NFT 1Ni manual

User’s Guide

Revision 1.0

Copyright

Notice

Deliberant 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. Deliberant 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 Deliberant.

FCC Statement

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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

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 modular complies with FCC 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 modular must be installed and operated with a minimum distance of 50 cm between the radiator and user body.

If the FCC identification number is not visible when the module is installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module. This exterior label can use wording such as the following: “Contains Transmitter Module FCC ID: V2V-NFT1NI Or Contains FCC ID: 7607A-NFT1NI”

When the module is installed inside another device, the user manual of this device must contain below warning statements;
1. 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.
(2) This device must accept any interference received, including interference that may cause undesired operation.
2. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

The devices must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product

Important note:

This module is intended for OEM integrator. The OEM integrator is responsible for the compliance to all the rules that apply to the product into which this certified RF module is integrated. Additional testing and certification may be necessary when multiple modules are used. 50 cm minimum distance has to be maintained between the antenna and the users for the host this module is integrated into. Under such configuration, the FCC radiation exposure limits set forth for a population/uncontrolled environment can be satisfied.

Any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate this equipment.

IC Statement

This device complies with Industry Canada’s licence-exempt RSSs. 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.

Cetappareilestconforme aux CNR exemptes de licenced'IndustrieCanada . Son fonctionnementestsoumis aux deux conditions suivantes :
(1) Cedispositif ne peut causer d'interférences ; et
(2) Cedispositifdoit accepter touteinterférence , y compris les interférences qui peuvent causer un mauvaisfonctionnement de l'appareil.

IC Radiation Exposure Statement:

This modular complies with IC 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 modular must be installed and operated with a minimum distance of 50 cm between the radiator and user body.

Cettemodulairedoitêtreinstalléetutilisé à une distance minimum de 50 cm entre le radiateur et le corps de l'utilisateur.

If the IC number is not visible when the module is installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module. This exterior label can use wording such as the following: “Contains IC: 7607A-NFT1NI”

When the module is installed inside another device, the user manual of this device must contain below warning statements;
1. This device complies with Industry Canada’s licence-exempt RSSs. 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.

Cetappareilestconforme aux CNR exemptes de licenced'IndustrieCanada . Son fonctionnementestsoumis aux deux conditions suivantes :
(1) Cedispositif ne peut causer d'interférences ; et
(2) Cedispositifdoit accepter touteinterférence , y compris les interférences qui peuvent causer un mauvaisfonctionnement de l'appareil.

The devices must be installed and used in strict accordance with the manufacturer's instructions as described in the user documentation that comes with the product

Important Radiation Exposure Statement:
This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 50cm between the radiator & your body.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 50 cm de distance entre la source de rayonnement et votre corps.

This module is intended for OEM integrator. The OEM integrator is still responsible for the IC compliance requirement of the end product, which integrates this module.

Trademarks

Deliberant logo is trademark of Deliberant LLC.

All other registered and unregistered trademarks in this document are the sole property of their respective owners.

Contents

About this Guide

Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts and wireless Internet access infrastructures.

Conventions Used in this Document

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

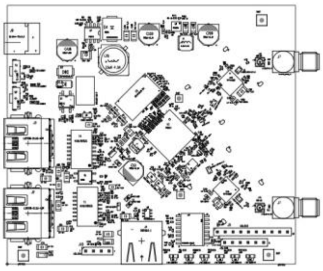
Abbreviation	Description
ACL	Access Control List
AES	Advanced Encryption Standard
AMSDU	Aggregated Mac Service Data Unit
AP	Access Point
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Control Protocol
EAP	Extensible Authentication Protocol
GHz	Gigahertz
GMT	Greenwich Mean Time.
GUI	Graphical User Interface

Abbreviation	Description
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
ISP	Internet Service Provider
IP	Internet Protocol
LAN	Local Area Network
LED	Light-Emitting Diode
MAC	Media Access Control
Mbps	Megabits per second
MHz	Megahertz
MIMO	Multiple Input, Multiple Output
MSCHAPv2	Microsoft version of the Challenge-handshake authentication protocol, CHAP.
NAT	Network address translation – translation of IP addresses (and ports)
PC	Personal Computer
PDA	Personal Digital Assistant
PTP	Point To Point
PSK	Pre-Shared Key
QoS	Quality of Service
PEAP	Protected Extensible Authentication Protocol
RSSI	Received Signal Strength Indication – received signal strength in mV, measured on BNC outdoor unit connector
RX	Receive
SISO	Simple Input, Simple Output
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
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
UAM	Universal Access Method
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
WISPr	Wireless Internet Service Provider roaming
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

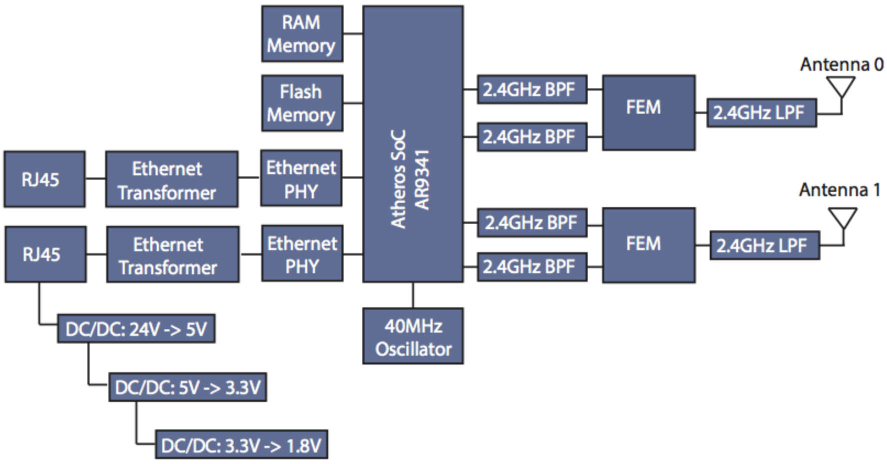
NFT 1Ni specification

The NFT 1Ni is a versatile, very efficient, and stable 2.4 GHz hardware platform. Platform is equipped with high output power 802.11n MIMO radio.

The robust hardware is coupled with an advanced and feature-rich operating system optimized for high performance communications which allows compatibility with older 802.11b/g standard while adding support for the latest wireless communications.



Block diagram



Note 1: Antenna 0 and Antenna 1 frequency range is 2412MHz - 2462MHz (CH1 to CH13).

Note 2: FEM - Front End Module. FEM includes RF PA, RF Switch and RF LNA.

Note 3: BPF – Band Pass Filter.

Note 4: LPF – Low Pass Filter.

Note 5: AR9341 contains contains internal Voltage Regulator making +1.2V from 3.3V.

Hardware information

Feature	Description	Notes
CPU	AR9341	
RAM	64MB	
Flash memory	16MB	
Watchdog timer	Built into CPU	
Reset push button	Connected to GPIO	
LED's	6 LED's connected to GPIO	Power, LAN, 4x received signal strength
Ethernet	2x 10/100 Ethernet port	
Power options	Power-Over-Ethernet or DC Jack	PoE polarity independent via Eth pins 4/5 and7/8.
Power supply	24V	
Serial port (UART)	Test points	3.3V TTL level, not end user accessible
Operating temperature range	From 0C to +65C	
Humidity	0 ~ 90 % (non-condensing)	
Power consumption	up to 4.6W	

Wireless information

Parameter	Description
WLAN standard	IEEE 802.11 b/g/n
Radio mode	MIMO 2x2
Radio frequency band	2.412 GHz to 2.462 GHz
Channel size	20, 40MHz
Modulation schemes	802.11 g/n: OFDM (64-QAM, 16-QAM, QPSK, BPSK) 802.11 b: DSS (CCK, DQPSK, DBPSK)
Data rates	802.11 n: 300, 270, 240, 180, 120, 90, 60, 30 Mbps 802.11 g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps 802.11 b: 11, 5.5, 2, 1 Mbps

Software

Features	
General	Ability to define/limit frequency, channel width, EIRP, modulation
Advanced wireless functionality	Auto-channel, auto-modulation
Operating mode	Router, Bridge
Wireless operating modes	AP auto WDS, Station, Station WDS, Virtual radios (VSSID), iPoll access point, iPoll client
Wireless security	WPA/WPA2 Personal, WPA/WPA2 Enterprise
Wireless QoS	WMM
WAN protocols	Static IP, DHCP client, PPPoE client
Network	NAT
Services	DHCP server, SNMP server, Wireless and Ethernet statistics
Management	HTTP GUI, SSH CLI, SNMP read, WNMS, troubleshooting file, reset via reset tool
Tools	Site survey, Antenna alignment

Power consumption

State	Current	Voltage	Power consumption
Idle	103 mA	24 V	2.47 W
Max load	192 mA	24 V	4.61 W

First Connection

The default product address is `192.168.2.66`.

