INFINITY

NFT series 7.3

User Guide

Revision 1.0
February 20, 2015

LigoWave

Copyright

Notice

LigoWave 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. LigoWave 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 is subject to written authorization from LigoWave.

Trademarks

FCC warning

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 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.

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.

FCC caution

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC radiation exposure statement

To comply with FCC RF exposure requirements in section 1.1307, a minimum separation distance of 3.9 feet is required between the antenna and all occupational persons, and a minimum separation distance of 8.7 feet is required between the antenna and all public persons.

CE mark warning

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

R&TTE compliance statement

This equipment complies with all the requirements of the Directive 1999/5/EC of the European Parliament and the Council of 9 March 1999 on Radio Equipment and Telecommunication Terminal Equipment and the Mutual Recognition of their Conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this manual and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

EU countries intended for use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, The Netherlands, Portugal, Spain, Sweden and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

EU countries not intended for use

None.

Contents

About This Guide

Purpose

This document provides information and procedures on installation, setup, configuration, and management of the LigoWave NFT unit.

Definitions, acronyms and abbreviations

The following typographic conventions and symbols are used throughout this document:

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

! Important information that should be observed.

bold Menu commands, buttons, input fields, links, and configuration keys are displayed in bold

italic References to sections inside the document are displayed in italic.

`code` File names, directory names, form names, system-generated output, and user typed entries are displayed in constant-width type

Abbreviation list

Abbreviation	Description
ACL	Access Control List
ACK	Acknowledgement
AES	Advanced Encryption Standard
AMSDU	Aggregated Mac Service Data Unit
AP	Access Point
ATPC	Automatic Transmit Power Control
DHCP	Dynamic Host Control Protocol
EAP	Extensible Authentication Protocol
GHz	Gigahertz
GMT	Greenwich Mean Time.
GUI	Graphical User Interface
IEEE	Institute of Electrical and Electronics Engineers
ISP	Internet Service Provider
IP	Internet Protocol
LAN	Local Area Network
LED	Light-Emitting Diode
MAC	Media Access Control
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MHz	Megahertz

Abbreviation	Description
MSCHAPv2	Microsoft version of the Challenge-handshake authentication protocol, CHAP.
NTP	Network Time Protocol
PC	Personal Computer
PSK	Pre-Shared Key
PEAP	Protected Extensible Authentication Protocol
RADIUS	Remote Authentication dial In User Service
RSSI	Received Signal Strength Indication – received signal strength in mV, measured on BNC outdoor unit connector
RX	Receive
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TTLS	Tunneled Transport Layer Security (EAP-TTLS) protocol
TX	Transmission
UDP	User Datagram Protocol
VAP	Virtual AP
VLAN	Virtual Local Area Network
WACL	Wireless Access Control List
WISPr	Wireless Internet Service Provider roaming
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

Device Access

First connection via Ethernet

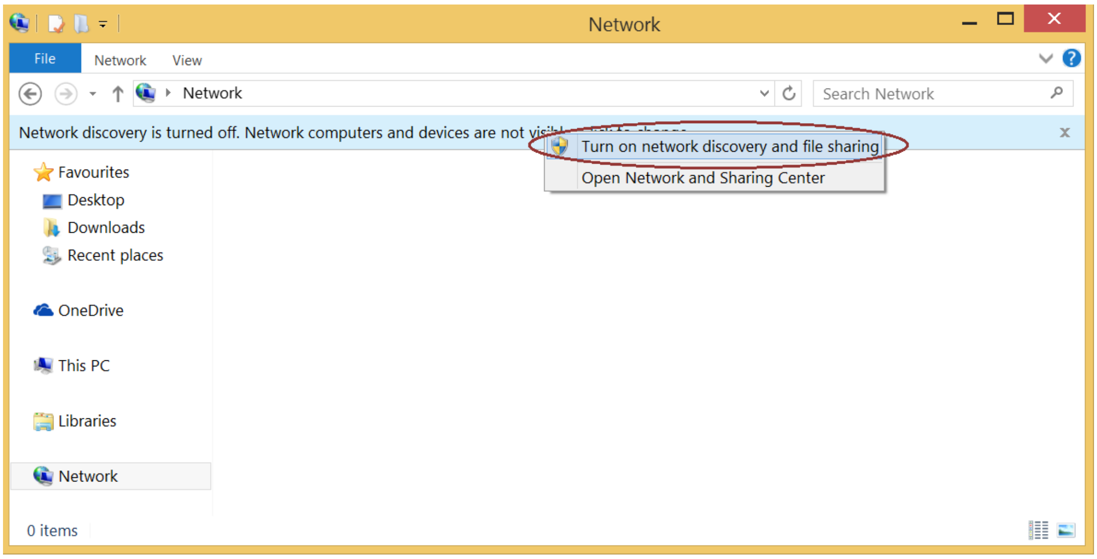
By default LigoWave NFT device obtains the IP address from the DHCP server. Follow the steps to access device on different OS:

In case the LigoWave NFT device is unable to obtain IP address from a DHCP server, it fallback to the default static IP 192.168.2.66.

Windows OS

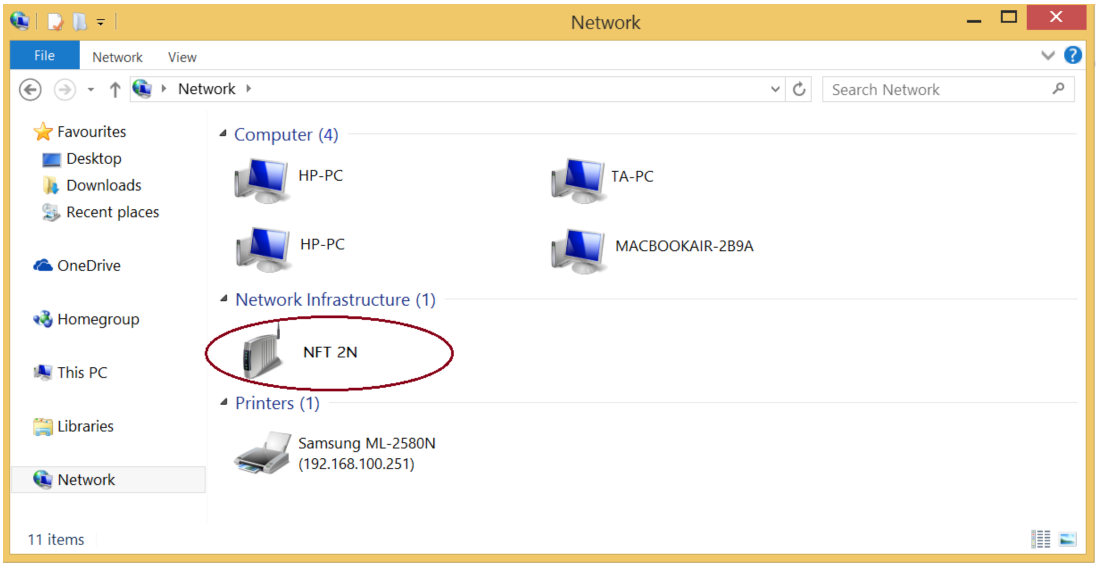
Step 1: Connect your PC directly to the LigoWave NFT device via Ethernet.

Step 2: Open Windows **Explorer**, click on **Network** drive, and turn on **Network discovery**:



Network discovery is turned off. Network computers and devices are not visibl

Step 3: Find the required LigoWave NFT device icon:

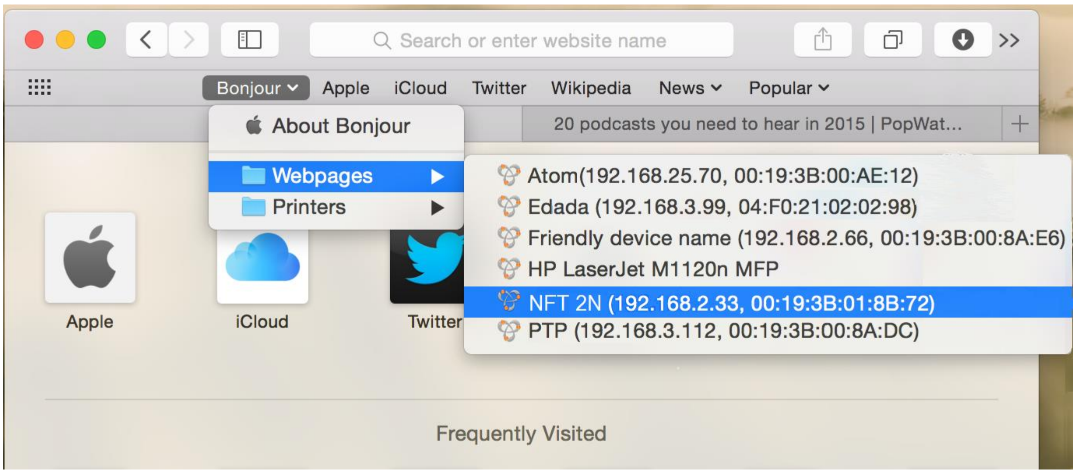


Step 4. Double-click on LigoWave NFT device icon – you will be redirected to the device webpage automatically.

MAC OS

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

Step 2: Run **Bonjour** application, click on **Webpages** and find the required LigoWave NFT device name:

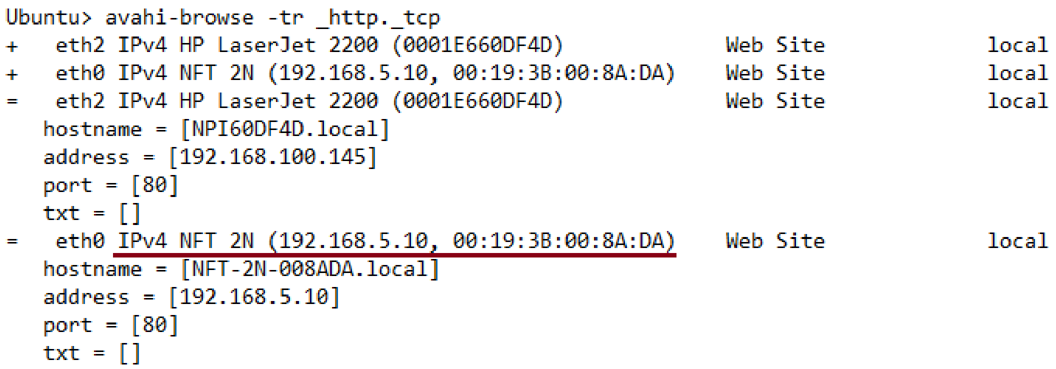

Search or enter website name
Bonjour
Apple
iCloud
Twitter
Wikipedia
News
Popular
About Bonjour
Webpages
Printers
20 podcasts you need to hear in 2015 | PopWat...
Atom(192.168.25.70, 00:19:3B:00:AE:12)
Edada (192.168.3.99, 04:F0:21:02:02:98)
Friendly device name (192.168.2.66, 00:19:3B:00:8A:E6)
HP LaserJet M1120n MFP
NFT 2N (192.168.2.33, 00:19:3B:01:8B:72)
PTP (192.168.3.112, 00:19:3B:00:8A:DC)
Apple
iCloud
Twitter
Frequently Visited

Step 3: Click on the selected item and the device web management interface will be loaded on the default web browser.

Linux (Ubuntu)

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

Step 2: Open terminal application GNOME Terminal (or Konsole for Kubuntu) and type command "`avahi-browse -tr _http._tcp`". Find the IP address of the required LigoWave device in the received output:



```
Ubuntu> avahi-browse -tr _http._tcp
+   eth2 IPv4 HP LaserJet 2200 (0001E660DF4D)          Web Site             local
+   eth0 IPv4 NFT 2N (192.168.5.10, 00:19:3B:00:8A:DA)  Web Site             local
=   eth2 IPv4 HP LaserJet 2200 (0001E660DF4D)          Web Site             local
   hostname = [NPI60DF4D.local]
   address = [192.168.100.145]
   port = [80]
   txt = []
=   eth0 IPv4 NFT 2N (192.168.5.10, 00:19:3B:00:8A:DA)  Web Site             local
   hostname = [NFT-2N-008ADA.local]
   address = [192.168.5.10]
   port = [80]
   txt = []
```

Step 3: Open a web browser ant type discovered IP in the address field to open device web management interface.

