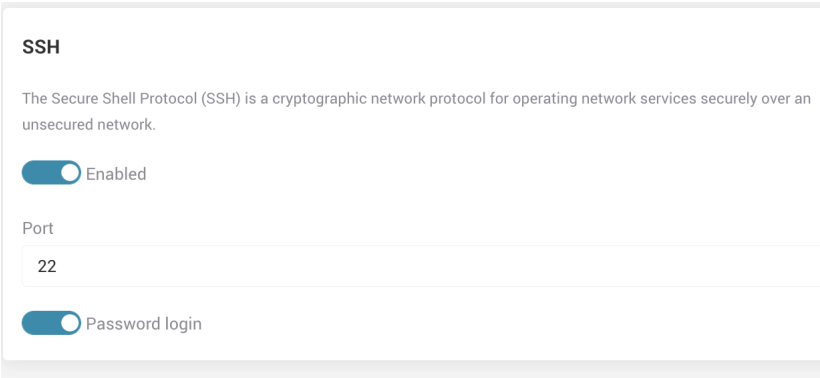


Figure 5.30.: SSH service tab

To use SSH connection for device management, the AP3400 board must be accessible by it‘s IP address from the computer that you are using to connect to the board.
AP3400
To connect via SSH you will also need to provide the username and password of an Admin level user. The AP3400 by default has one Admin level user ("root"), and you can create more users in Settings -> Users configuration page.

Telnet Services

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.

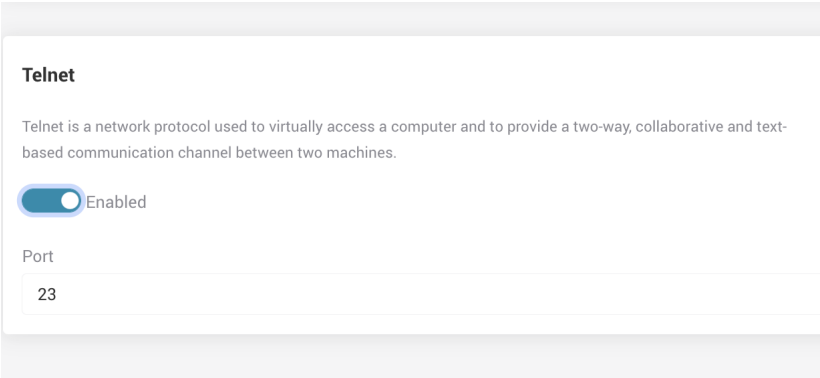


Figure 5.31.: Telnet service tab

NTP Services

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.

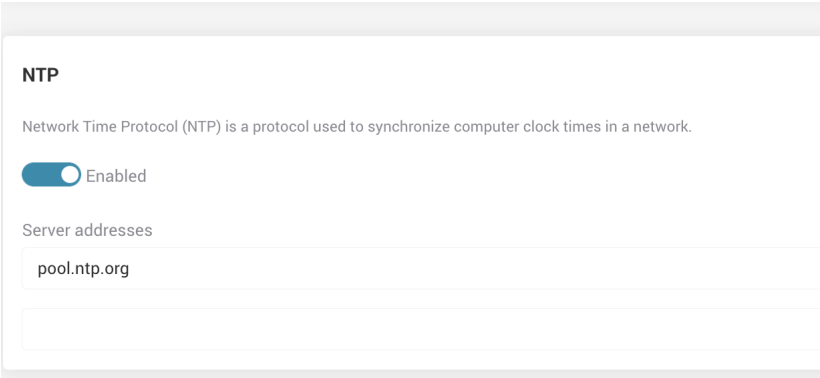


Figure 5.32.: NTP service tab

- 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.

Device Discovery

Device discovery allows your AP3400 board to advertise its capabilities, identity, and other information onto a LAN. Device discovery service also allows the AP3400 board to receive such information from other networked devices.