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

Follow the steps for first connection to the device:

Step 1. Connect an Ethernet cable between your computer and the AP.

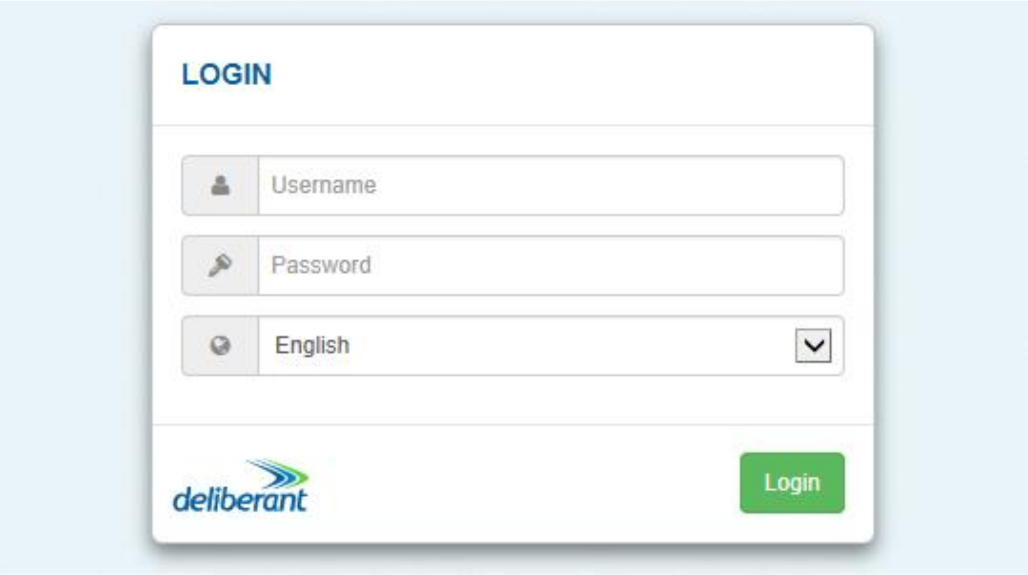
Step 2. Make sure your computer is set to the same subnet as the AP, i.e. 192.168.2.150

Step 3. Start your Web browser.

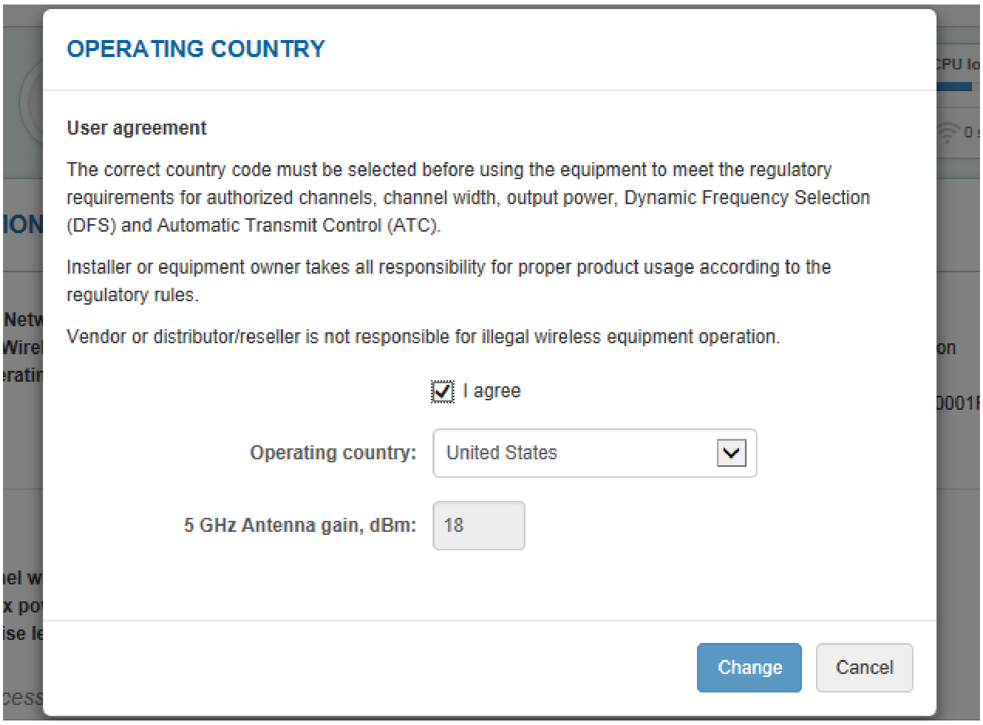
Step 4. Each devices uses following default settings:

- WAN IP: **192.168.2.66**
- Subnet mask: **255.255.255.0**
- Username: **admin**
- Password: **admin01**

The initial login screen looks as follow:



Step 5. **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

5 GHz Antenna gain, dBm: 18

Step 6. After successful administrator login you will see the main page of the device Web management interface. The device now is ready for configuration.

Configuration Guide

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 are three general buttons located on the right top corner of the WEB GUI allowing managing device configuration:

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

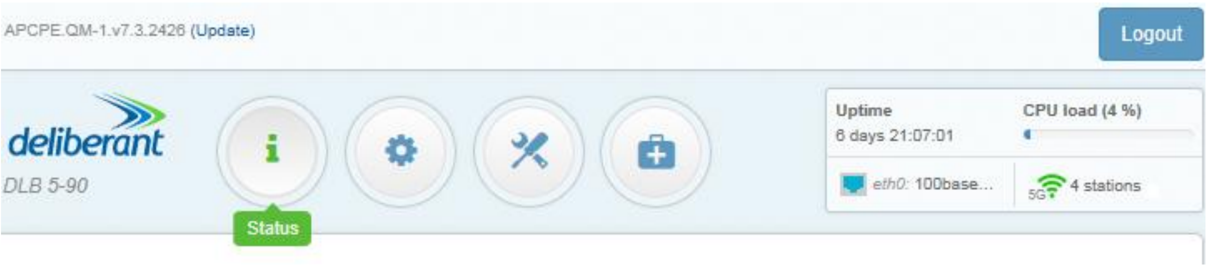
Test changes – if pressed the device will start operating with newly set configuration settings for 3 minutes. During this test time the administrator is able to gauge if device is working properly, and then Save changes. In case wrong settings were chosen (or even after faulty settings administrator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



APCPE.QM-1.v7.3.2426 (Update)

DLB 5-90

Uptime
6 days 21:07:01

CPU load (4 %)