First access to web management interface

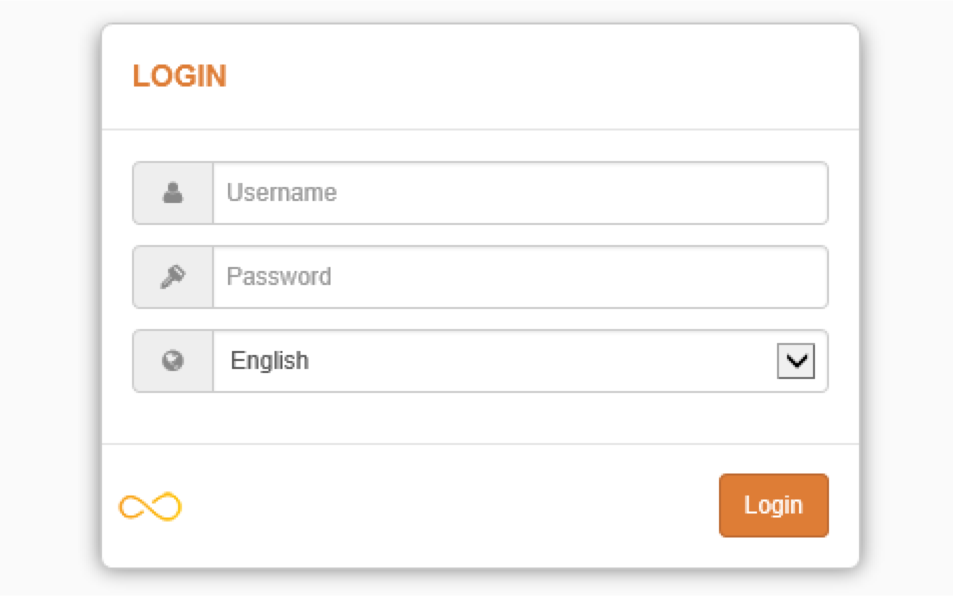
The default administrator login settings are:
Login: **admin**
Password: **admin01**

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

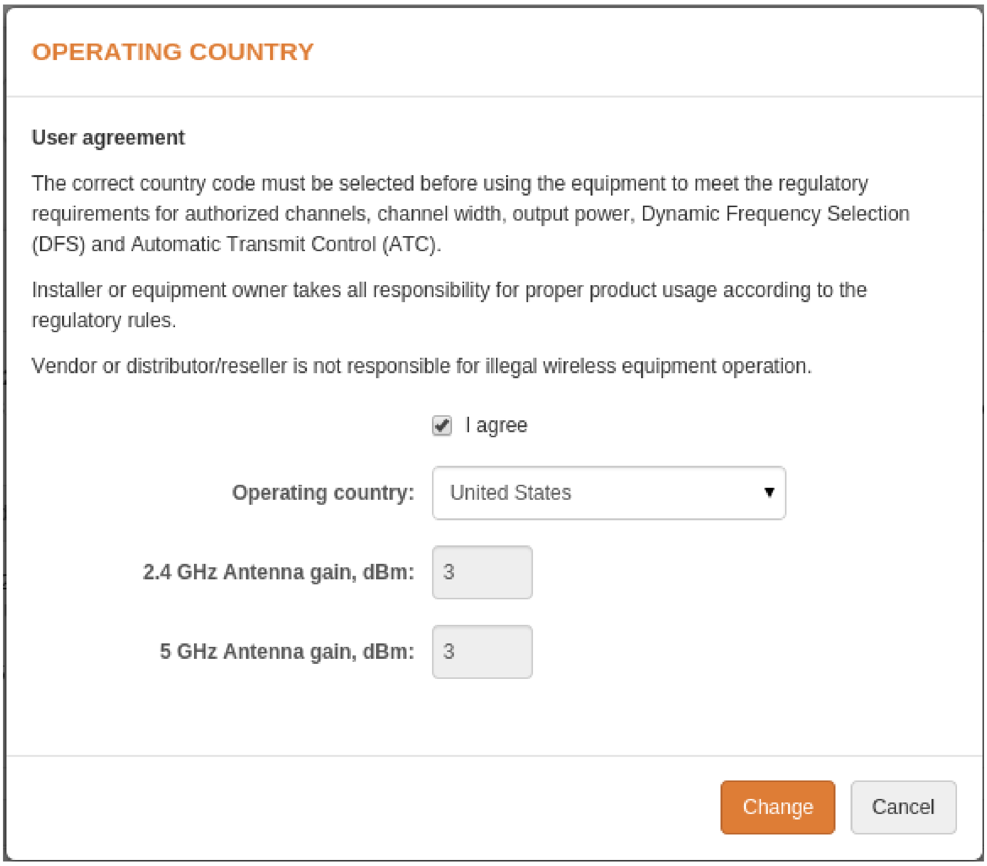
Step 1. Start your Web browser.

Step 2. Enter the device IP address in the web browser's IP field and specify default login settings **admin/admin01**.

The initial login screen looks as follow:



Step 3. **Confirm the user agreement.** According to the chosen country the regulatory domain settings may differ. You are not allowed to select radio channels and RF output power values other the permitted values for your country and regulatory domain.



OPERATING COUNTRY

User agreement

The correct country code must be selected before using the equipment to meet the regulatory requirements for authorized channels, channel width, output power, Dynamic Frequency Selection (DFS) and Automatic Transmit Control (ATC).

Installer or equipment owner takes all responsibility for proper product usage according to the regulatory rules.

Vendor or distributor/reseller is not responsible for illegal wireless equipment operation.

☑ I agree

Operating country: United States

2.4 GHz Antenna gain, dBm: 3

5 GHz Antenna gain, dBm: 3

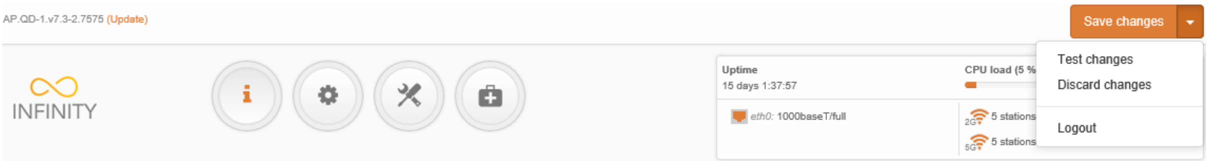
Step 4. After successful administrator login you will see the main page of the device Web management interface. The device now is ready for configuration.

LigoWave NFT Configuration

This document contain product‘s powerful web management interface configuration description allowing setups ranging from very simple to very complex.

Appling and saving configuration changes

There is one general button containing three actions located on the right top corner of the WEB GUI allowing managing device configuration:



Uptime 15 days 1:37:57

CPU load (5 %

eth0: 1000baseT/full

2G 5 stations

5G 5 stations

Save changes – if pressed new configuration settings are applied instantly and written to the permanent device memory.

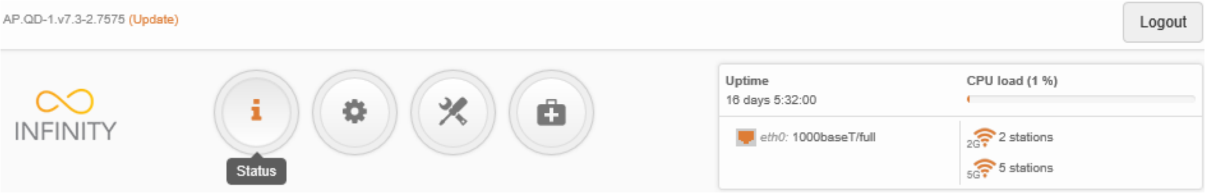
Test changes – if pressed the device will start operating with newly set configuration settings for 3 minutes. During this test time the administrator is able to gauge if device is working properly, and then Save changes. In case wrong settings were chosen (or even after faulty settings administrator have lost connection with the device), the device automatically reverts back configuration to an old one.

Discard changes – if pressed parameter changes are discarded. It should be noted that if Save changes is pressed it is not possible to discard changes.

It is not required to press **Save changes** in every Web GUI tab. The device remembers all changes made in every tab and after action button is used, all changes will be applied.

Status

After login, the main Web management page displays Status Information page. The header of Web management page displays main information about device: Firmware version, Product name, Uptime, CPU load, Ethernet port(s) status, Connected client count.



Uptime 16 days 5:32:00

CPU load (1 %)

eth0: 1000baseT/full

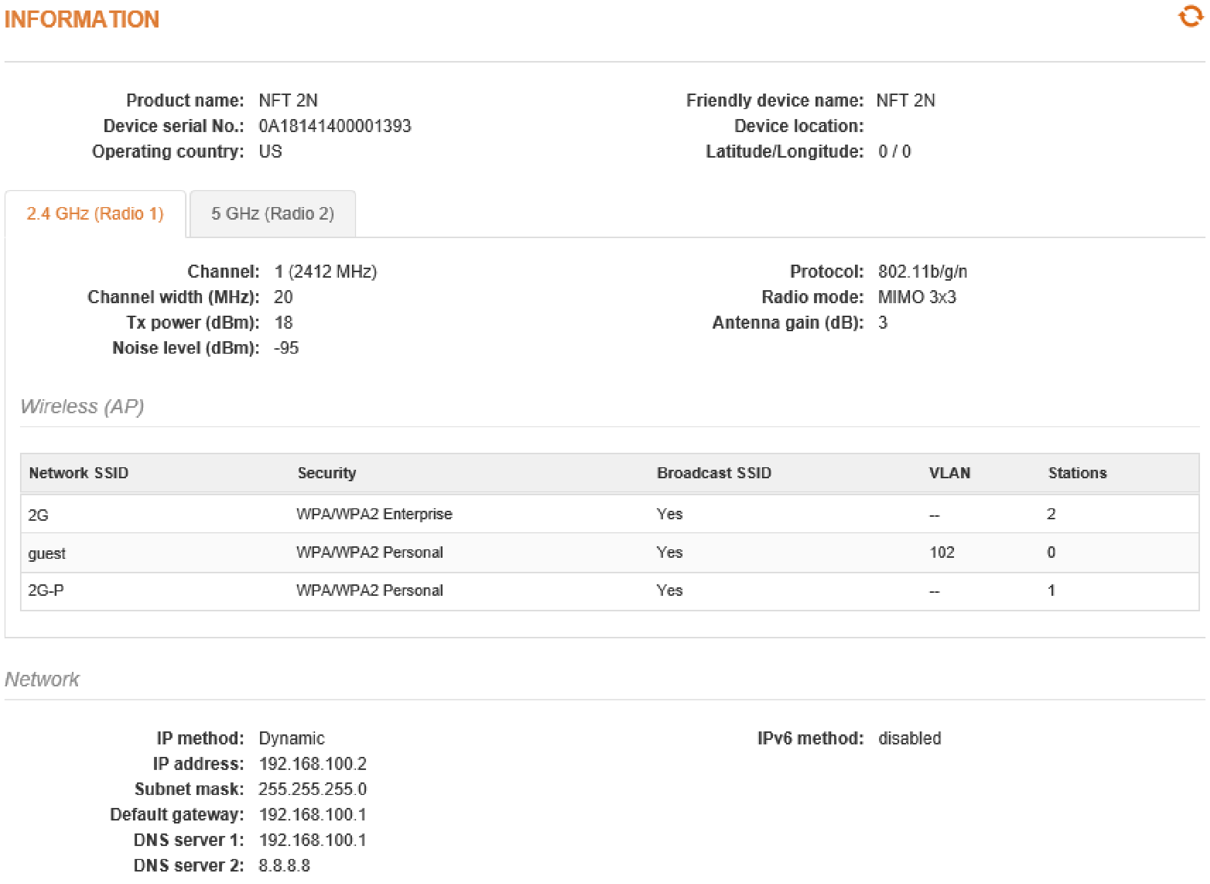
2G 2 stations

5G 5 stations

Figure 1 - Web Management Interface

Information

The Information page displays a summary of status information of your device. It shows important information for the LigoWave NFT operating mode, radio and network settings.



INFORMATION

Product name: NFT 2N
Device serial No.: 0A18141400001393
Operating country: US

Friendly device name: NFT 2N
Device location:
Latitude/Longitude: 0 / 0

Channel: 1 (2412 MHz)
Channel width (MHz): 20
Tx power (dBm): 18
Noise level (dBm): -95

Protocol: 802.11b/g/n
Radio mode: MIMO 3x3
Antenna gain (dB): 3

Wireless (AP)

Network SSID	Security	Broadcast SSID	VLAN	Stations
2G	WPA/WPA2 Enterprise	Yes	--	2
guest	WPA/WPA2 Personal	Yes	102	0
2G-P	WPA/WPA2 Personal	Yes	--	1

Network

IP method: Dynamic
IP address: 192.168.100.2
Subnet mask: 255.255.255.0
Default gateway: 192.168.100.1
DNS server 1: 192.168.100.1
DNS server 2: 8.8.8.8

IPv6 method: disabled

Figure 2 – Device Information Page

The Information page of a dual-band device is divided into two tabs (for 2.4GHz and 5GHz radio), each containing appropriate information.

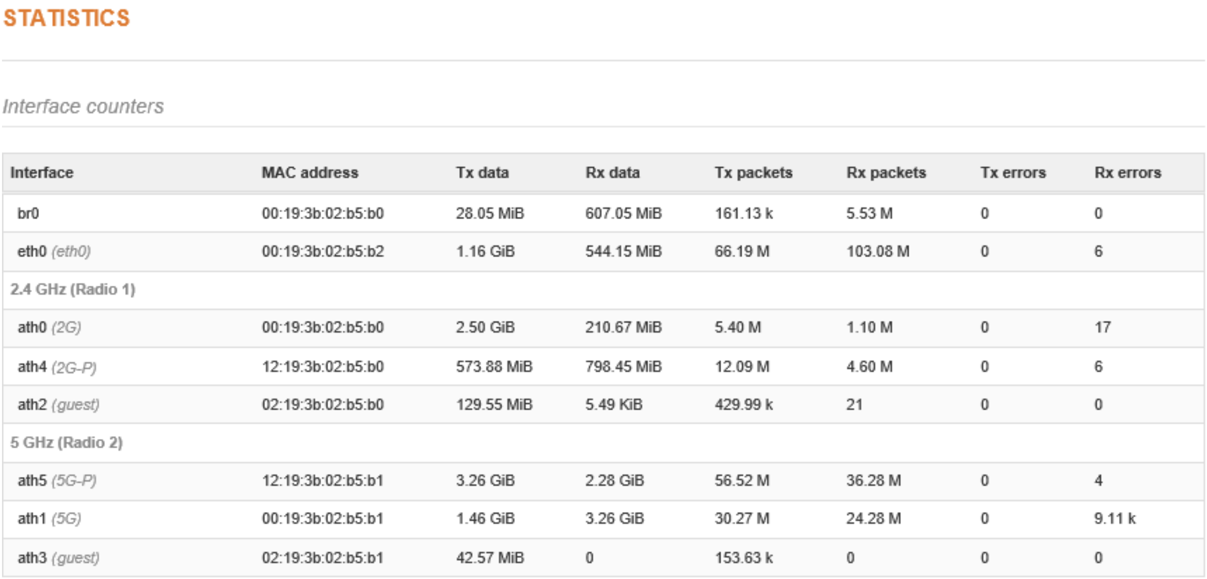
Wireless (AP) – table displays general VAP (Virtual AP) information: SSID, Security type, SSID Broadcast status, VLAN and number and connected clients.

Network– displays a short summary about current network configuration.

Click the refresh ⟳ icon, on the upper right corner, to update information.