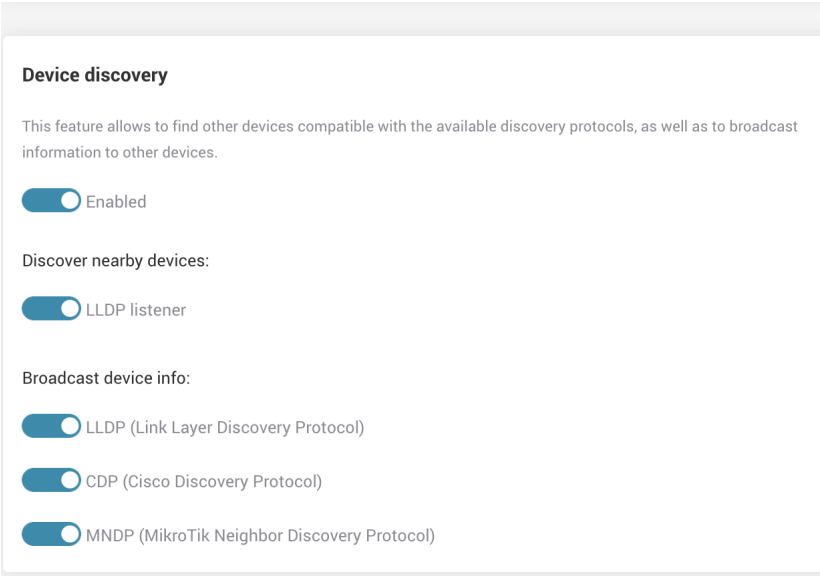


Figure 5.33.: Device discovery tab

Discover nearby devices service allows the AP3400 board to learn information about other devices on its network links:

- LLDP server - Link Layer Discovery Protocol (LLDP) server - allows the AP3400 board to learn information about other devices on its LAN network links. Such information, when available, is displayed under Settings -> Tools -> Device discovery.

Broadcast device info allows your AP3400 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 Services

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.

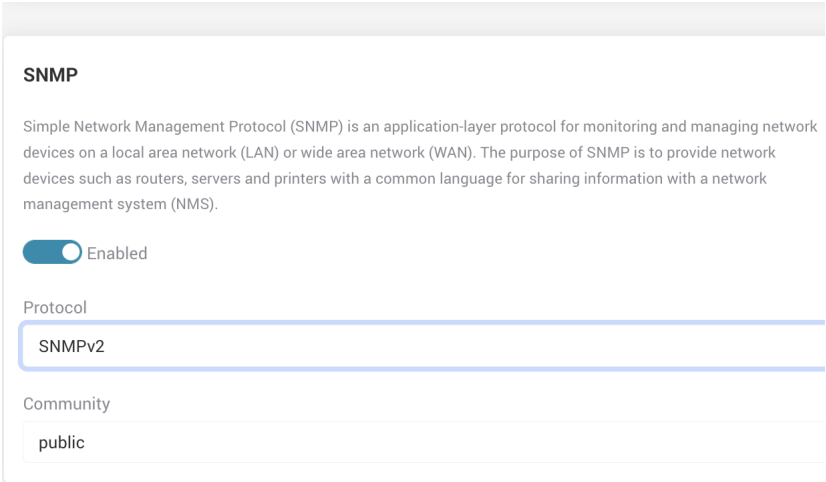


Figure 5.34.: SNMP service tab

AP3400 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).

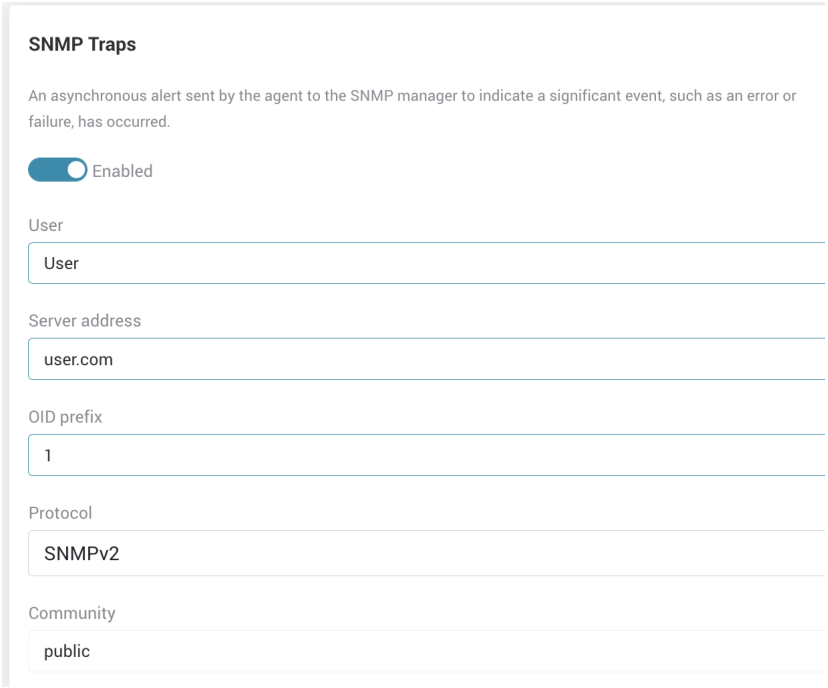


Figure 5.35.: SNMP Traps

- 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 - 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.