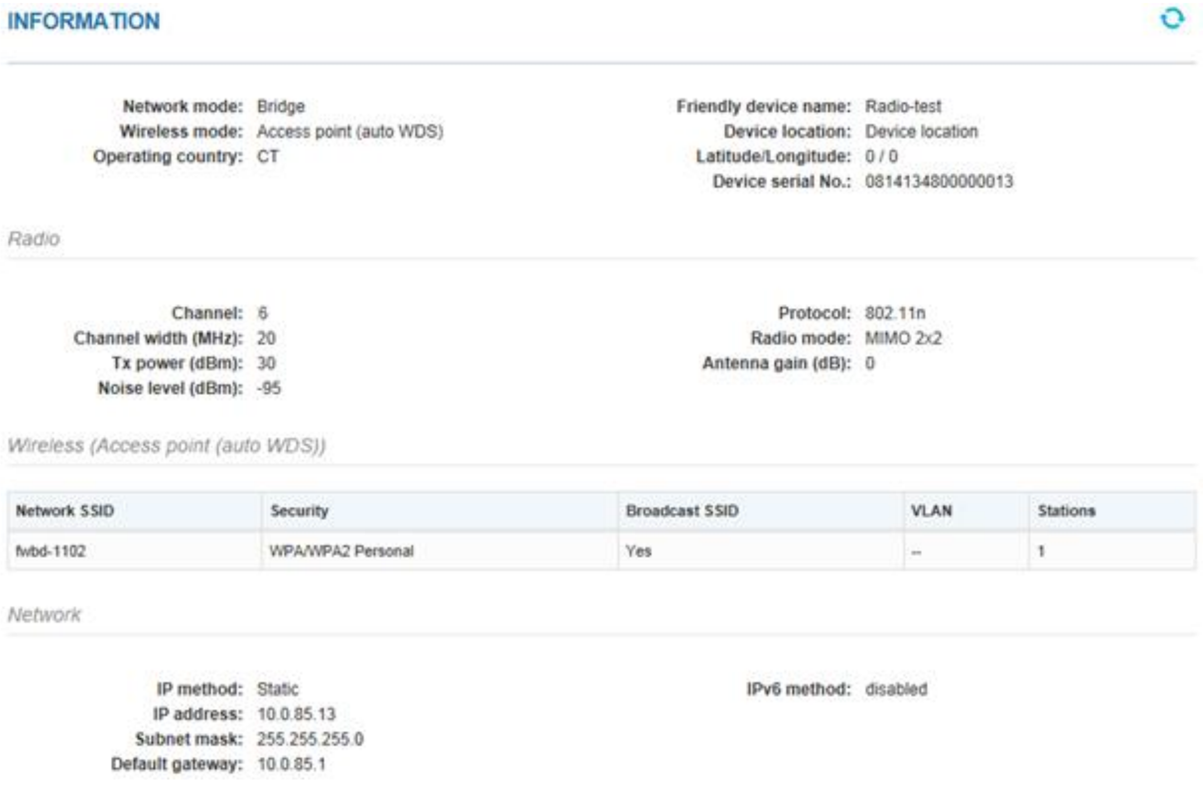
eth0: 100base...

5G 4 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 APC operating mode, radio and network settings.



INFORMATION

Network mode: Bridge
Wireless mode: Access point (auto WDS)
Operating country: CT

Friendly device name: Radio-test
Device location: Device location
Latitude/Longitude: 0 / 0
Device serial No.: 0814134800000013

Radio

Channel: 6
Channel width (MHz): 20
Tx power (dBm): 30
Noise level (dBm): -95

Protocol: 802.11n
Radio mode: MIMO 2x2
Antenna gain (dB): 0

Wireless (Access point (auto WDS))

Network SSID	Security	Broadcast SSID	VLAN	Stations
fwbd-1102	WPA/WPA2 Personal	Yes	--	1

Network

IP method: Static
IP address: 10.0.85.13
Subnet mask: 255.255.255.0
Default gateway: 10.0.85.1

IPv6 method: disabled

Figure 2 – Device Information Page

Radio – displays summary of the radio interface configuration.

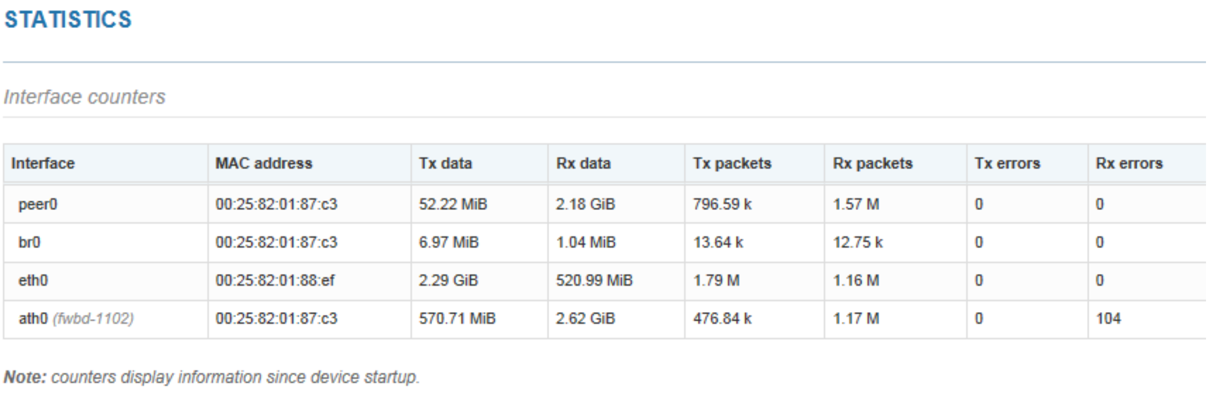
Wireless – displays general information about the wireless connection. The wireless information will differ on Access Point, Station, iPoll wireless modes:

- **Access point (autoWDS)** and **(Access Point (iPoll 2)** – displays access point operating information: SSID, Security type, SSID Broadcast status, VLAN and number of connected clients.
- **Station (WDS/iPoll)** and **Station (ARPNAT)** – displays settings at which the station is connected to the access point: SSID, Security type, Peer's MAC address, Tx/Rx rate, Protocol.

Network mode – displays short summary about current network configuration (bridge or router).

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
peer0	00:25:82:01:87:c3	52.22 MiB	2.18 GiB	796.59 k	1.57 M	0	0
br0	00:25:82:01:87:c3	6.97 MiB	1.04 MiB	13.64 k	12.75 k	0	0
eth0	00:25:82:01:88:ef	2.29 GiB	520.99 MiB	1.79 M	1.16 M	0	0
ath0 *(fwbd-1102)*	00:25:82:01:87:c3	570.71 MiB	2.62 GiB	476.84 k	1.17 M	0	104

Note: *counters display information since device startup.*

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.

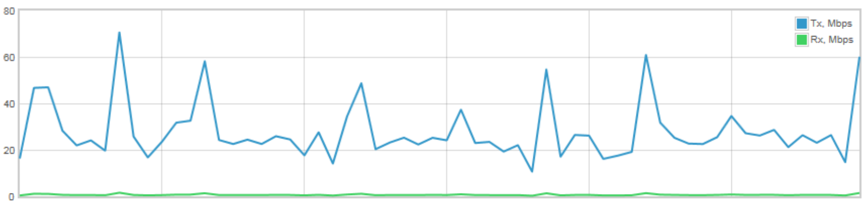
Rx packets – displays the number of received packets.

Tx errors – displays the number of the TX errors.

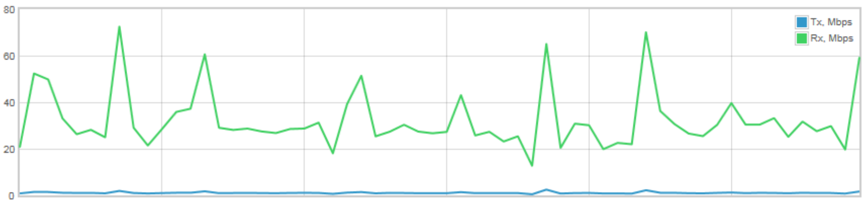
Rx errors – displays the number of the RX errors.

The wired and wireless interface graphs display real-time data traffic. If particular device is working as Station, the additional graph of the signal and noise levels will be displayed:

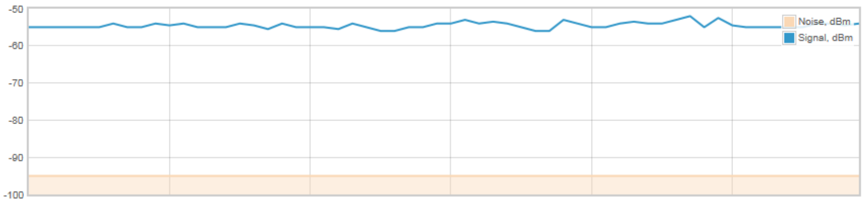
Wired (eth0) traffic (last 5 min.)



Wireless (ath0) traffic (last 5 min.)



Signal and noise level (last 5 min.)