Statistics

The **Statistics** sections id divided into two sections and displays network interface counters and traffic graphs of wired and wireless interfaces:



STATISTICS

Interface counters

Interface	MAC address	Tx data	Rx data	Tx packets	Rx packets	Tx errors	Rx errors
br0	00:19:3b:02:b5:b0	28.05 MiB	607.05 MiB	161.13 k	5.53 M	0	0
eth0 *(eth0)*	00:19:3b:02:b5:b2	1.16 GiB	544.15 MiB	66.19 M	103.08 M	0	6
2.4 GHz (Radio 1)							
ath0 *(2G)*	00:19:3b:02:b5:b0	2.50 GiB	210.67 MiB	5.40 M	1.10 M	0	17
ath4 *(2G-P)*	12:19:3b:02:b5:b0	573.88 MiB	798.45 MiB	12.09 M	4.60 M	0	6
ath2 *(guest)*	02:19:3b:02:b5:b0	129.55 MiB	5.49 KiB	429.99 k	21	0	0
5 GHz (Radio 2)							
ath5 *(5G-P)*	12:19:3b:02:b5:b1	3.26 GiB	2.28 GiB	56.52 M	36.28 M	0	4
ath1 *(5G)*	00:19:3b:02:b5:b1	1.46 GiB	3.26 GiB	30.27 M	24.28 M	0	9.11 k
ath3 *(guest)*	02:19:3b:02:b5:b1	42.57 MiB	0	153.63 k	0	0	0

Figure 3 – Network Statistics: Interface counters

Interface counters – displays table of interface statistics. The SSID name is displayed in the brackets near the radio interface (and VAPs).

MAC address– displays the MAC address of the particular interface.

Tx data – displays the transmitted data.

Rx data – displays the received data.

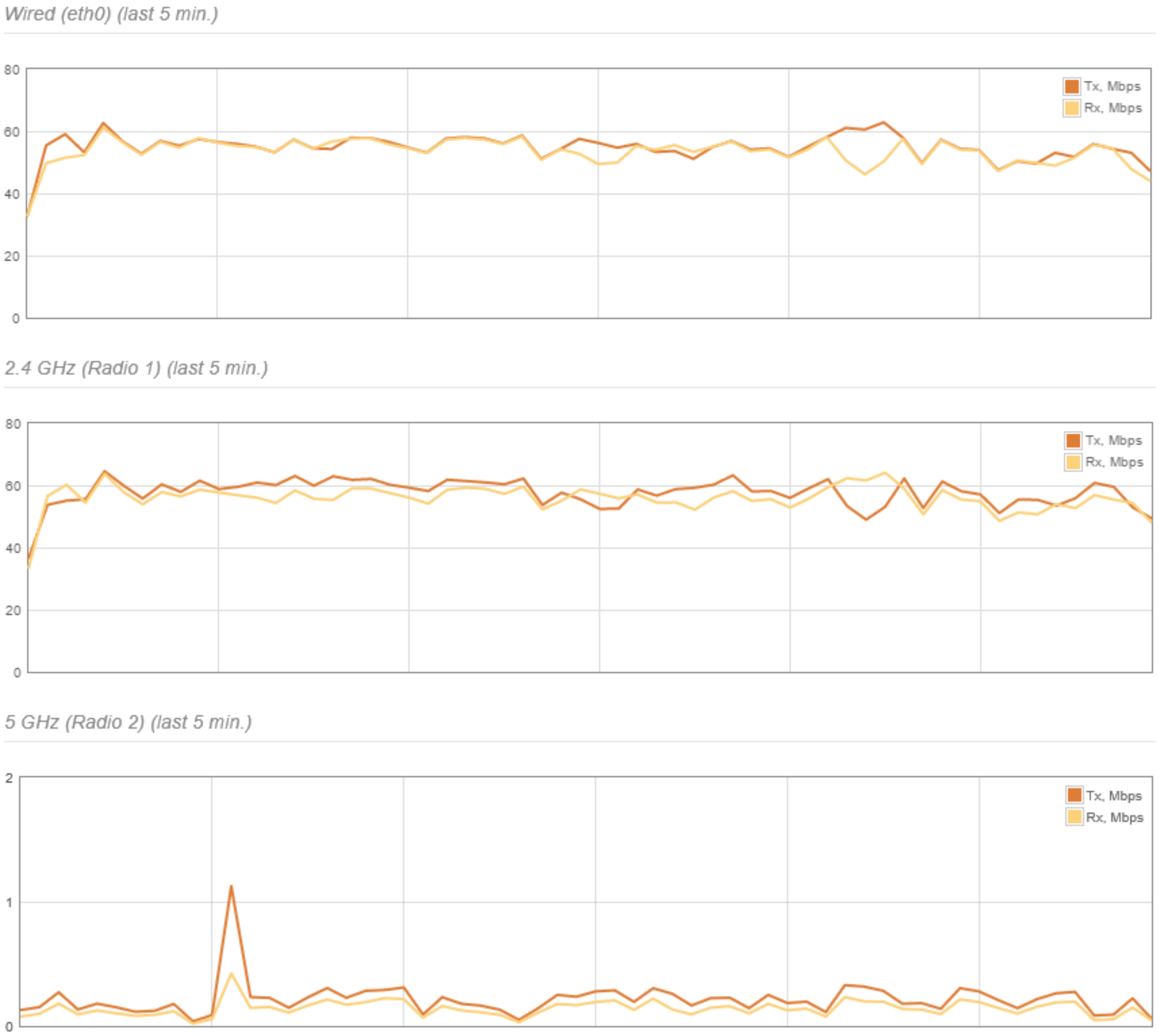
Tx packets – displays the number of transmitted packets.

Rx packets – displays the number of received packets.

Tx errors – displays the number of the TX errors.

Rx errors – displays the number of the RX errors.

The wired and wireless interface graphs display real-time data traffic.



Wired (eth0) (last 5 min.)

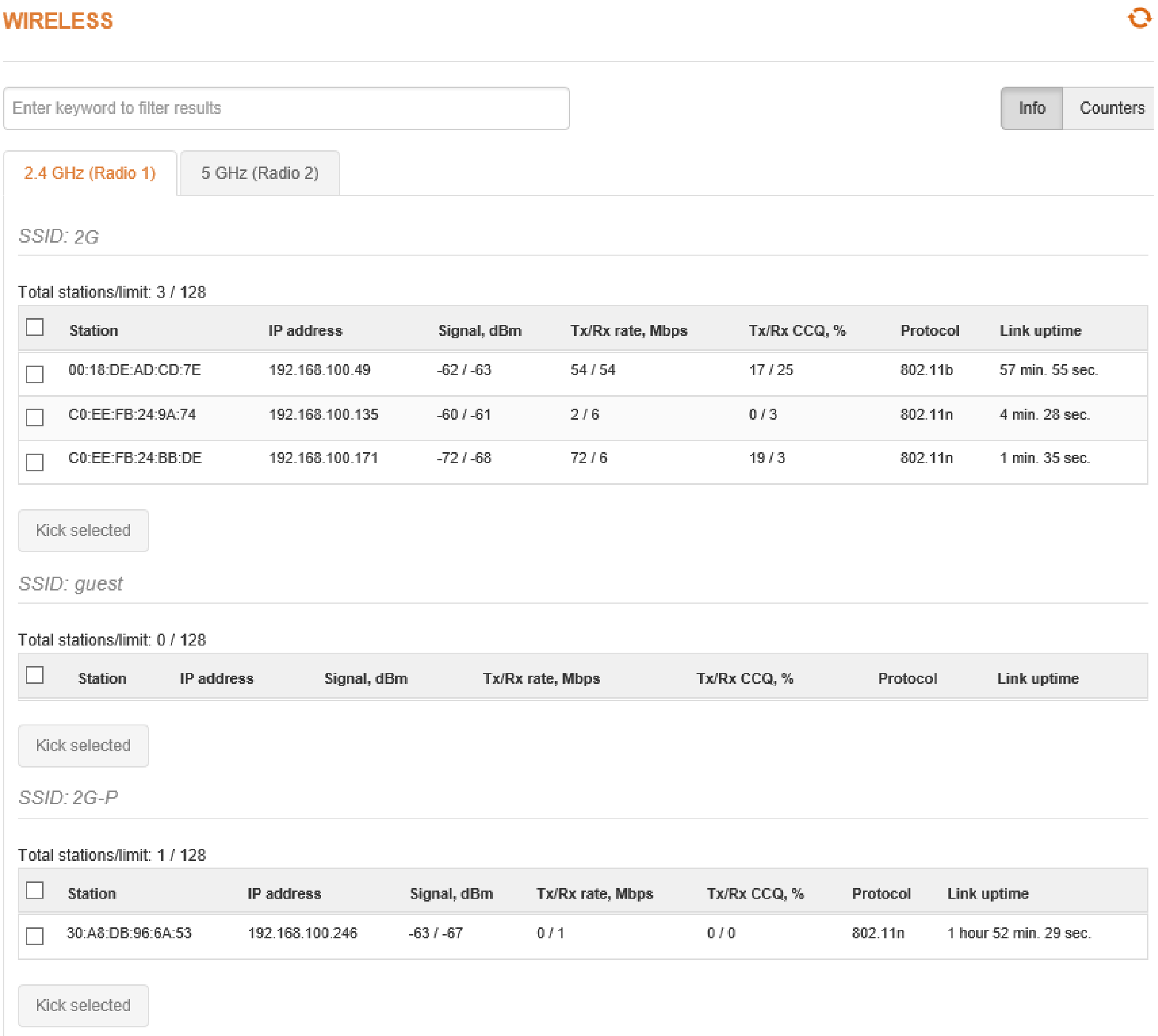
2.4 GHz (Radio 1) (last 5 min.)

5 GHz (Radio 2) (last 5 min.)

Figure 4 – Network Statistics: Graphs

Wireless

The Wireless page displays the receive/transmit statistics between AP and successfully associated wireless clients (click **Counters** tab, if necessary to view information of connected clients in Rx/Tx numerical expressions):



SSID: 2G

Total stations/limit: 3 / 128

□	Station	IP address	Signal, dBm	Tx/Rx rate, Mbps	Tx/Rx CCQ, %	Protocol	Link uptime
□	00:18:DE:AD:CD:7E	192.168.100.49	-62 / -63	54 / 54	17 / 25	802.11b	57 min. 55 sec.
□	C0:EE:FB:24:9A:74	192.168.100.135	-60 / -61	2 / 6	0 / 3	802.11n	4 min. 28 sec.
□	C0:EE:FB:24:BB:DE	192.168.100.171	-72 / -68	72 / 6	19 / 3	802.11n	1 min. 35 sec.

SSID: guest

Total stations/limit: 0 / 128

□	Station	IP address	Signal, dBm	Tx/Rx rate, Mbps	Tx/Rx CCQ, %	Protocol	Link uptime

SSID: 2G-P

Total stations/limit: 1 / 128

□	Station	IP address	Signal, dBm	Tx/Rx rate, Mbps	Tx/Rx CCQ, %	Protocol	Link uptime
□	30:A8:DB:96:6A:53	192.168.100.246	-63 / -67	0 / 1	0 / 0	802.11n	1 hour 52 min. 29 sec.

Figure 5 – Access Point's Wireless Statistics

The Wireless page of a dual-band device is divided into two tabs (for 2.4GHz and 5GHz radio), each containing appropriate information.

In case the access point has more than one wireless interface (VAPs), the appropriate number of tables with information about connected wireless clients will be displayed.

Station – displays MAC address and Friendly name of the successfully connected wireless client.

IP address – displays wireless client IP address.

Signal – indicates the signal strength of the access point main and auxiliary antennas that the station communicates with displayed dBm.

Tx/Rx rate – displays transmit/receive data rates in Mbps.

Tx/Rx CCQ, % - displays the wireless Client Connection Quality (CCQ), the value in percent that shows how effective the bandwidth is used regarding the theoretically maximum available bandwidth.

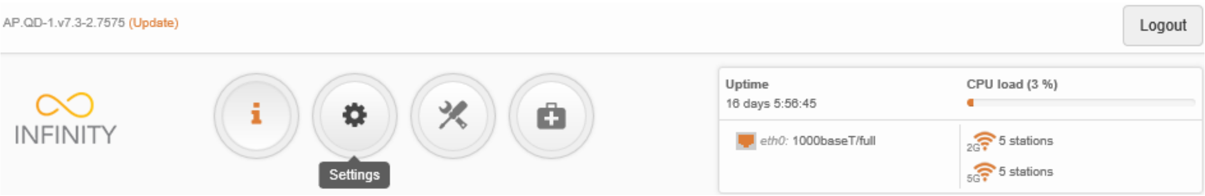
Protocol – displays the protocol at which the access point communicates with the particular station.

Link uptime – displays the duration of the particular session.

Kick selected – select to end the connection to this station.

Click the refresh ⟳ icon, on the upper right corner, to update statistics..