For SNMPv3 Protocol AP3400 uses such configuration:

- ***Authentication protocol: SHA***
- ***Security level: AuthPriv (Authentication and privacy policy)***
- ***Privacy protocol: AES***

Remote Syslog

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

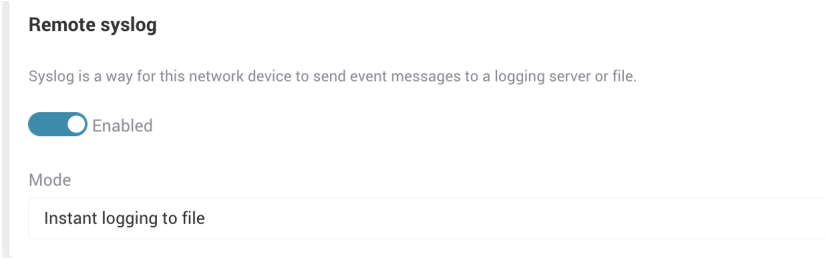


Figure 5.36.: Remote Syslog

- 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 under "/etc/logread.out" address.
- 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.

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.

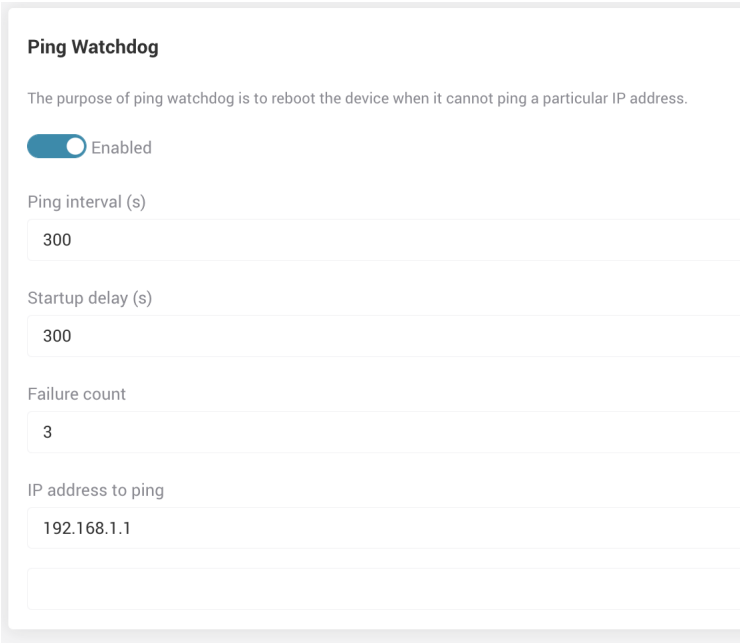


Figure 5.37.: Ping Watchdog Settings

5.2.4. System Configuration

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

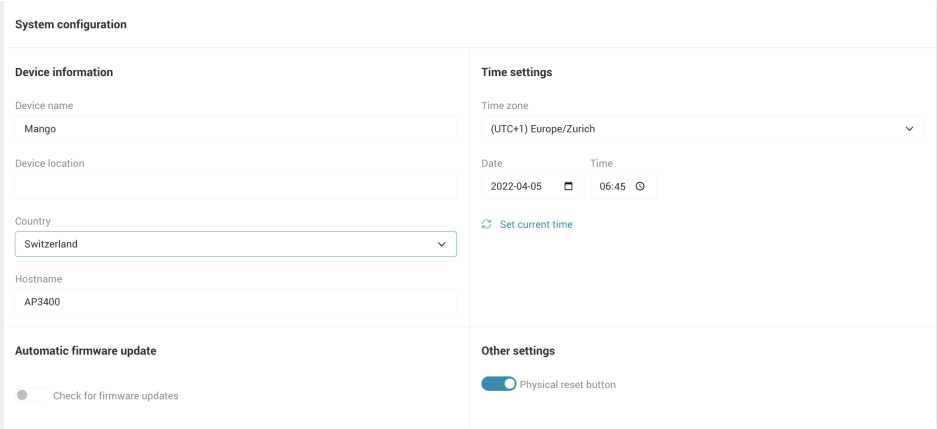


Figure 5.38.: System Configuration Settings

Country and time settings

Country - select the country in which your AP3400 device is located. Different countries / regions have different regulations for wireless radio usage. It is important to select your actual country, so your AP3400 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 drop-down, and from the Date and Time selectors.