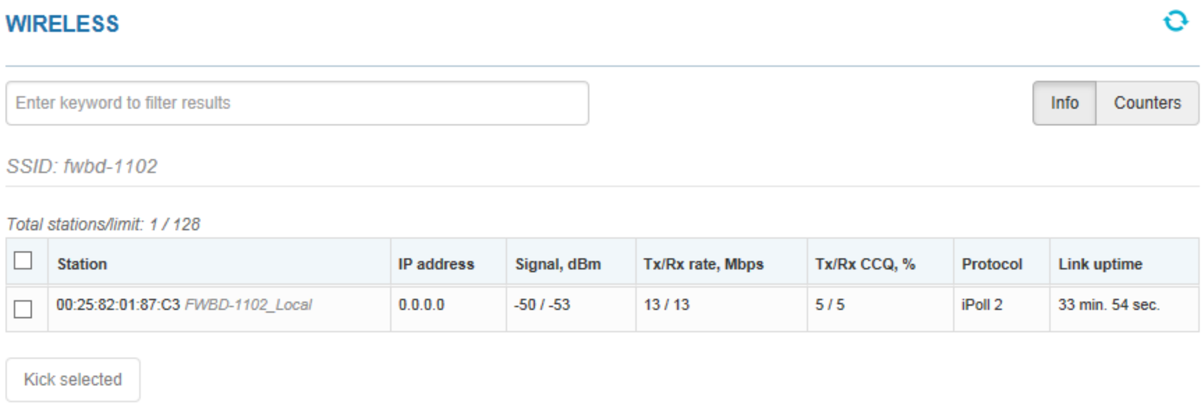


Wireless

Status Wireless section is not available if APC is operating as Station (WDS/iPoll) or Station (ARPNAT). In this case all necessary information about wireless connection with AP unit will be on

Information page, wireless table.

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 counters):



SSID: fwbd-1102

Total stations/limit: 1 / 128

□	Station	IP address	Signal, dBm	Tx/Rx rate, Mbps	Tx/Rx CCQ, %	Protocol	Link uptime
□	00:25:82:01:87:C3 *FWBD-1102_Local*	0.0.0.0	-50 / -53	13 / 13	5 / 5	iPoll 2	33 min. 54 sec.

Figure 4 – Access Point's Wireless Statistics

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.

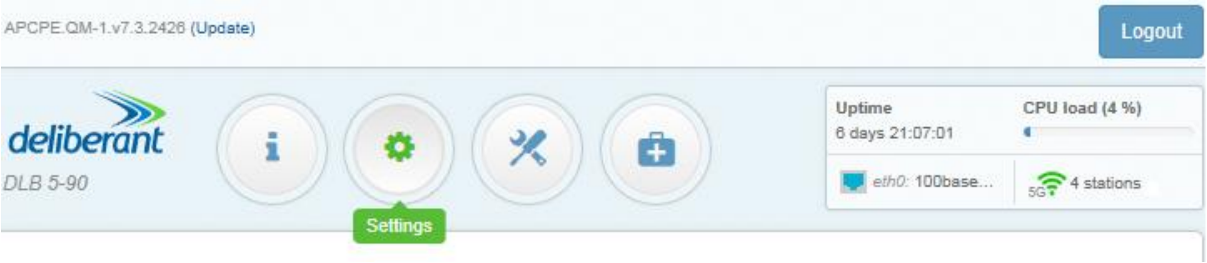
Tx/Rx CCQ, % - displays the wireless Client Connection Quality (CCQ), the value in percent that shows how effective the bandwidth is used regarding the theoretically maximum available bandwidth.

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

Link uptime – displays the duration of the particular session.

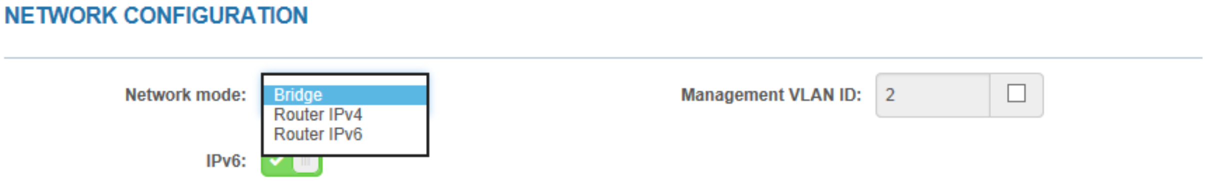
Kick selected – select to end the connection to this station.

Settings



Network Configuration

The **Settings | Network Configuration** page allows you to control the network configuration of the device. First, the device operation mode must be defined to work as a bridge or router (IPv4 or IPv6). The content of the window varies depending on your selection:


NETWORK CONFIGURATION

Network mode: Bridge
Router IPv4
Router IPv6

IPv6: ✓

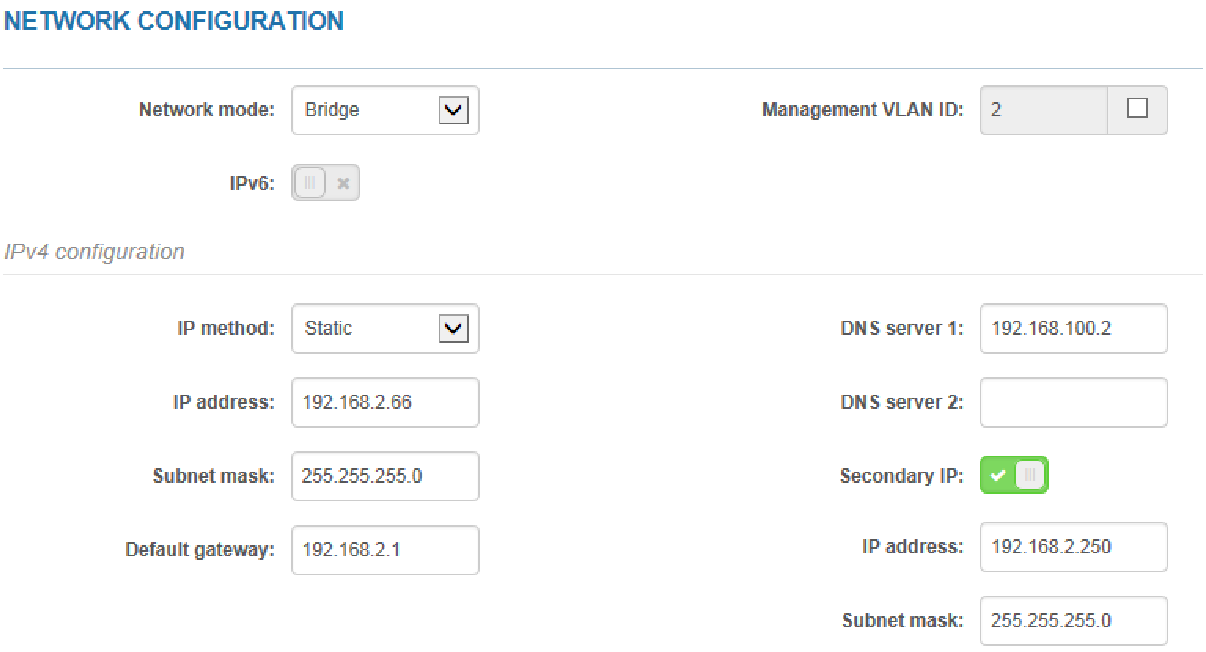
Management VLAN ID: 2 □

Figure 5 – Network Mode Options

Network mode – choose the device operating mode. Network settings will vary according to the selected Network mode. The Bridge mode allows configuring device IPv4 and IPv6 LAN IP settings, while the Router mode requires more parameters such as LAN network settings, WAN network settings, LAN DHCP settings.

Bridge Mode

When device is configured to operate in Bridge mode, only device LAN settings should be configured on the **Network configuration** page:



NETWORK CONFIGURATION

Network mode: Bridge

Management VLAN ID: 2 □

IPv6: ○ ×

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

Figure 6 – Bridge Mode Settings

Enable management VLAN – 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.

IPv4 Configuration

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.