Settings


AP.QD-1.v7.3-2.7575 (Update)

Uptime
16 days 5:56:45

CPU load (3 %)

eth0: 1000baseT/full

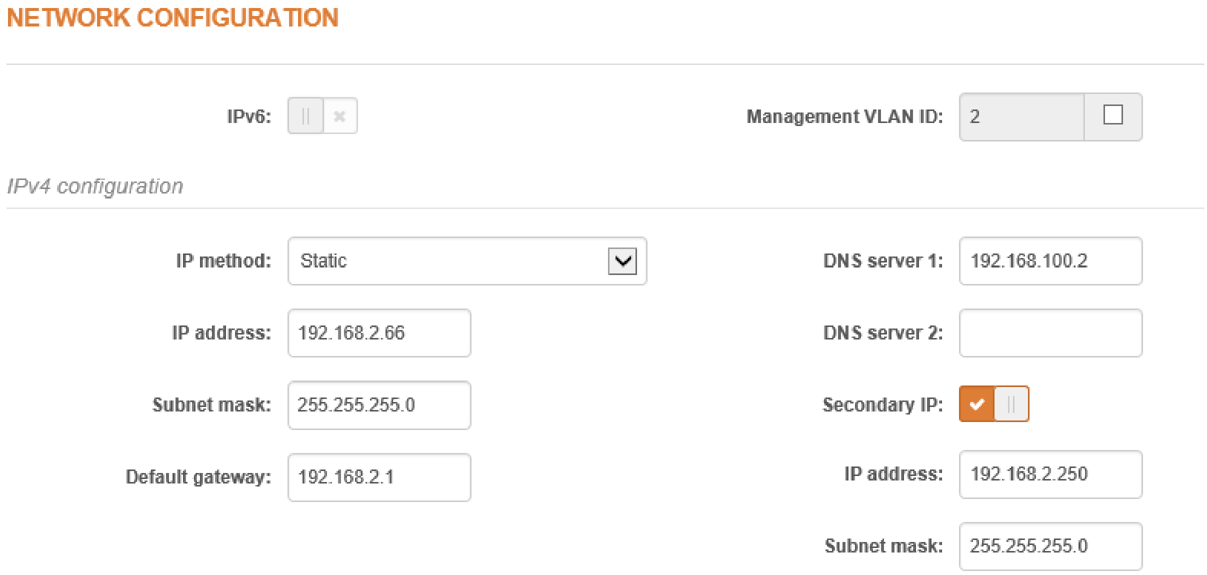
2G 5 stations

5G 5 stations

Network configuration

The **Settings | Network Configuration** page allows you to control the network LAN configuration of the device.

IPv4 configuration


NETWORK CONFIGURATION

IPv6: ☒

Management VLAN ID: 2 □

IPv4 configuration

IP method:	Static	DNS server 1:	192.168.100.2
IP address:	192.168.2.66	DNS server 2:	
Subnet mask:	255.255.255.0	Secondary IP:	✓
Default gateway:	192.168.2.1	IP address:	192.168.2.250
		Subnet mask:	255.255.255.0

Figure 6 – IPv4 LAN Settings

Management VLAN – select to enable a VLAN tagging for management traffic. Access to the AP for management purposes can further be limited using VLAN tagging. By defining Management VLAN, the device will only accept management frames that have the appropriate Management VLAN ID. All other frames using any management protocol will be rejected.

Management VLAN ID – specify the VLAN ID [2-4095]. When device interfaces are configured with a specific VLAN ID value, only management frames that matching configured VLAN ID will be accepted by device.

When you specify a new management VLAN, your HTTP connection to the device will be lost. For this reason, you should have a connection between your management device and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN router.

When assigning IP address make sure that the chosen IP address is unused and belongs to the same IP subnet as your wired LAN, otherwise you will lose the connection to the device from your current PC. If you enable the DHCP client, the browser will lose the connection after saving, because the IP address assigned by the DHCP server is not predictable.

IP method – specify IP reception method: IP addresses can either be retrieved from a DHCP server or configured manually:

- **Static** – the IP address must be specified manually.
- **Dynamic** – the IP address for this device will be assigned from the DHCP server. If DHCP server is not available, the device will try to get an IP. If has no success, it will use pre-configured fallback IP address. The fallback IP settings can be changed to custom values.

IP address – specify IP address for device

Subnet mask – specify a subnet mask for device.

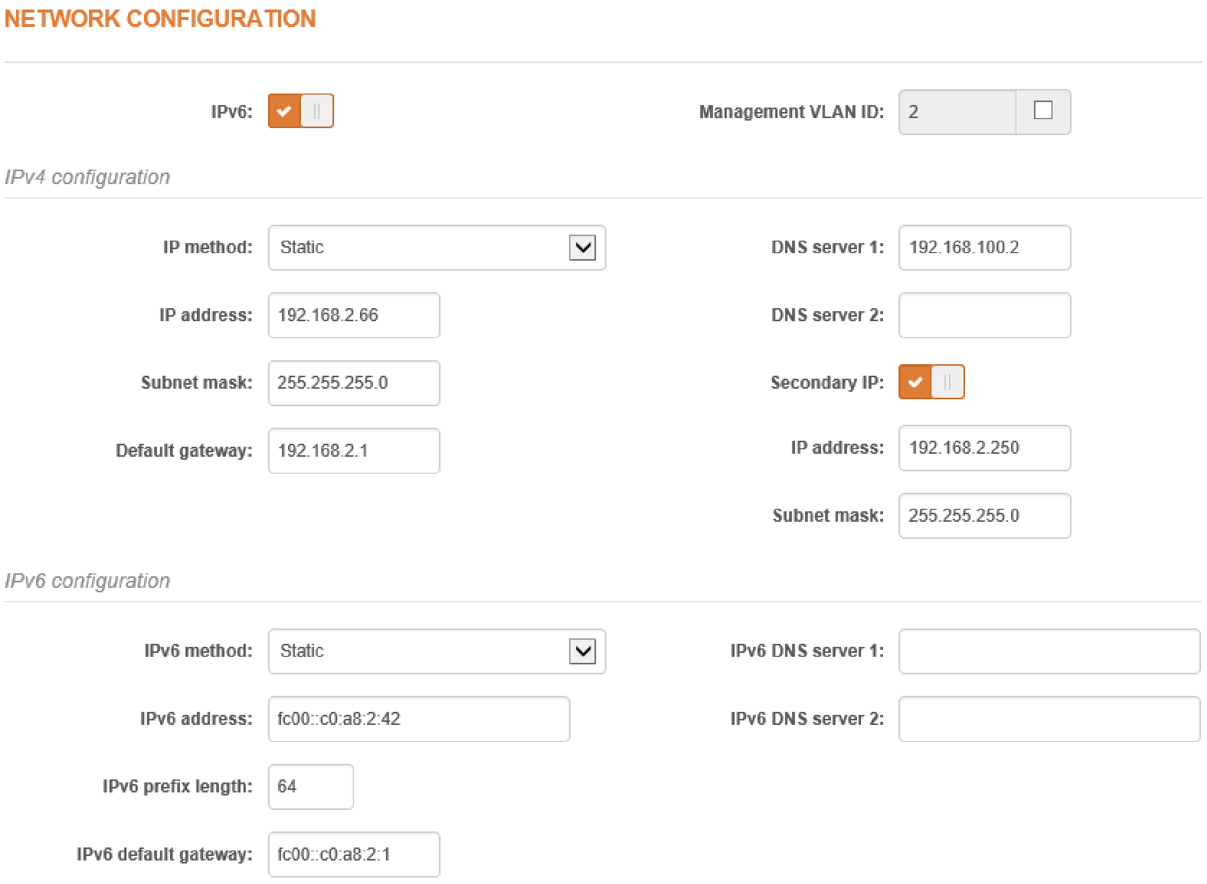
Default gateway – specify a gateway IP address for device.

DNS server – specify the Domain Naming Server.

Secondary IP – specify the alternative IP address and the netmask for LigoWave NFT unit management.

IPv6 configuration

Click the **IPv6** slide to enable IPv6 network configuration:



NETWORK CONFIGURATION

IPv6: ✓

Management VLAN ID: 2 □

IPv4 configuration

IP method: Static

IP address: 192.168.2.66

Subnet mask: 255.255.255.0

Default gateway: 192.168.2.1

DNS server 1: 192.168.100.2

DNS server 2:

Secondary IP: ✓

IP address: 192.168.2.250

Subnet mask: 255.255.255.0

IPv6 configuration

IPv6 method: Static

IPv6 address: fc00::c0:a8:2:42

IPv6 prefix length: 64

IPv6 default gateway: fc00::c0:a8:2:1

IPv6 DNS server 1:

IPv6 DNS server 2:

Figure 7 –IPv6 LAN Settings

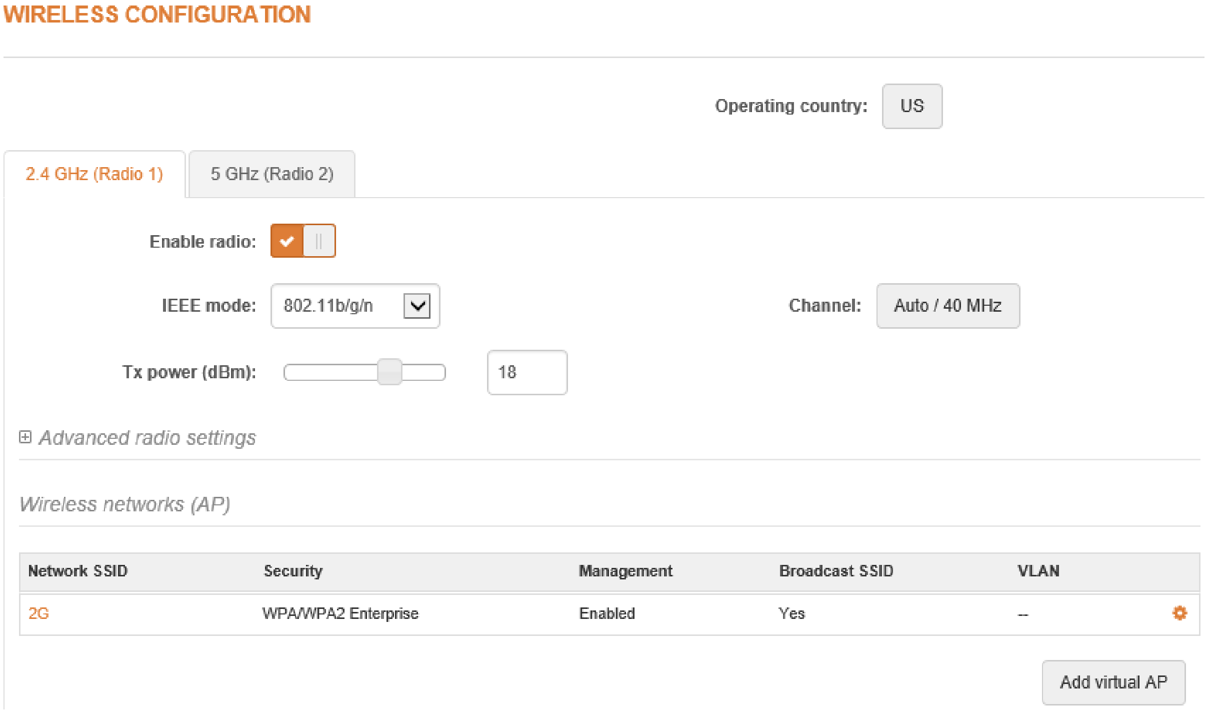
IPv6 method – specify IPv6 reception method: IPv6 addresses can either be retrieved from a DHCPv6 server or configured manually:

- **Dynamic stateless IP** – the DHCPv6 client only obtains network parameters other than IPv6 address
- **Dynamic stateful IP** – the DHCPv6 clients require IPv6 address together with other network parameters (e.g. DNS Server, Domain Name, etc.).
- **Static** – the IPv6 address must be specified manually.
  - **IPv6 address** – specify the **IPv6 Address** for the interface.
  - **IPv6 prefix length**– enter the **Prefix Length** for the address.
  - **IPv6 default gateway** – specify IPv6 address for default gateway.
  - **IPv6 DNS server** – specify the Domain Naming Server IPv6 addresses.

Wireless settings

Before changing radio settings manually verify that your settings will comply with local government regulations. At all times, it is the responsibility of the end-user to ensure that the installation complies with local radio regulations.

The Wireless page of the LigoWave NFT device web management is divided into two tabs (for 2.4GHz and 5GHz radio), each containing appropriate wireless settings:



WIRELESS CONFIGURATION

Operating country: US

Enable radio: ☑

IEEE mode: 802.11b/g/n

Channel: Auto / 40 MHz

Tx power (dBm): 18

Wireless networks (AP)

Network SSID	Security	Management	Broadcast SSID	VLAN
2G	WPA/WPA2 Enterprise	Enabled	Yes	--

Figure 8 – Wireless Configuration

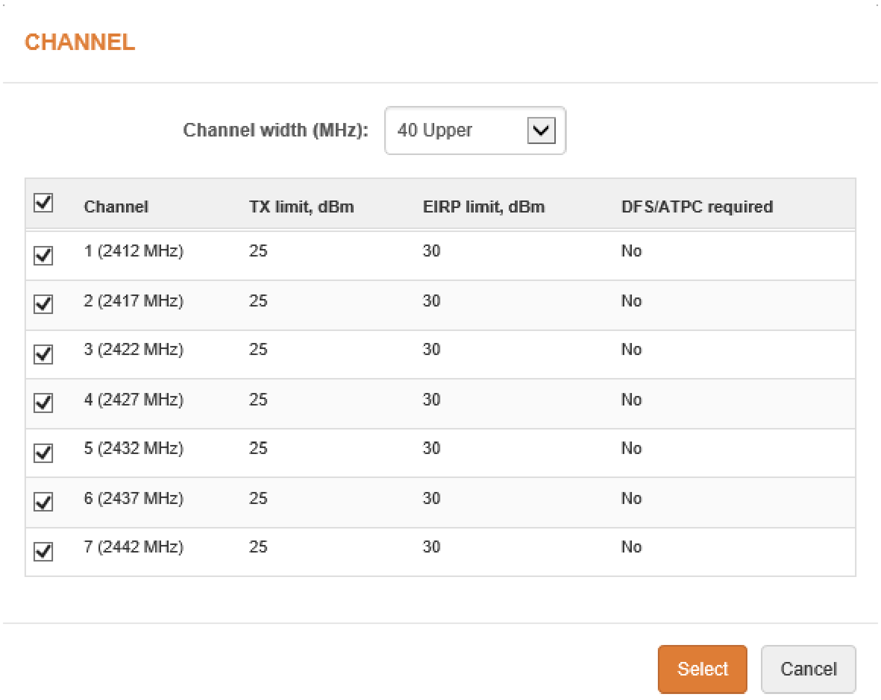
Operating country – displays LigoWave NFT unit operating country. The country selection determines the available channels and transmission power level based on regulatory restrictions in the operating country. The country has been selected on the first step of the LigoWave NFT unit's installation, though can be updated if required.