Device name, location and hostname

The information you enter in the three textual fields describing your AP3400 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.

- 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 identificator 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).

Automatic update checker

With the automatic update functionality, your AP3400 board is able to periodically check for newer firmware versions. Whenever new firmware is available on the server, your AP3400 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.

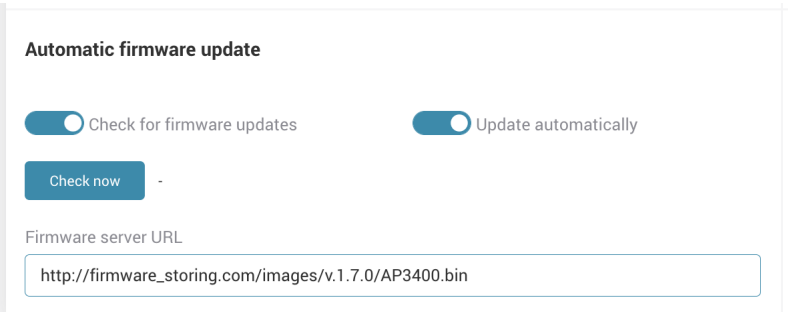


Figure 5.39.: Automatic Updater Settings

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, AP3400 will automatically update (without notifying the user) when new firmware is available.
- "Check now" button - click if you want AP3400 to check for an update at that moment. Link: https://share.netmodule.com/public/system-software/firmware/
- 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.

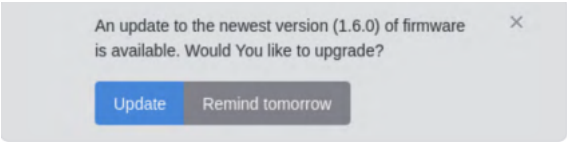


Figure 5.40.: Firmware Updater Notification

Physical reset button

AP3400 physical reset button has a capability to enable or disable the functioning of it.

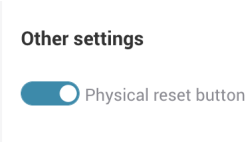


Figure 5.41.: Physical Reset Button

5.2.5. User Configuration

In AP3400 you can additional users, give them different access of **Admin**, **Installer**, **Observer**.

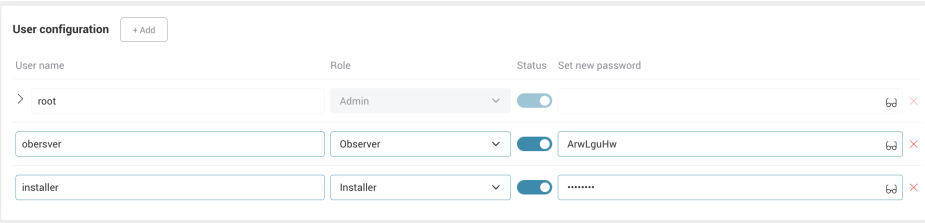


Figure 5.42.: User Configuration

- User name - must consist of 1-24 symbols. Special symbols are not valid.
- Roles:
  - Admin - has root privileges, can access and change device parameters, make configuration resets.
  - Installer - only able to view parameters and install firmware on the device.
  - Observer - user which can only view device parameters.
- Status - you can disable certain user without deleting them.

– Password - consists of 5-32 symbols, special characters not allowed. Automatically generates a random password when new "+Add" is pressed. Can be viewed by pressing glasses icon on the right.

5.3. Tools

AP3400 Website interface has useful tools for troubleshooting, gathering information or performing various tests on the device. To utilise them go to Tools section on the side menu.