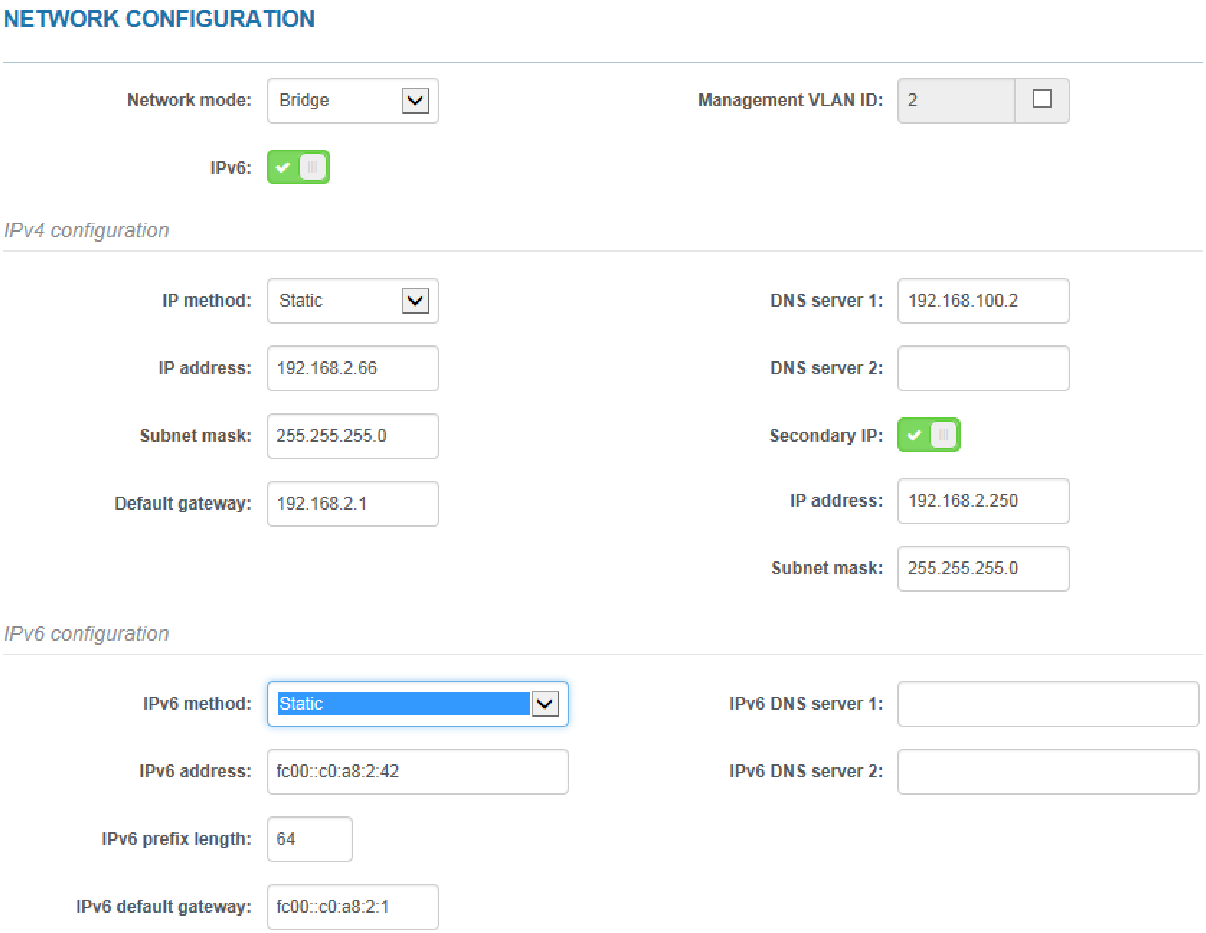
Default gateway – specify a gateway IP address for device.

DNS server – specify the Domain Naming Server.

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

IPv6 Configuration

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



NETWORK CONFIGURATION

Network mode: Bridge

Management VLAN ID: 2 □

IPv6: ✓

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 – Bridge IPv6 Settings

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

- **Static** – the IPv6 address must be specified 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.).

IPv6 address – specify the IPv6 Address for the interface.

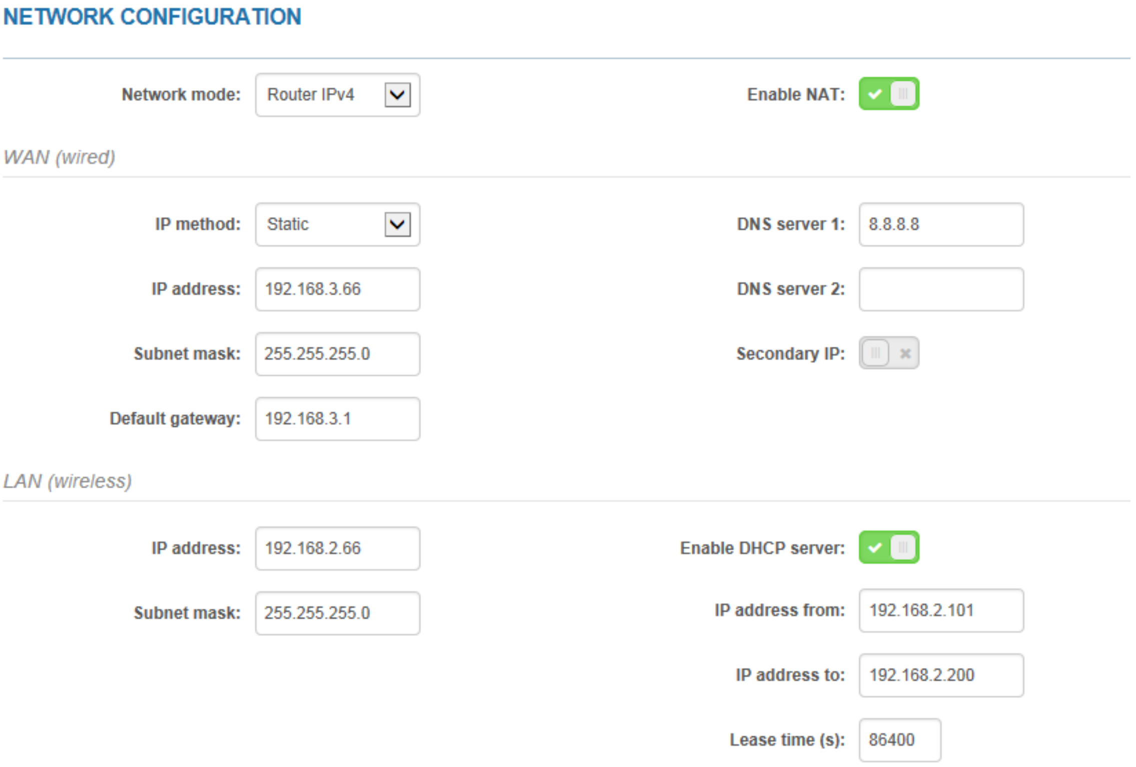
IPv6 prefix length– enter the Prefix Length for the address.

IPv6 default gateway – specify IPv6 address for default gateway.

IPv6 DNS server – specify the Domain Naming Server IPv6 addresses.

Router IPv4 Mode

This section allows customizing parameters of the Router to suit the needs of network, including ability to use the built-in DHCP server. When device is configured to operate as Router, the following sections should be specified: WAN network settings, LAN network settings and LAN DHCP settings.



NETWORK CONFIGURATION

Network mode: Router IPv4

Enable NAT: ✓

WAN (wired)

IP method: Static

IP address: 192.168.3.66

Subnet mask: 255.255.255.0

Default gateway: 192.168.3.1

DNS server 1: 8.8.8.8

DNS server 2:

Secondary IP: ✗

LAN (wireless)

IP address: 192.168.2.66

Subnet mask: 255.255.255.0

Enable DHCP server: ✓

IP address from: 192.168.2.101

IP address to: 192.168.2.200

Lease time (s): 86400

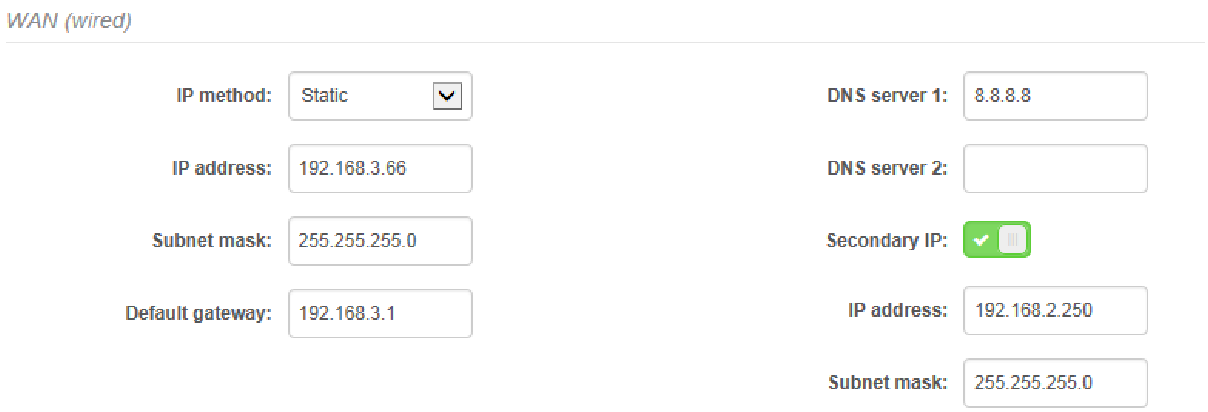
Figure 8 – Router IPv4 Settings

Enable NAT – select to enable NAT (Network Address Translation), that functions by transforming the private IP address of packets originating from hosts on your network so that they appear to be coming from a single public IP address and by restoring the destination public IP address to the appropriate private IP address for packets entering the private network, the multiple PCs on your network would then appear as a single client to the WAN interface.