Enable radio – use slide to enable or disable particular LigoWave NFT radio.

IEEE mode – specify the wireless network mode, depending on radio [802.11a, 802.11n, 802.11a/n].

Tx power (dBm) – set the unit's transmitting power at which the device will transmit data. The larger the distance, the higher transmit power is required. To set transmit power level use the slider or enter the value manually. When entering the transmit power value manually, the slider position will change according to the entered value. The maximum transmit power level is limited to the allowed value by country in which device is operating regulatory agency.

Channel – displays the channel at which the AP is operating, or indicates that autochannel function is used. Click on the **Channel** button and the channel selection window will be displayed:



CHANNEL

Channel width (MHz): 40 Upper

☑	Channel	TX limit, dBm	EIRP limit, dBm	DFS/ATPC required
☑	1 (2412 MHz)	25	30	No
☑	2 (2417 MHz)	25	30	No
☑	3 (2422 MHz)	25	30	No
☑	4 (2427 MHz)	25	30	No
☑	5 (2432 MHz)	25	30	No
☑	6 (2437 MHz)	25	30	No
☑	7 (2442 MHz)	25	30	No

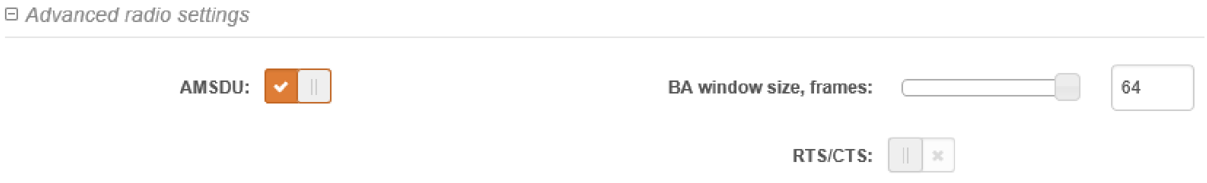
Figure 9 – Channel List Table

Channel width – select the width of the operating radio channel. The LigoWave NFT supports 20, 40 Lower and 40 Upper channel widths.

Channel table – select the channel(s) at which the NFT AP will operate. If more than one channel is selected, then autochannel feature will be enabled. Automatic channel selection allows AP to select a channel which is not used by any other wireless device or, if there are no free channels available - to select a channel which is least occupied. The table displays detailed information about each channel: TX limit, EIRP limit and DFS or ATPC.

Advanced radio settings

Advanced parameters allow configuring the device to get the best performance/capacity of the link:



⊟ *Advanced radio settings*

AMSDU: ✓

BA window size, frames: 64

RTS/CTS: ✗

Figure 10 - Wireless Advanced Settings

AMSDU – enable the AMSDU packet aggregation. If enabled, the maximum size of the 802.11 MAC frames will be increased. Available only on 802.11n or 802.11a/n IEEE modes.

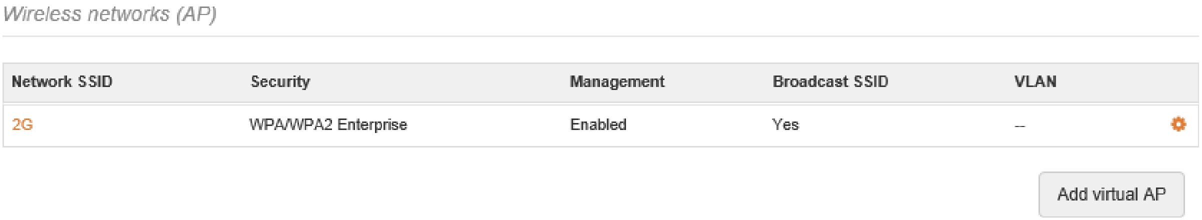
BA window size – specify BA (Block ACK) window size in frames [1-64].

RTS/CTS – specify the RTS threshold using slider or enter the value manually [0-2347 bytes]. The RTS threshold determines the packet size of a transmission and, through the use of an access point, helps control traffic flow.

Wireless networks (VAP) settings

Each LigoWave NFT unit supports up to eight (8) VAPs peer radio.

The **Wireless Networks** table allows to configure the principal wireless radio parameters as well as create another 8 wireless networks (Virtual APs) in addition per radio. All VAPs may be active at the same time meaning that client devices can associate to the access point using any of the VAPs.

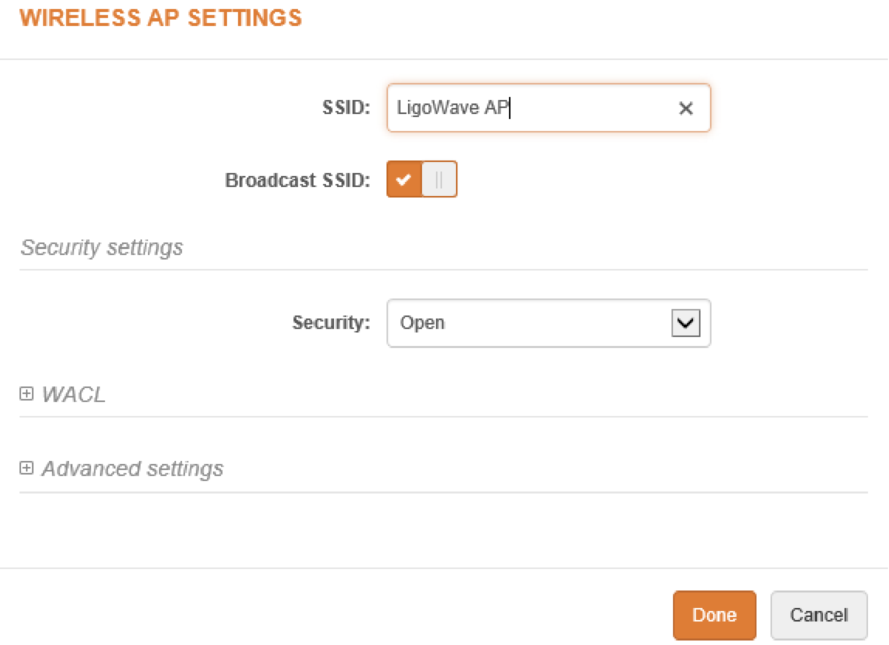


Wireless networks (AP)

Network SSID	Security	Management	Broadcast SSID	VLAN
2G	WPA/WPA2 Enterprise	Enabled	Yes	--

Figure 11 - Wireless Settings

Click on the icon ⚙ for editing, or click on **Add virtual AP** button to create a new VAP:



WIRELESS AP SETTINGS

SSID: LigoWave AP

Broadcast SSID: ✓

Security settings

Security: Open

Figure 12 – Wireless AP Settings

SSID – specify the SSID of the wireless network.

Broadcast SSID – enables or disables the broadcasting of the SSID.

For detailed information about security settings and WACL refer at the respective sections *Wireless security* and *Wireless ACL*.

Wireless security

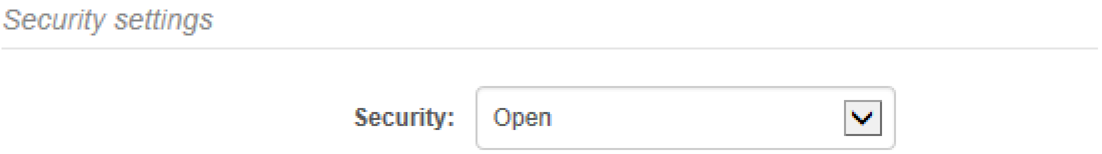
The wireless security settings will be used by the wireless stations for association, thus wireless station security settings must conform the settings configured on the AP that station is associated with.

Each VAP of the LigoWave NFT supports following authentication/encryption methods:

- **Open** – no encryption.
- **Personal WPA/WPA2** – authorizes and identifies clients based on a secret key that changes automatically at regular intervals.
- **Enterprise WPA/WPA2** – RADIUS server based authentication (requires configured RADIUS server).

Open

By default there is no encryption enabled on the LigoWave NFT device:



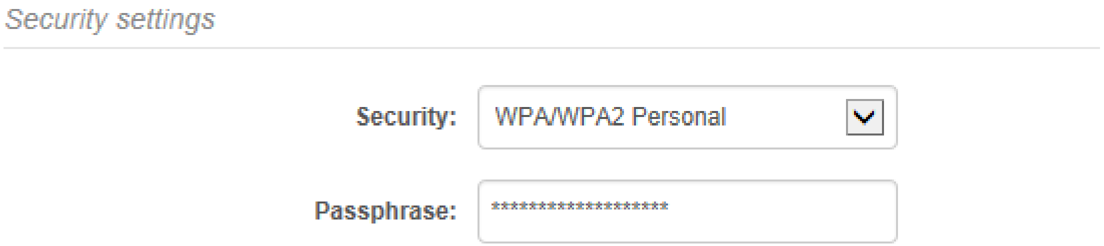
Security settings

Security: Open

Figure 13 – Wireless Security: Open with RADIUS MAC Authentication Enabled

WPA/WPA2 Personal

To setup WPA/WPA2 Personal encryption, need to select appropriate security type and specify the passphrase:



Security settings

Security: WPA/WPA2 Personal

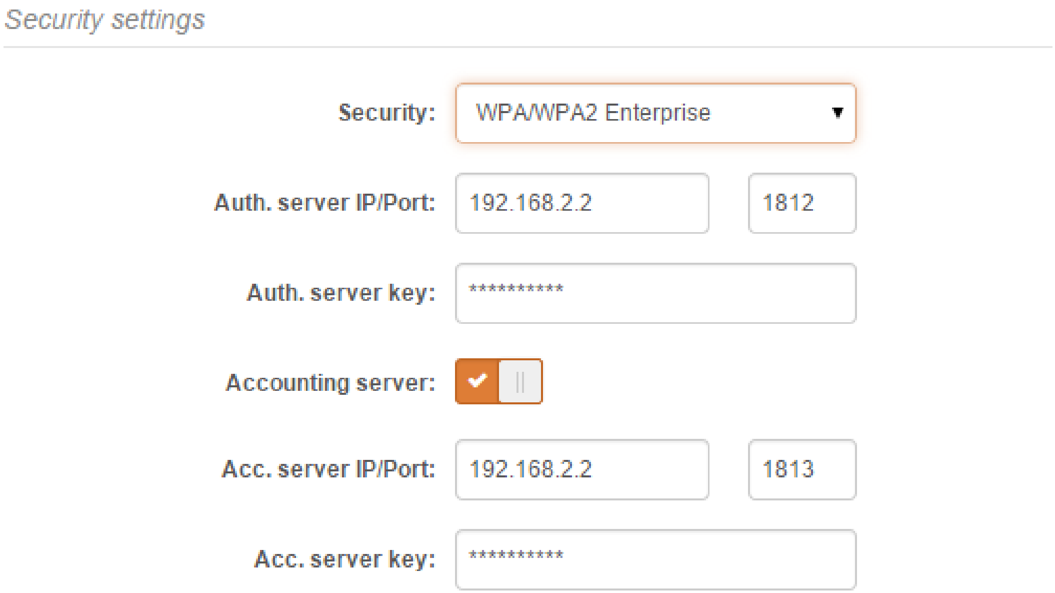
Passphrase: *******************

Figure 14 –Wireless Security: Personal WPA/WPA2 Security

Passphrase – specify WPA or WPA2 passphrase [8-63 characters].

WPA/WPA2 Enterprise for Access Points

LigoWave NFT has possibility to configure WPA/WPA2 Enterprise encryption with RADIUS authentication. Properly configured AP will accept wireless stations requests and will send the information to configured RADIUS server for client authentication.



Security settings

Security: WPA/WPA2 Enterprise

Auth. server IP/Port: 192.168.2.2 1812

Auth. server key: **********

Accounting server: ✓

Acc. server IP/Port: 192.168.2.2 1813

Acc. server key: **********

Figure 15 –Wireless Security: Enterprise WPA/WPA2 Security for AP

The properly configured RADIUS server is required for **WPA/WPA2 Enterprise** encryption.

Auth. server IP/Port – specify the IP address and the port of the authentication RADIUS server where the authentication requests will be send to.

Auth. server key – enter the key for the authentication on specified RADIUS server.

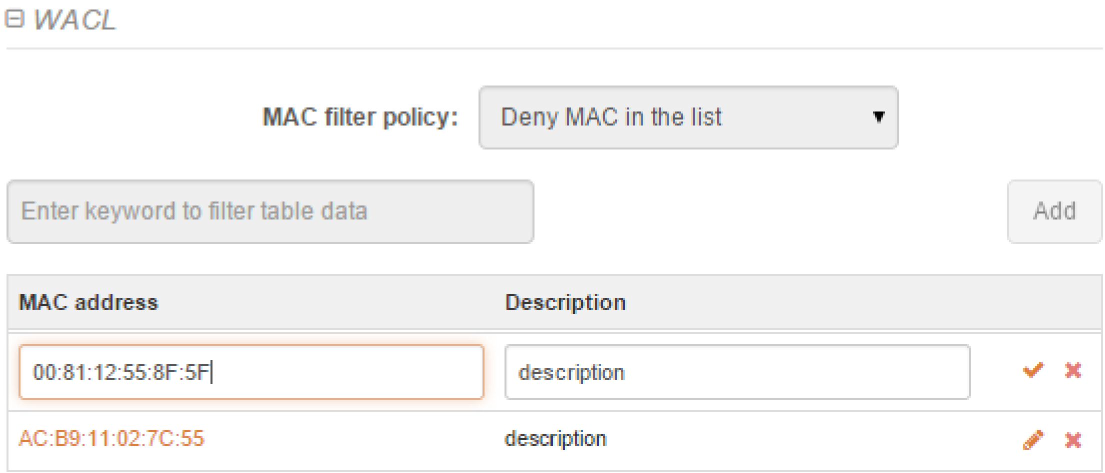
Accounting server – use slide to enable accounting RADIUS server, if required.

Acc. server IP/Port – specify the IP address and the port of the accounting RADIUS server where the accounting stats will be send to.