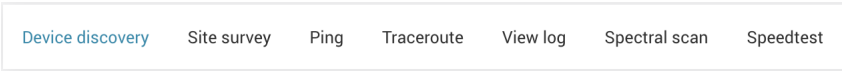


Figure 5.43.: Tools Menu

5.3.1. Device Discovery

Device detects other devices if they are advertising via LLDP, CPD or MDNP in the Network and displays them in this menu. Such information of the detected device is printed:

- Chassis ID
- Local Port ID
- Remote Port ID
- Management IPv4 address
- Management IPv6 address
- System Name
- System Description
- VLAN ID

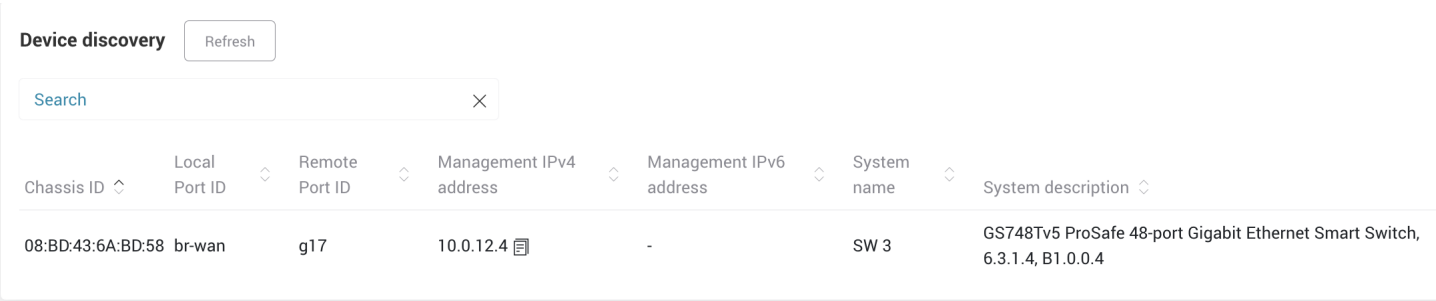


Figure 5.44.: Device discovery

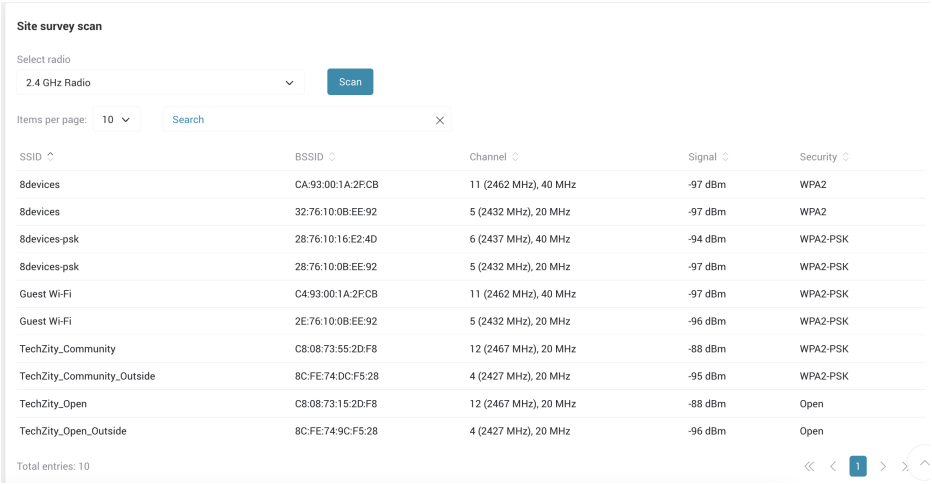
5.3.2. Site survey

Scans the network for wireless Access Points on a selection radio band.

Only activated radios will be shown in the selection.

Such information if presented:

- SSID
- BSSID
- Channel
- Signal
- Security



SSID	BSSID	Channel	Signal	Security
8devices	CA:93:00:1A:2F:CB	11 (2462 MHz), 40 MHz	-97 dBm	WPA2
8devices	32:76:10:0B:EE:92	5 (2432 MHz), 20 MHz	-97 dBm	WPA2
8devices-psk	28:76:10:16:E2:4D	6 (2437 MHz), 40 MHz	-94 dBm	WPA2-PSK
8devices-psk	28:76:10:0B:EE:92	5 (2432 MHz), 20 MHz	-97 dBm	WPA2-PSK
Guest Wi-Fi	C4:93:00:1A:2F:CB	11 (2462 MHz), 40 MHz	-97 dBm	WPA2-PSK
Guest Wi-Fi	2E:76:10:0B:EE:92	5 (2432 MHz), 20 MHz	-96 dBm	WPA2-PSK
TechZity_Community	C8:08:73:55:2D:F8	12 (2467 MHz), 20 MHz	-88 dBm	WPA2-PSK
TechZity_Community_Outside	8C:FE:74:DC:F5:28	4 (2427 MHz), 20 MHz	-95 dBm	WPA2-PSK
TechZity_Open	C8:08:73:15:2D:F8	12 (2467 MHz), 20 MHz	-88 dBm	Open
TechZity_Open_Outside	8C:FE:74:9C:F5:28	4 (2427 MHz), 20 MHz	-96 dBm	Open

Figure 5.45.: Site Survey Scan results

5.3.3. Ping

Ping tools lets you ping IPv4 or IPv6 address with iteration of pings. The result is shown in a Unix style.

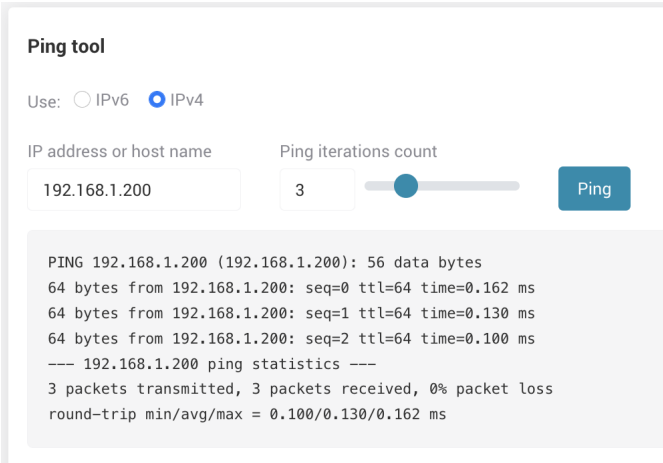


Figure 5.46.: Ping results

5.3.4. Traceroute

It is a network tool used to determine the path of the packets take from one IP address to another. It provides the hostname, IP address, and the response time to a ping. Enter the IPv4 or IPv6 address that you want to lookup and the output will be shown in Unix style.

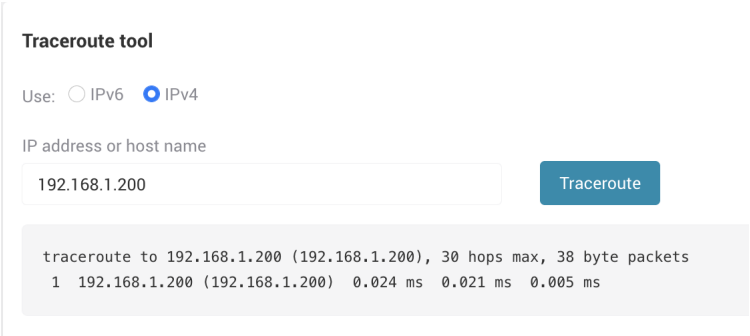


Figure 5.47.: Traceroute results

5.3.5. Device log

This tool shows the information from the device log, if there were any errors on the device backend. There is a search function to search for certain logs.

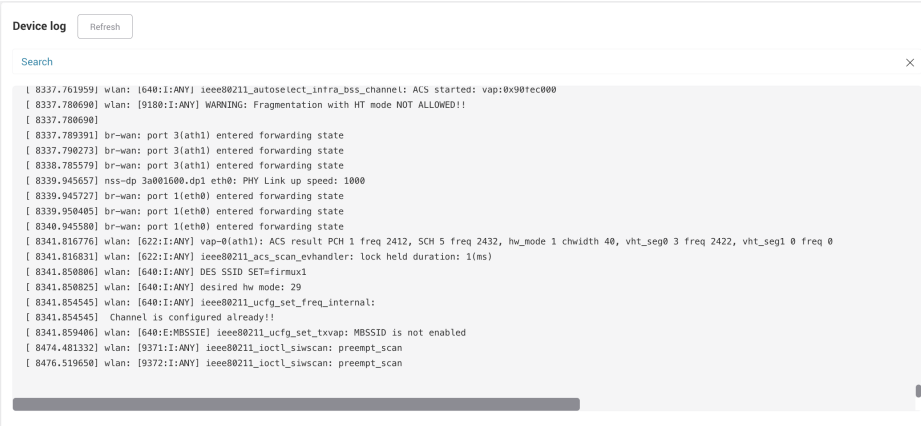


Figure 5.48.: Device log

5.3.6. Speedtest

AP3400 is able to perform speedtest, it is required for the board to reach internet in order to connect to the servers to test speed.