WAN Settings

WAN network settings include settings related to the WAN interface. The access type of the WAN interface can be configured as: Static IP, Dynamic IP, PPPoE client.

IP method – choose **Static** to specify IP settings for device WAN interface:



WAN (wired)

IP method: Static

IP address: 192.168.3.66

Subnet mask: 255.255.255.0

Default gateway: 192.168.3.1

DNS server 1: 8.8.8.8

DNS server 2:

Secondary IP: ✓

IP address: 192.168.2.250

Subnet mask: 255.255.255.0

Figure 9 – Router IPv4 WAN Settings: Static IP

IP address – specify static IP address.

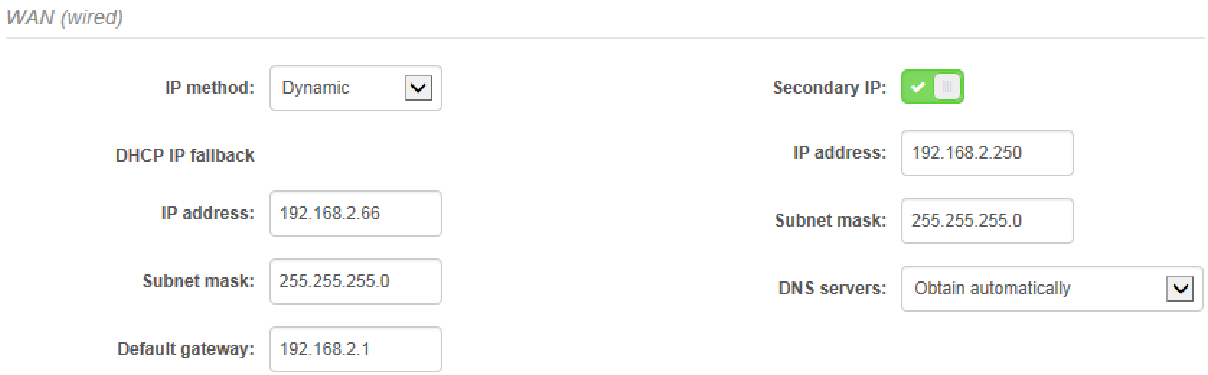
Subnet mask – specify a subnet mask.

Default gateway – specify a gateway.

DNS server – specify primary and/or secondary DNS server

Secondary IP – enable to specify the alternative IP address and the netmask for APC unit management.

WAN mode – choose **Dynamic** to enable DHCP client on the WAN side. This option does not need any parameters:



WAN (wired)

IP method: Dynamic

DHCP IP fallback

IP address: 192.168.2.66

Subnet mask: 255.255.255.0

Default gateway: 192.168.2.1

Secondary IP: ✓

IP address: 192.168.2.250

Subnet mask: 255.255.255.0

DNS servers: Obtain automatically

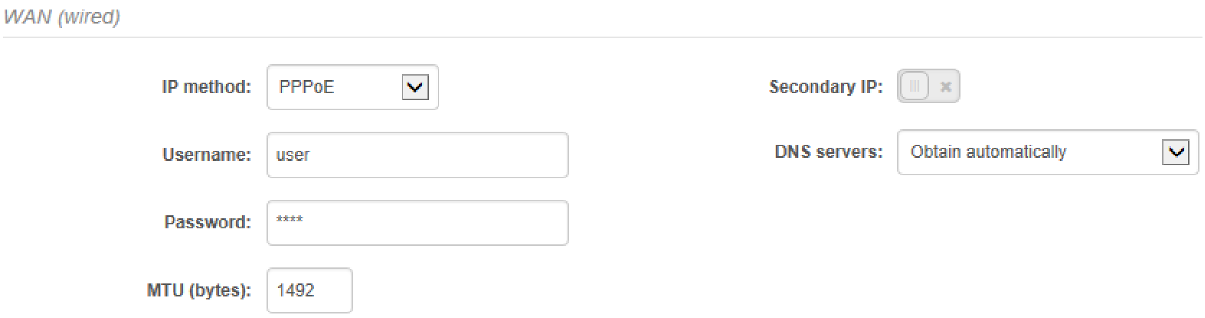
Figure 10 – Routers IPv4 WAN Settings: Dynamic IP

DHCP fallback setting – specify IP address, Subnet mask, Default gateway and optionally DNS server for DHCP fallback. In case the APC unit will not get the IP address from the DHCP, the specified fallback IP settings will be used.

Enable secondary IP – specify the alternative IP address and the netmask for APC unit management.

DNS servers – allows selecting if automatically assigned or alternative DNS servers should be used

WAN mode – choose PPPoE to configure WAN interface to connect to an ISP via a PPPoE:



WAN (wired)

IP method: PPPoE

Username: user

Password: ****

MTU (bytes): 1492

Secondary IP: ☐

DNS servers: Obtain automatically

Figure 11 – Routers IPv4 WAN Settings: PPPoE client

User name – specify the user name for PPPoE.

Password – specify the password for PPPoE.

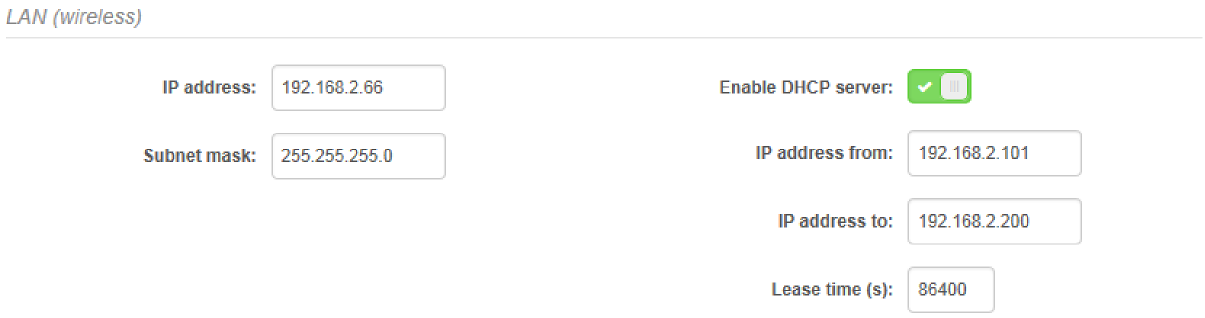
MTU – specify the MTU (Maximum Transmission Unit) in bytes.

Enable secondary IP – specify the alternative IP address and the netmask for APC unit management.

DNS settings – allows selecting if automatically assigned or alternative DNS servers should be used.

LAN Network Settings

LAN configuration include settings related to the LAN interface.



LAN (wireless)

IP address: 192.168.2.66

Subnet mask: 255.255.255.0

Enable DHCP server: ☑

IP address from: 192.168.2.101

IP address to: 192.168.2.200

Lease time (s): 86400

Figure 12 – Router LAN Settings

IP address – specify the IP address of the device LAN interface.

Subnet mask – specify the subnet mask of the device LAN interface.

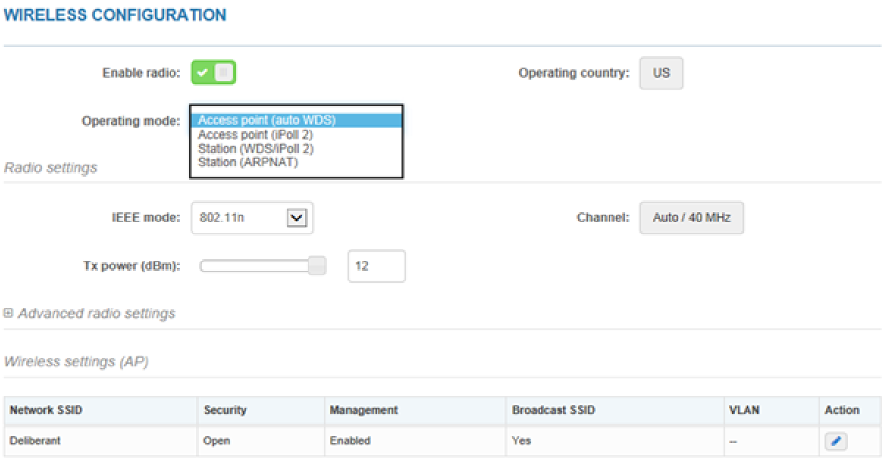
Enable DHCP server – select to enable DHCP server on LAN interface.