Acc. server key – enter the key for the authentication on specified accounting RADIUS server.

Wireless ACL

Access Control provides the ability to limit associations wirelessly, based on MAC address, to an AP by creating an Access Control List (ACL) on each wireless interface (including VAPs).



MAC filter policy: Deny MAC in the list

MAC address	Description	
00:81:12:55:8F:5F	description	✓ ✖
AC:B9:11:02:7C:55	description	✎ ✖

Figure 16 – Wireless ACL Configuration

MAC filter policy – define the main VAP policy:

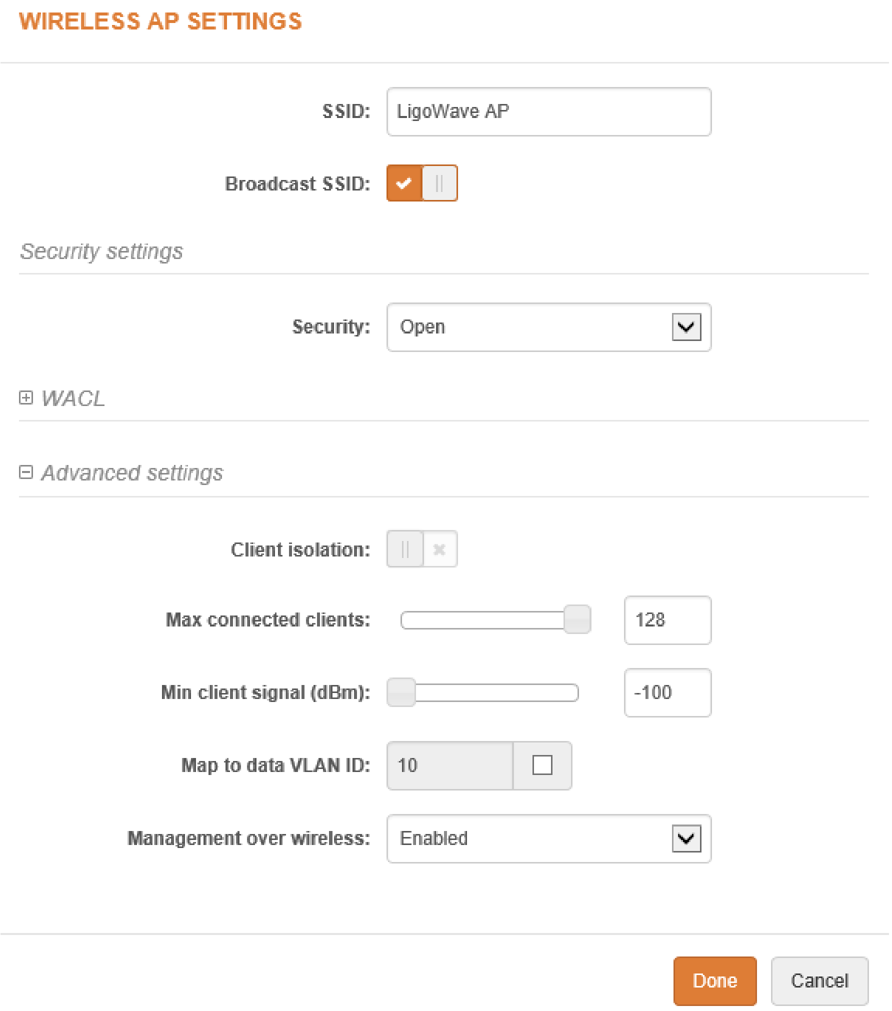
- **Open** – no rules applied.
- **Allow MAC in the list** – only listed MAC clients can connect to the VAP (white list).
- **Deny MAC in the list** – only listed MAC clients can NOT connect to the VAP (black list).

To add new rule, click the **Add** button, specify MAC address and click verification icon ✓.

To remove the rule, click the delete icon ✖ next to required record.

To edit the rule, click the pencil icon ✎ next to required record.

Advanced settings



WIRELESS AP SETTINGS

SSID: LigoWave AP

Broadcast SSID: ✓

Security settings

Security: Open

⊞ WACL

⊟ Advanced settings

Client isolation: ✗

Max connected clients: 128

Min client signal (dBm): -100

Map to data VLAN ID: 10 □

Management over wireless: Enabled

Figure 17 – VAP Advanced Settings

Client isolation – select to enable the layer 2 isolation that blocks clients from communicating with each other. Client isolations is available only in Access Point (auto WDS) and Access Point Repeater mode.

Max connected clients - specify the maximum number of associated wireless clients on the AP radio.

Min client signal (dBm) - if enabled, the AP will drop the connection for clients that have signal level below configured threshold.

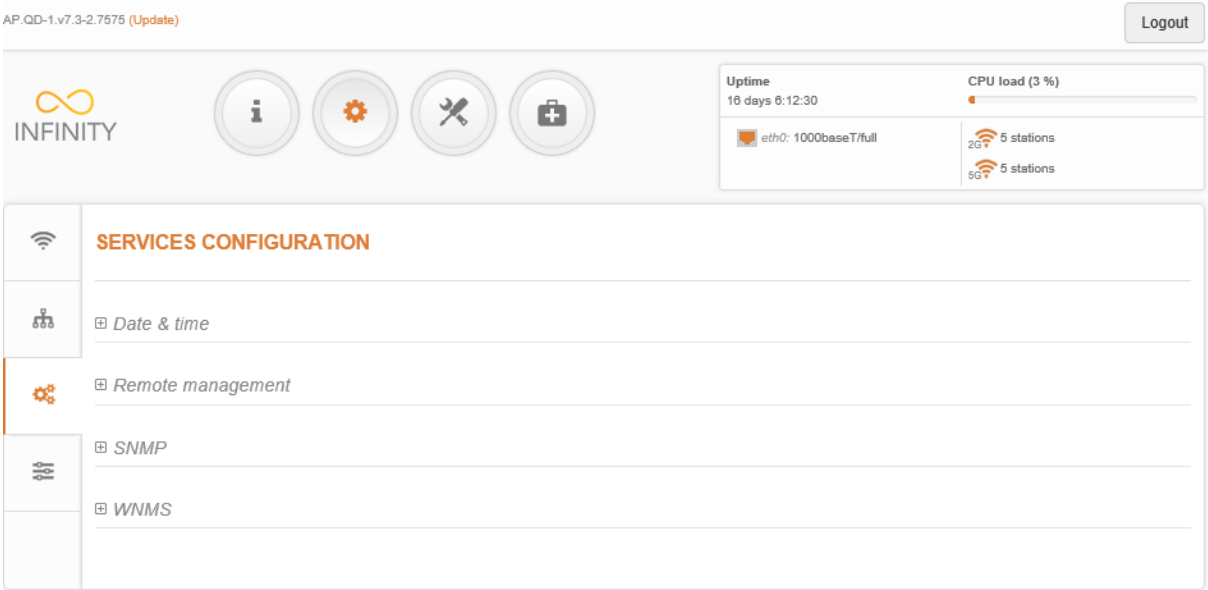
Map to data VLAN ID – specify the VLAN ID for traffic tagging on particular VAP interface. The Station devices that associate using the particular SSID will be grouped into this VLAN.

Management over wireless – controls the wireless administrative access. For security reasons, it is recommended disable wireless access and instead requires a physical network connection using an Ethernet cable for administrative access to LigoWave NFT.

Services configuration

Use **Services** menu is divided into further five sections:

- Date & time
- Remote management
- SNMP
- WNMS



Uptime
16 days 6:12:30

CPU load (3 %)

eth0: 1000baseT/full

2G 5 stations
5G 5 stations

SERVICES CONFIGURATION

⊞ Date & time

⊞ Remote management

⊞ SNMP

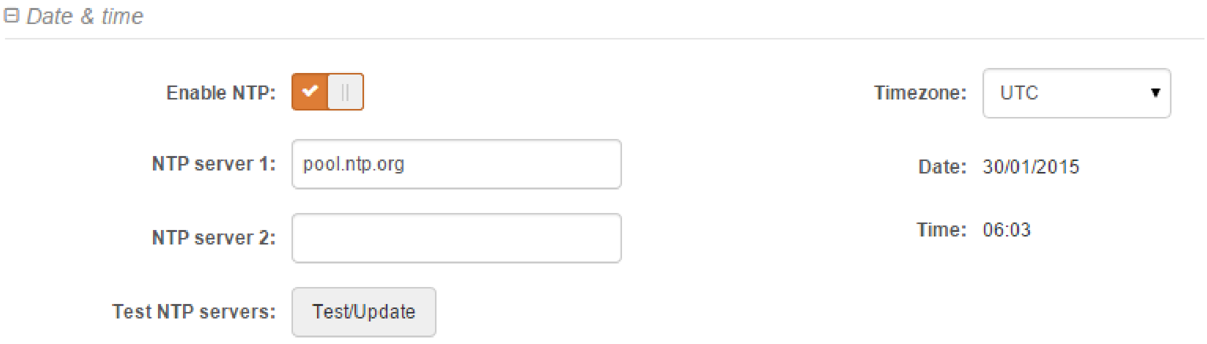
⊞ WNMS

Figure 18 - Services Menu

Date & time

Use this section to manage the system time and date on the device automatically, using the Network Time Protocol (NTP), or manually, by setting the time and date on the device.

The NTP (Network Time Protocol) client synchronizes the clock of the device with the defined time server. Choose NTP from the configuration menu, select your location time zone and enter NTP server in order to use the NTP service.



⊟ Date & time

Enable NTP: ☑

Timezone: UTC

NTP server 1: pool.ntp.org

Date: 30/01/2015

NTP server 2:

Time: 06:03

Test NTP servers: Test/Update

Figure 19 – Date&time: NTP Configuration

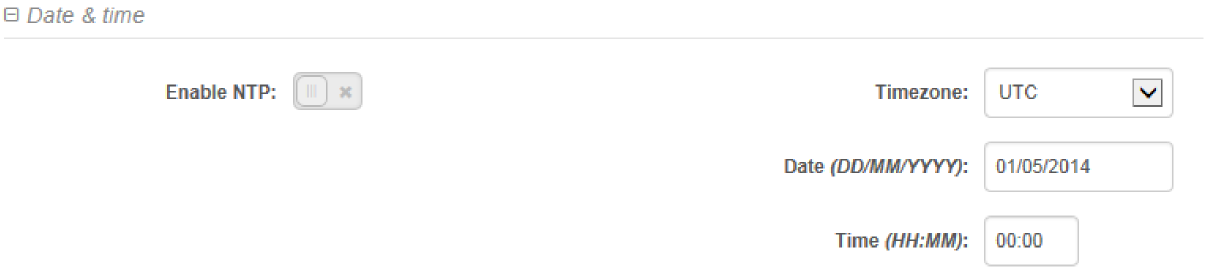
Enable NTP – select this option as enabled to configure NTP.

Timezone – select the timezone. Time zone should be specified as a difference between local time and GMT time.

NTP server – specify the trusted NTP server IP or hostname for time synchronization.

Test NTP servers - click this button to check if the specified servers responses successfully.

To adjust the clock settings manually, disable NTP option and specify the following settings:



⊟ *Date & time*

Enable NTP: ☐

Timezone: UTC

Date *(DD/MM/YYYY)*: 01/05/2014

Time *(HH:MM)*: 00:00

Figure 20 – Date&time: Manual Configuration

Enable NTP – disable this option to set date&time manually.

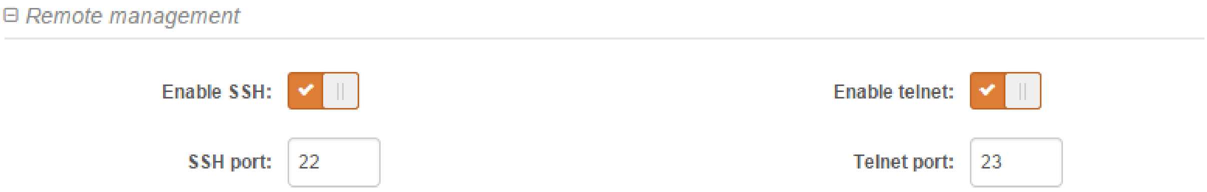
Timezone – select the timezone. Time zone should be specified as a difference between local time and UTC time.

Date – specify the new date value in format DD/MM/YYYY

Time – specify the time in format HH:MM.

Remote management

Use this menu to manage access to the LigoWave NFT via SSH and Telnet:



⊟ *Remote management*

Enable SSH: ✓

Enable telnet: ✓

SSH port: 22

Telnet port: 23

Figure 21 – Remote Management Configuration

Enable SSH – enable or disable SSH access to device.

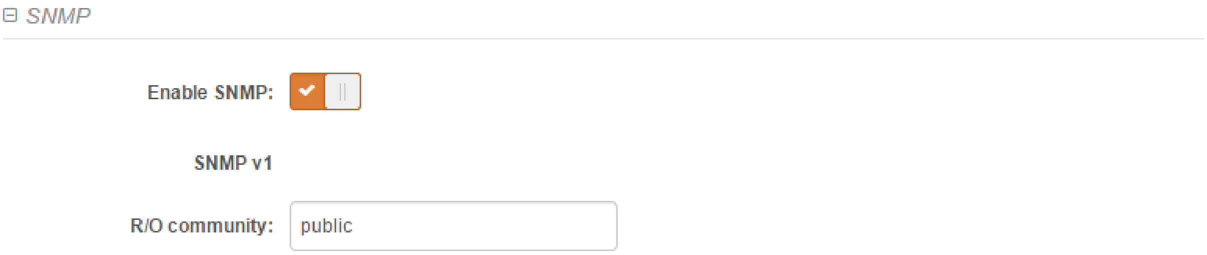
SSH port – specify the SSH service port. By default SSH port is 22.

Enable telnet – enable or disable telnet access to device.

Telnet port – specify the telnet port. By default SSH port is 23.