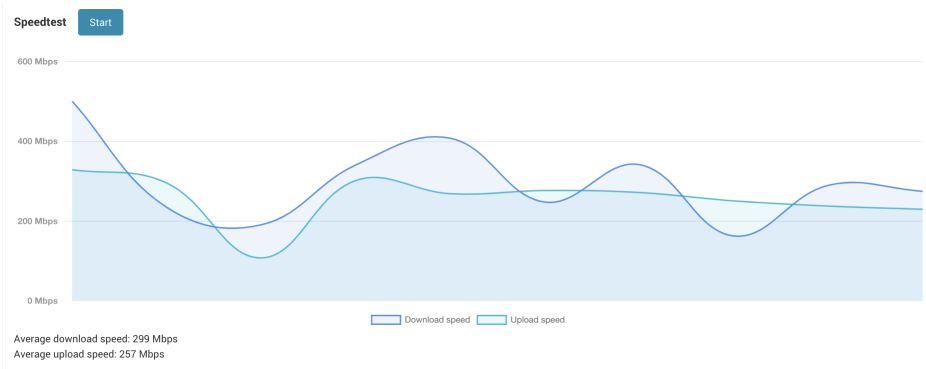


Figure 5.49.: Speedtest results

A. Appendix

A.1. Abbrevations

Abbreviation	Description
ANY	Generally includes all options offered by the current section
APN	Access Point Name
ASU	Arbitrary Strength Unit
CID	A Cell ID is a generally unique number used to identify each Base Transceiver Station (BTS).
CID	Cell-ID
CLI	Command Line Interface, a generic interface to query the router or perform system tasks
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ETHx	Corresponds to Ethernet interfaces (either single or switched ones)
FQDN	Fully qualified domain name
GHz	GigaHertz
GNSSx	Specifies a Global Navigation Satellite System module
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
ICCID	Integrated Circuit Card Identifier
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
INx	Specifies a digital I/O input port (DIx)
LAC	Location Area Code
LAC	The Location Area Code corresponds to an identifier of a set of base stations that are grouped together to optimize signaling
LAI	Location Area Identification
LAI	The Location Area Identity is a globally unique number that identifies the country, network provider and location area
LANx	LAN interfaces which are generally based on Ethernet interfaces (including bridges)
MAC	Media Access Control
Mbps	Megabits per second
MCC	Mobile Country Code
MCS	Modulation Coding Scheme

Abbreviation	Description
MEID	Mobile Equipment Identifier
MHz	MegaHertz
MNC	Mobile Network Code
Mobilex	Identifies a WWAN modem
MOBILEIPx	Refers to a Mobile IP tunnel interface
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NTP	Network Time Protocol
OUTx	Specifies a digital I/O output port (DOx)
PPTPx	Specifies a PPTP tunnel interface
PSK	Pre-Shared Key
RSRP	Referenz Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indication
SDK	Script Development Kit which can be used to program applications
SERIALx	Identifies a serial port
SIMx	Specifies the SIM slot as seen on the front panel
SIM	Subscriber Identity Module
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Service Set Identifiers, can be used to define multiple WLAN networks on a module
STP	Spanning Tree Protocol
TAPx	Specifies an OpenVPN tunnel interface (based on TAP)
TUNx	Specifies an OpenVPN tunnel interface (based on TUN)
USSD	Unstructured Supplementary Service Data
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol

Abbreviation	Description
WAN	WAN links include all Wide Area Network interfaces which are currently activated in the system
WDS	Wireless Distribution System
WLANx	Refers to a Wireless LAN interface which will be represented as additional LAN interface when configured as access point
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
WWANx	Refers to a Wireless Wide Area Network (2G/3G/4G) connection

Table A.1.: Abbreviations

In general, internal interfaces are written lower-case and may have a different naming. Their index starts from zero, whereas interfaces seen by the user will be written in capital letters starting from one.