- **IP address from** – specify the starting IP address of the DHCP address pool.
- **IP address to** – specify the ending IP address of DHCP address pool.
- **Lease time** – specify the expiration time in seconds for the IP address assigned by the DHCP server.

Wireless

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 APC device can operate in four wireless modes: Access Point (autoWDS), Access Point (iPoll 2), Station (auto iPoll 2) and Station (ARPNAT).



WIRELESS CONFIGURATION

Enable radio: ✓

Operating country: US

Operating mode:

Radio settings

IEEE mode: 802.11n

Channel: Auto / 40 MHz

Tx power (dBm): 12

⊞ *Advanced radio settings*

Wireless settings (AP)

Network SSID	Security	Management	Broadcast SSID	VLAN	Action
Deliberant	Open	Enabled	Yes	--	

Figure 13 – Device Wireless Operating Mode

Depending on the wireless operation mode selection some of the displayed configuration parameters will differ (e.g. security or advanced wireless settings).

Operating mode – select wireless operation mode:

- **Station (auto iPoll 2)** – with this wireless mode the APC will act as Station and will automatically turn on iPoll 2 mode if detects that selected AP is operating in iPoll 2 protocol.
- **Station (ARPNAT)** – in this mode Station connects to other radios operating as an Access Point.

Wireless Mode: Access Point (auto WDS)

Enable radio – use slide to enable or disable APC radio.

Operating country - displays APC 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 APC unit's installation, though can be updated if required.

IEEE mode – specify the wireless network mode.

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 the button and the channel selection window will be displayed:

Channel width – The default channel bandwidth for 802.11 radio is 20MHz. The 802.11n allow channel bonding in such way the total channel width becomes 40MHz.

Channel table – select the channel(s) at which the Access Point 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.

Advanced Radio Settings

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

Max 802.11n MCS index – choose the maximum rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. If there will be an interference encountered, the APC will step down to the highest rate that allows data transmission.

Max legacy data rate – choose the maximum data rate in Mbps at which AP should transmit packets. The AP will attempt to transmit data at the highest data rate set. If there will be an interference encountered, the APC will step down to the highest rate that allows data transmission.

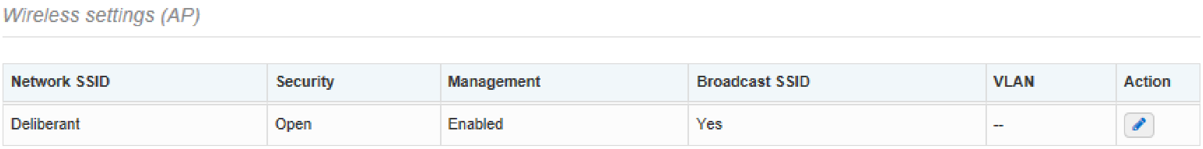
AMSDU – enable the AMSDU packet aggregation. If enabled, the maximum size of the 802.11 MAC frames will be increased.

Short GI – enable short guard interval. If selected, then 400ns value will be used, else 800ns.

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.

ACK timeout – specify the ACK timeout using slider or enter the value manually. Ack timeout can be entered by defining the link distance or specifying time value. Too low value of the ACK timeout will give very low throughput. A high value may slow down the link in noisy environment. A low value is far worse than a value slightly too high. ACK Timeout value should be tuned to the optimal value for the maximum link throughput.

Wireless Settings (AP)

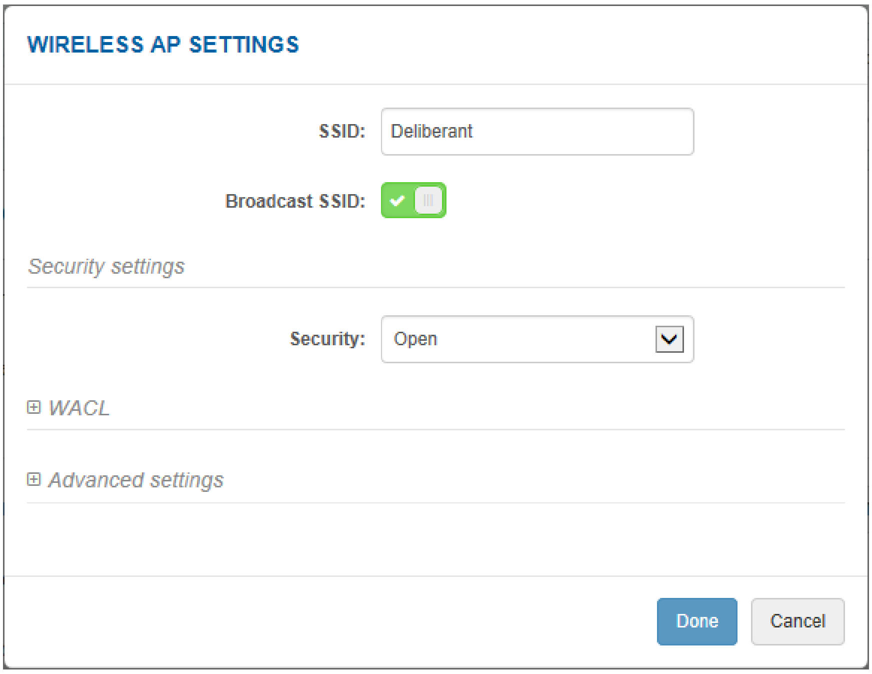


Wireless settings (AP)

Network SSID	Security	Management	Broadcast SSID	VLAN	Action
Deliberant	Open	Enabled	Yes	--	✎

Figure 14 - Wireless Settings

The wireless table allows configure main AP parameters, such as SSID, Security, WACL, etc. Click on the edit icon ✎ and the wireless settings window will be displayed:



WIRELESS AP SETTINGS

SSID: Deliberant

Broadcast SSID: ✓

Security settings

Security: Open

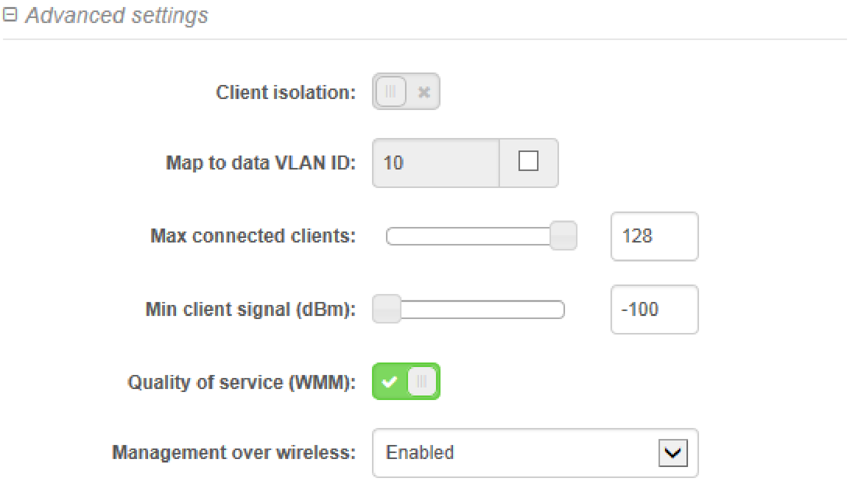
Figure 15 – Wireless AP Settings

SSID – specify the SSID of the wireless network device.

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

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

Advanced AP Settings



⊟ *Advanced settings*

Client isolation: ✕

Map to data VLAN ID: 10 □

Max connected clients: 128

Min client signal (dBm): -100

Quality of service (WMM): ✓

Management over wireless: Enabled

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.