SNMP

SNMP is the standard protocol that is widely used for remote network management over the Internet. With the SNMP service enabled, the device will act as SNMP agent.



⊟ *SNMP*

Enable SNMP: ✓

SNMP v1

R/O community: public

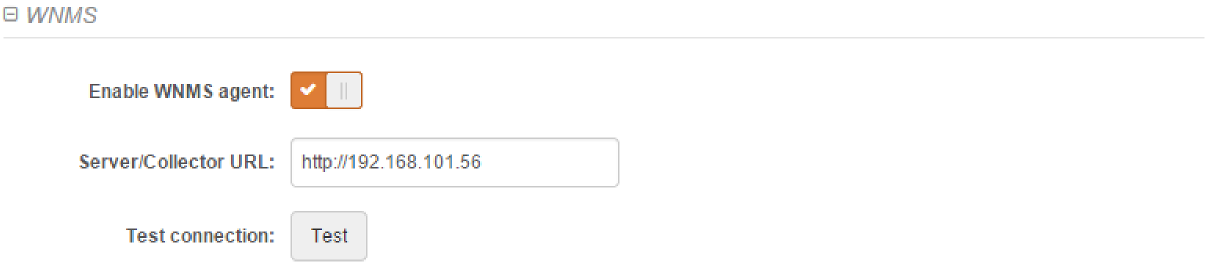
Figure 22 – SNMP Service Settings

Enable SNMP – specify the SNMP service status.

R/O community – specify the read-only community name for SNMP version 1 and version 2c. The read-only community allows LigoWave NFT unit manager to read values, but denies any attempt to change values.

WNMS

Wireless Network Management System (WNMS) is a centralized monitoring and management system for wireless network devices. The communication between managed devices and the WNMS server is always initiated by the WNMS client service running on every device.



⊟ *WNMS*

Enable WNMS agent: ☑

Server/Collector URL: http://192.168.101.56

Test connection: Test

Enable WNMS agent – select to enable WNMS agent.

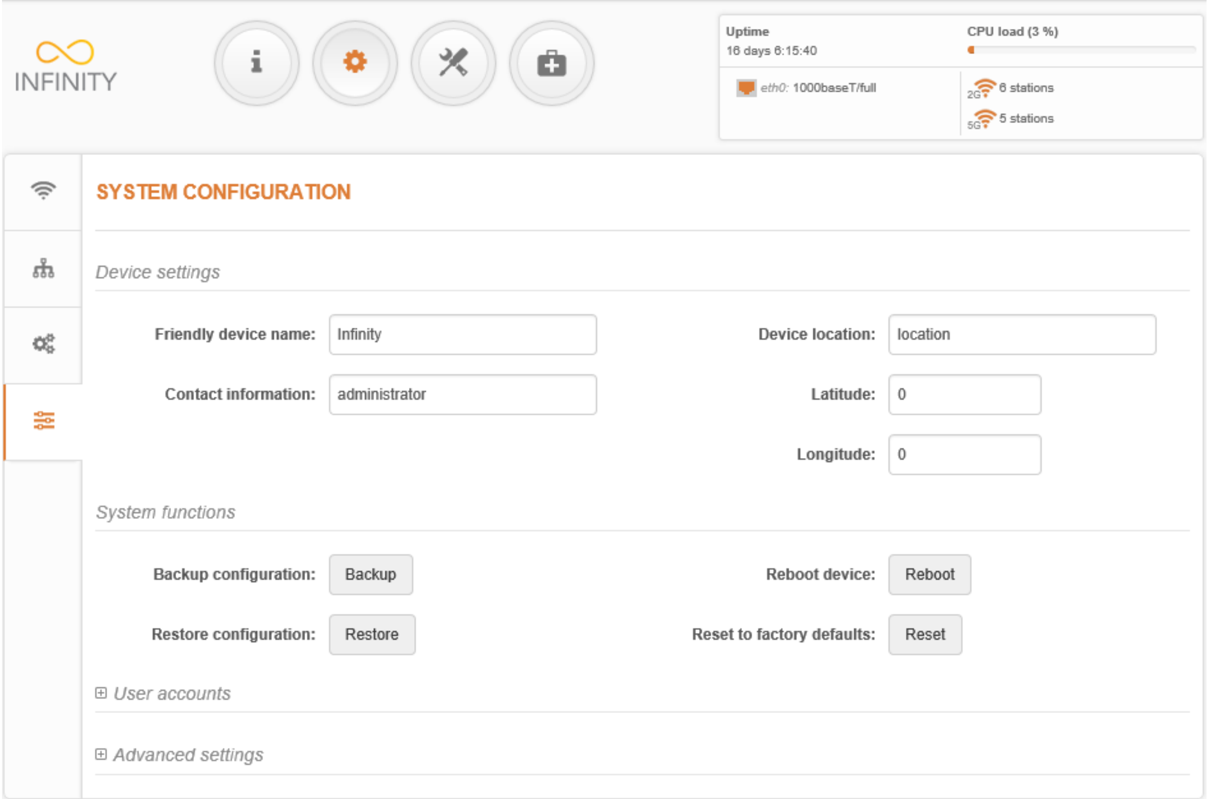
Server/Collector URL – specify the URL of the WMS server to which that heartbeat notifications will be sent to.

Test connection - click this button to check if the specified server responses successfully.

System configuration

System menu allows you to manage main LigoWave NFT settings and perform main system actions (reboot, restore configuration, etc.). The section is divided into further sections:

- Device settings
- System functions
- User accounts
- Advanced settings



SYSTEM CONFIGURATION

Device settings

Friendly device name: Infinity

Device location: location

Contact information: administrator

Latitude: 0

Longitude: 0

System functions

Backup configuration: Backup

Reboot device: Reboot

Restore configuration: Restore

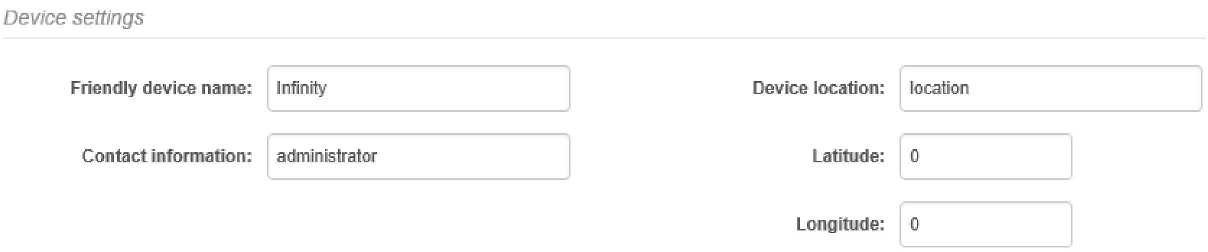
Reset to factory defaults: Reset

⊞ *User accounts*

⊞ *Advanced settings*

Figure 23 - System Menu

Device settings



Device settings

Friendly device name:	Infinity	Device location:	location
Contact information:	administrator	Latitude:	0
		Longitude:	0

Figure 24- Device Settings

Friendly device name – specify name of the LigoWave NFT that will be used to identify the unit.

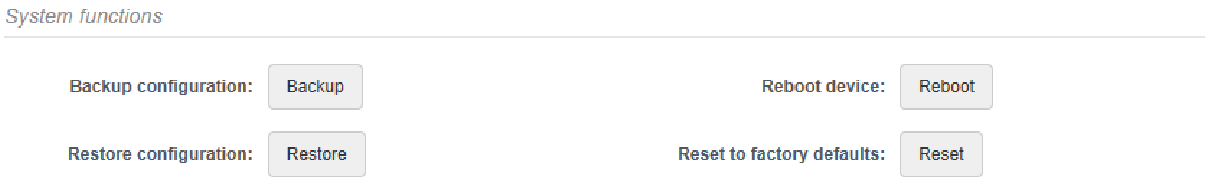
Contact information – specify the name of the contact person, such as a network administrator, for the LigoWave NFT.

Device location – describe the location of the device.

Longitude – specify the longitude coordinates of the device [specific decimal format, e.q. 54.869446].

Latitude – specify the latitude coordinates of the device [specific decimal format, e.q. 23.891058]. Both coordinates helps indicate accurate location of the device.

System functions



System functions

Backup configuration: Backup
Restore configuration: Restore
Reboot device: Reboot
Reset to factory defaults: Reset

Figure 25 - System Functions

Backup configuration – click to save the current 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.

Restore configuration – click to upload an existing configuration file to the device. After the configuration file is uploaded, the new configuration will be effective after the *Save changes* button is pressed.

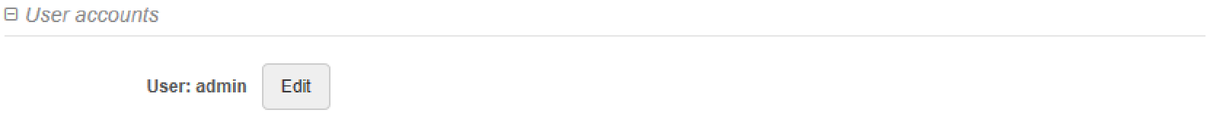
Reboot device – reboot device with the last saved configuration.

Reset device to factory defaults – click to restore unit's factory configuration.

Resetting the device is an irreversible process. Current configuration and the administrator password will be set back to the factory default.

User accounts

For security reasons it is recommended to change the default administrator username and password as soon as possible.



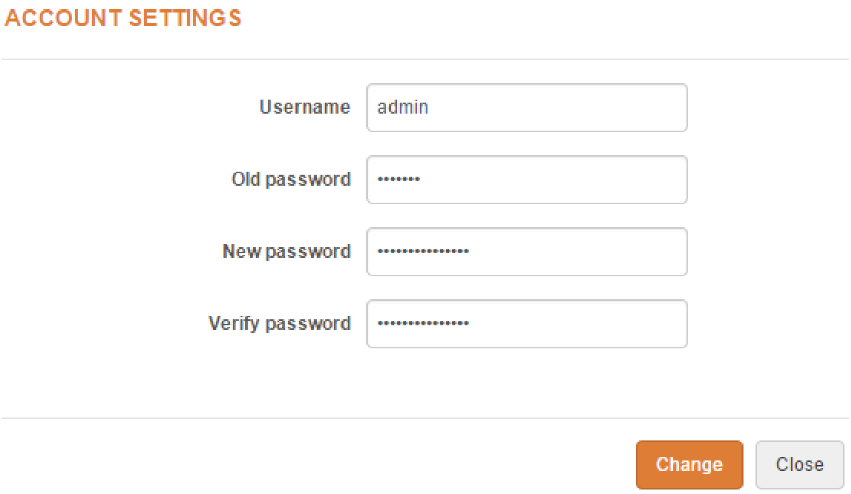
⊟ User accounts

User: admin Edit

Figure 26 – User Accounts

Default administrator logon settings are:
Username: **admin**
Password: **admin01**

Click **Edit** button next to user for changing credentials:



ACCOUNT SETTINGS

Username: admin
Old password: •••••••
New password: •••••••••••••••
Verify password: •••••••••••••••

Figure 27 – User Account Settings

Username – change the administrator's username.

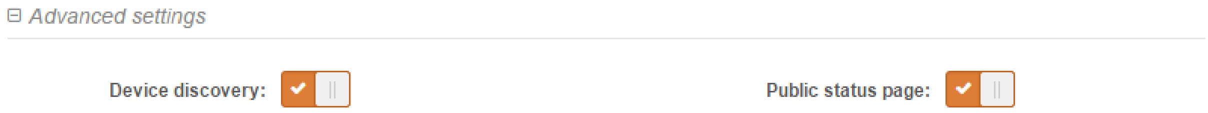
Old password – enter the old administrator password.

New password – enter the new administrator password for user authentication.

Verify password – re-enter the new password to verify its accuracy.

The only way to gain access to the web management if you forget the administrator password is to reset the unit to factory default settings.

Advanced settings



⊟ Advanced settings

Device discovery: ✓

Public status page: ✓

Figure 28 – Device discovery

Device discovery – select to enable LigoWave NFT discovery function. Enable this feature to allow the LigoWave NFT unit discovery within reach of a single multicast packet

Public status page –enable or disable the permission for not logged users to view the Status page.

Firmware upgrade

The current version of the device firmware is shown on the upper left corner of the Web interface.

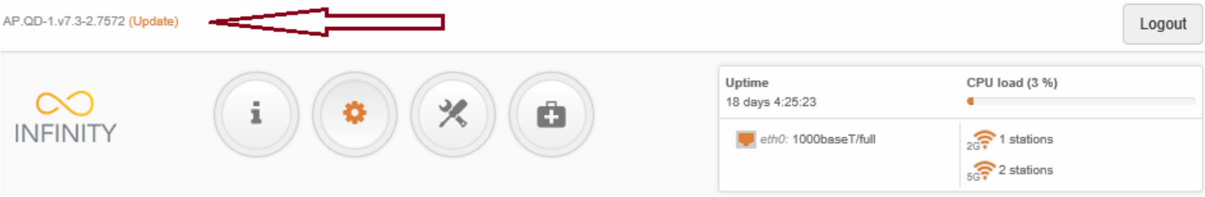
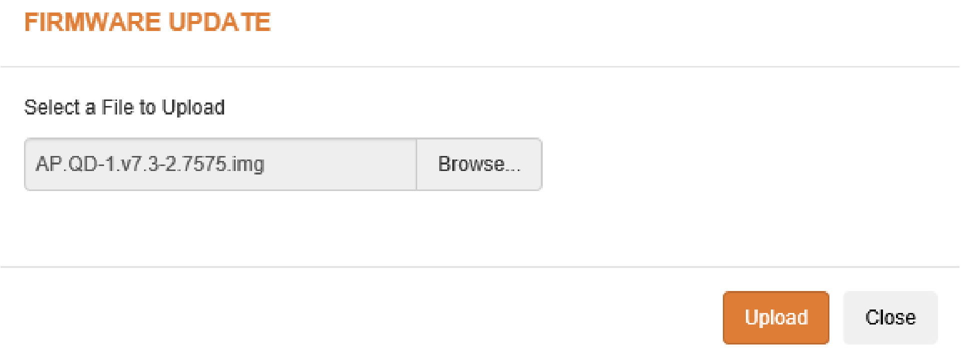


Figure 29 – Firmware Version

The device system firmware upgrade is compatible with all configuration settings. When the device is upgraded with a newer version or the same version builds, all the system's configuration will be preserved after the upgrade.

Click the **(Update)** link near the running firmware name and select the proper firmware image in the Firmware Update pop-up window, then click **Upload** button:

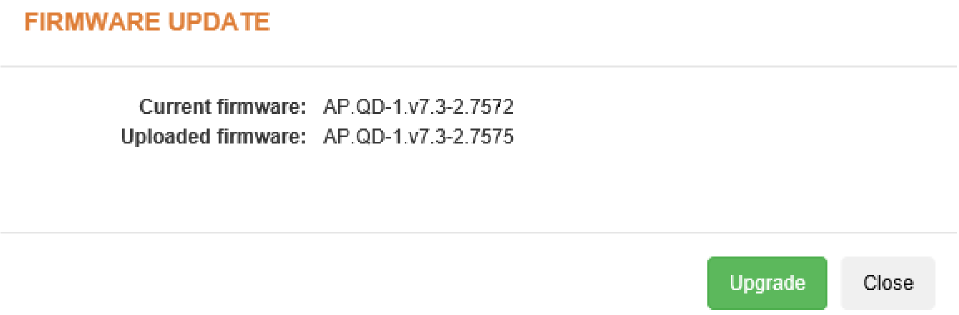

FIRMWARE UPDATE

Select a File to Upload

AP.QD-1.v7.3-2.7575.img

Figure 30 – Firmware Upload

The new firmware image is uploaded to the controller's temporary memory. It is necessary to save the firmware into the device permanent memory. Click the **Upgrade** button:


FIRMWARE UPDATE

Current firmware: AP.QD-1.v7.3-2.7572
Uploaded firmware: AP.QD-1.v7.3-2.7575

Figure 31 –Firmware Upgrade

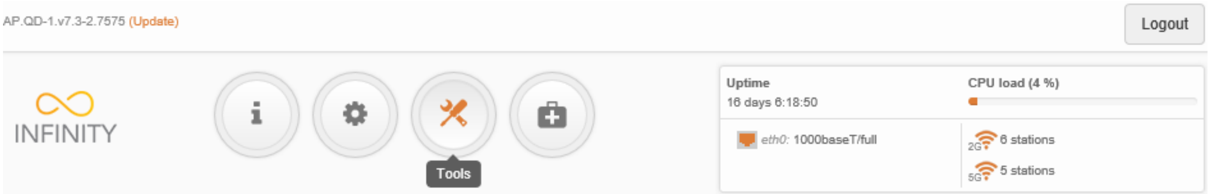
Current version – displays version of the current firmware.

Uploaded version – displays version of the uploaded firmware.

Upgrade – upgrade device with the uploaded image and reboot the system.

Do not switch off and do not disconnect the device from the power supply during the firmware upgrade process as the device could be damaged.

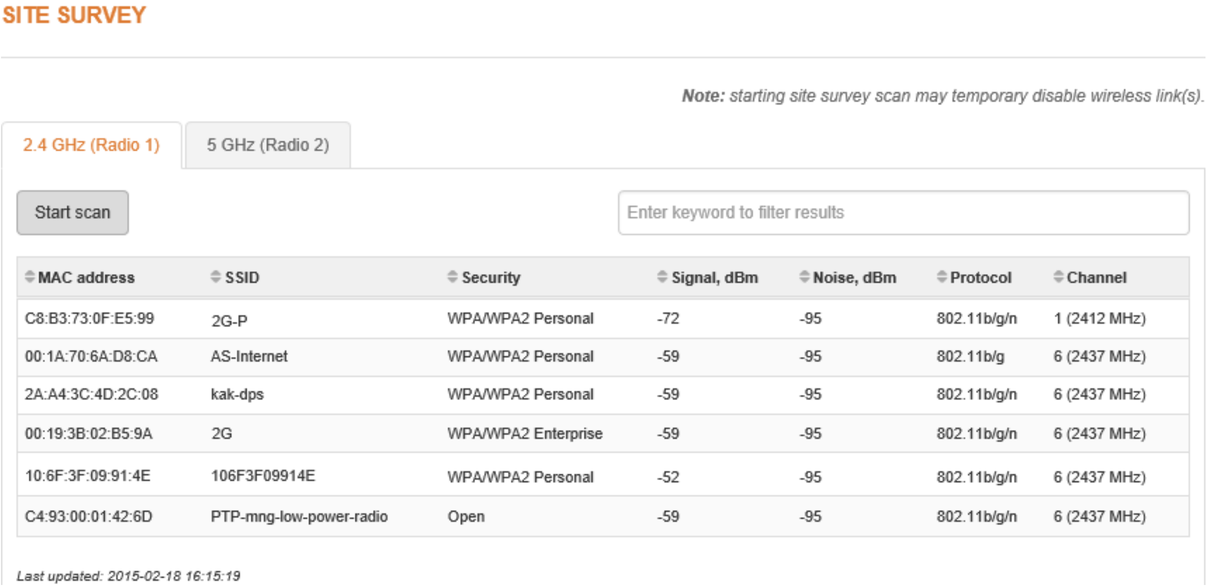
Tools



Site survey

The Site Survey tool shows overview information for wireless networks in a local geographic area on each LigoWave NFT device radio interface. Using this test, an administrator can scan for working wireless devices, check their operating channels, encryption and see signal/noise levels.

To perform the Site Survey test currently, click the **Start scan**:



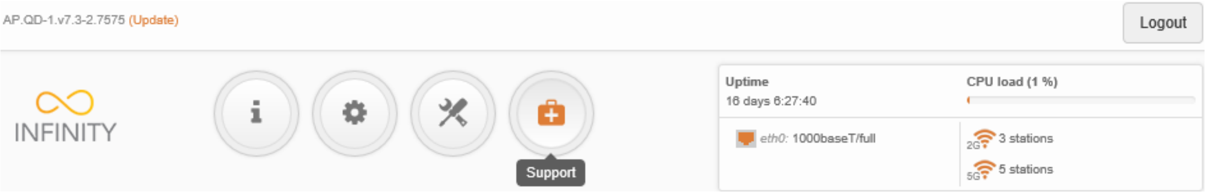
Note: starting site survey scan may temporary disable wireless link(s).

MAC address	SSID	Security	Signal, dBm	Noise, dBm	Protocol	Channel
C8:B3:73:0F:E5:99	2G-P	WPA/WPA2 Personal	-72	-95	802.11b/g/n	1 (2412 MHz)
00:1A:70:6A:D8:CA	AS-Internet	WPA/WPA2 Personal	-59	-95	802.11b/g	6 (2437 MHz)
2A:A4:3C:4D:2C:08	kak-dps	WPA/WPA2 Personal	-59	-95	802.11b/g/n	6 (2437 MHz)
00:19:3B:02:B5:9A	2G	WPA/WPA2 Enterprise	-59	-95	802.11b/g/n	6 (2437 MHz)
10:6F:3F:09:91:4E	106F3F09914E	WPA/WPA2 Personal	-52	-95	802.11b/g/n	6 (2437 MHz)
C4:93:00:01:42:6D	PTP-mng-low-power-radio	Open	-59	-95	802.11b/g/n	6 (2437 MHz)

Last updated: 2015-02-18 16:15:19

Figure 32 – Site Survey Results

Support



Troubleshooting

The troubleshooting file contains valuable information about device configuration, routes, log files, command outputs, etc. When using the troubleshooting file, the device quickly gathers troubleshooting information automatically, rather than requiring you to gather each piece of information manually. This is helpful for submitting problems to the support team.

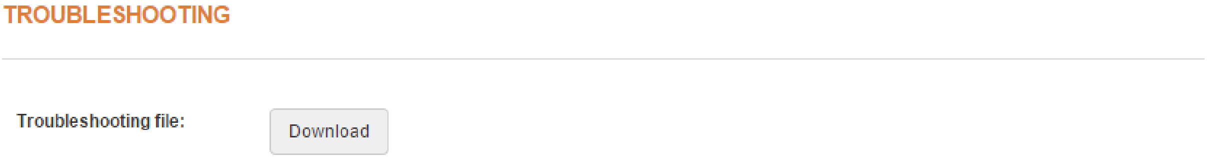
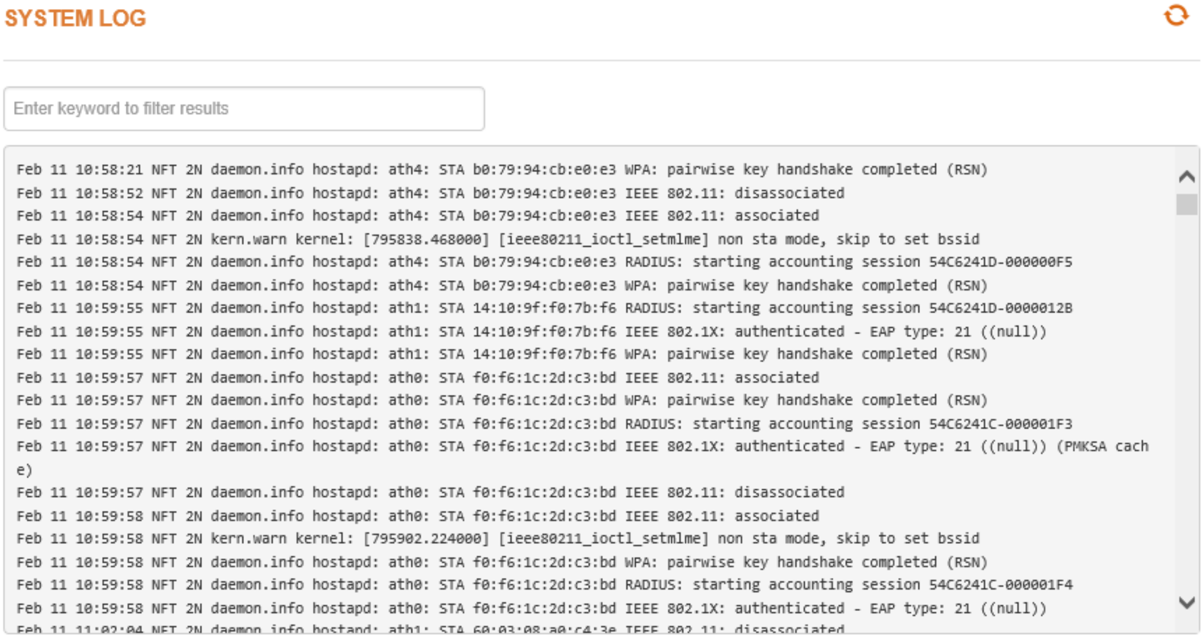


Figure 33 – Troubleshooting File Download

Download– click to download the troubleshooting file. This may take a few minutes to gather information and to complete download.

System log

The system log viewer utility provides debug information about the system services and protocols. If the device's malfunction occurs recorded messages can help operators to locate misconfiguration and system errors.



```
Feb 11 10:58:21 NFT 2N daemon.info hostapd: ath4: STA b0:79:94:cb:e0:e3 WPA: pairwise key handshake completed (RSN)
Feb 11 10:58:52 NFT 2N daemon.info hostapd: ath4: STA b0:79:94:cb:e0:e3 IEEE 802.11: disassociated
Feb 11 10:58:54 NFT 2N daemon.info hostapd: ath4: STA b0:79:94:cb:e0:e3 IEEE 802.11: associated
Feb 11 10:58:54 NFT 2N kern.warn kernel: [795838.468000] [ieee80211_ioctl_setmlme] non sta mode, skip to set bssid
Feb 11 10:58:54 NFT 2N daemon.info hostapd: ath4: STA b0:79:94:cb:e0:e3 RADIUS: starting accounting session 54C6241D-000000F5
Feb 11 10:58:54 NFT 2N daemon.info hostapd: ath4: STA b0:79:94:cb:e0:e3 WPA: pairwise key handshake completed (RSN)
Feb 11 10:59:55 NFT 2N daemon.info hostapd: ath1: STA 14:10:9f:f0:7b:f6 RADIUS: starting accounting session 54C6241D-0000012B
Feb 11 10:59:55 NFT 2N daemon.info hostapd: ath1: STA 14:10:9f:f0:7b:f6 IEEE 802.1X: authenticated - EAP type: 21 ((null))
Feb 11 10:59:55 NFT 2N daemon.info hostapd: ath1: STA 14:10:9f:f0:7b:f6 WPA: pairwise key handshake completed (RSN)
Feb 11 10:59:57 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd IEEE 802.11: associated
Feb 11 10:59:57 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd WPA: pairwise key handshake completed (RSN)
Feb 11 10:59:57 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd RADIUS: starting accounting session 54C6241C-000001F3
Feb 11 10:59:57 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd IEEE 802.1X: authenticated - EAP type: 21 ((null)) (PMKSA cach
e)
Feb 11 10:59:57 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd IEEE 802.11: disassociated
Feb 11 10:59:58 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd IEEE 802.11: associated
Feb 11 10:59:58 NFT 2N kern.warn kernel: [795902.224000] [ieee80211_ioctl_setmlme] non sta mode, skip to set bssid
Feb 11 10:59:58 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd WPA: pairwise key handshake completed (RSN)
Feb 11 10:59:58 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd RADIUS: starting accounting session 54C6241C-000001F4
Feb 11 10:59:58 NFT 2N daemon.info hostapd: ath0: STA f0:f6:1c:2d:c3:bd IEEE 802.1X: authenticated - EAP type: 21 ((null))
Feb 11 11:02:04 NFT 2N daemon.info hostapd: ath1: STA 60:03:08:a0:c4:3e IEEE 802.11: disassociated
```

Figure 34 – Device System Log

Click the refresh icon, on the upper right corner, to view current system messages.

Index