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

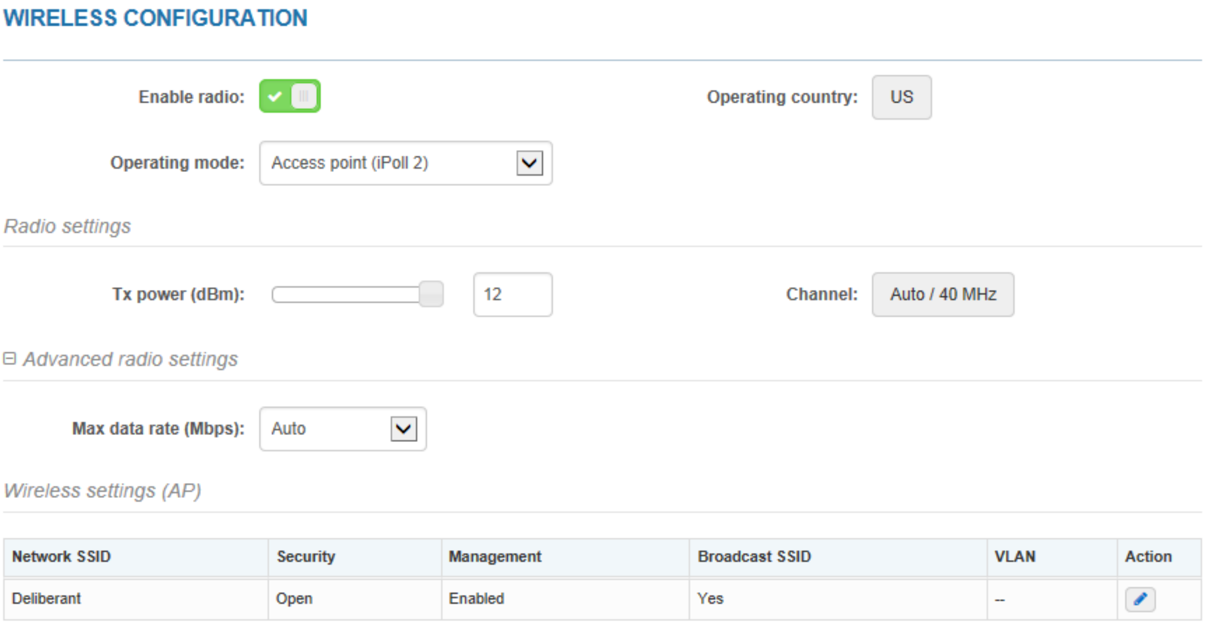
Max connected clients - specify the maximum number of associated wireless clients on the AP radio.

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

Quality of service (WMM) – enable to support quality of service for prioritizing traffic.

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 APC.

Wireless Mode: Access Point (iPoll 2)



WIRELESS CONFIGURATION

Enable radio: ✓

Operating country: US

Operating mode: Access point (iPoll 2)

Radio settings

Tx power (dBm): 12

Channel: Auto / 40 MHz

⊟ *Advanced radio settings*

Max data rate (Mbps): Auto

Wireless settings (AP)

Network SSID	Security	Management	Broadcast SSID	VLAN	Action
Deliberant	Open	Enabled	Yes	--	✎

Figure 16 – iPoll Access Point's Wireless Settings

Enable radio – use slide to enable or disable APC radio.

Operating country - displays APC 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 APC unit's installation, though can be updated if required.

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 the button and the channel selection window will be displayed:

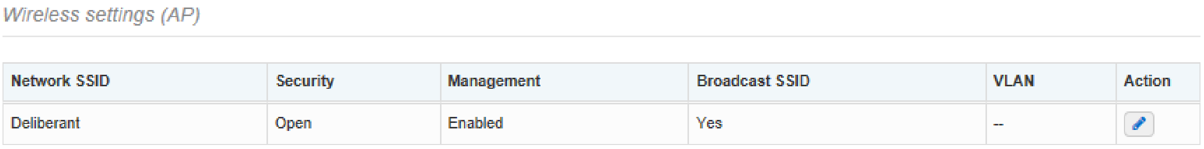
Channel width – The default channel bandwidth for 802.11 radio is 20MHz. The 802.11n allow channel bonding in such way the total channel width becomes 40MHz.

Channel table – select the channel(s) at which the Access Point iPoll 2 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.

Advanced Radio Settings

Max data rate (Mbps) – choose the maximum rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. If there will be an interference encountered, the APC will step down to the highest rate that allows data transmission.

Wireless Settings (AP)



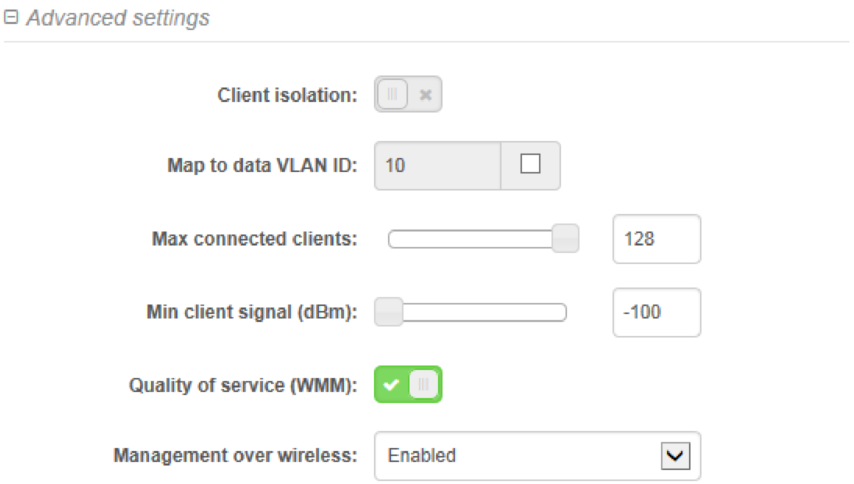
Wireless settings (AP)

Network SSID	Security	Management	Broadcast SSID	VLAN	Action
Deliberant	Open	Enabled	Yes	--	✎

Figure 17 - Wireless Settings

The wireless table allows configure main AP parameters, such as SSID, Security, WACL, etc. Click on the edit icon ✎ and the wireless settings window will be displayed:

Advanced AP Settings



⊟ *Advanced settings*

Client isolation: ☒

Map to data VLAN ID: 10 □

Max connected clients: 128

Min client signal (dBm): -100

Quality of service (WMM): ✓

Management over wireless: Enabled

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.

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

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.

Quality of service (WMM) – enable to support quality of service for prioritizing traffic.

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 APC.

Wireless Mode: Station (WDS/iPoll 2)

With this wireless mode, the APC will operate as wireless Station, though it automatically switch on the iPoll 2 mode if the specified access point will be detected as an AP iPoll 2. If the Station finds two networks with the same SSID, where one is iPoll 2, another 11n, the connection priority will be iPoll 2.

Enable radio – use slide to enable or disable APC radio.

Operating country - displays APC 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 APC unit's installation, though can be updated if required.

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 width - The default channel bandwidth for 802.11 radio is 20MHz. The 802.11n allow channel bonding in such way the total channel width becomes 40MHz.

Advanced Radio Settings

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

Max 802.11n MCS index – choose the maximum rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. If there will be an interference encountered, the device will step down to the highest rate that allows data transmission.

Max legacy data rate – choose the maximum data rate in Mbps at which device should transmit packets. It will attempt to transmit data at the highest data rate set. If there will be an interference encountered, the device will step down to the highest rate that allows data transmission.

AMSDU – enable the AMSDU packet aggregation. If enabled, the maximum size of the 802.11 MAC frames will be increased.

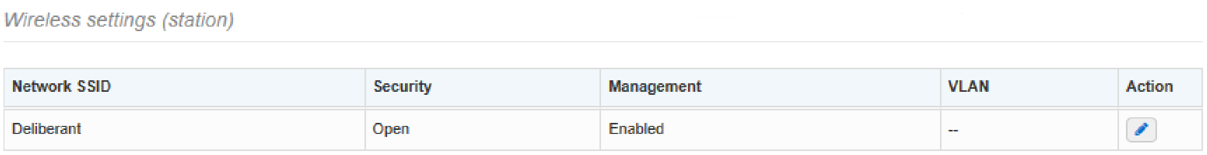
Short GI – enable short guard interval. If selected, then 400ns value will be used, else 800ns.

Fragmentation – specify the Fragmentation threshold using slider or enter the value manually [256-2346 bytes]. This is the maximum size for a packet before data is fragmented into multiple packets. Setting the Fragmentation threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

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.

ACK timeout – specify the ACK timeout using slider or enter the value manually. Ack timeout can be entered by defining the link distance or specifying time value. Too low value of the ACK timeout will give very low throughput. A high value may slow down the link in noisy environment. A low value is far worse than a value slightly too high. ACK Timeout value should be tuned to the optimal value for the maximum link throughput.

Wireless Settings (Station)

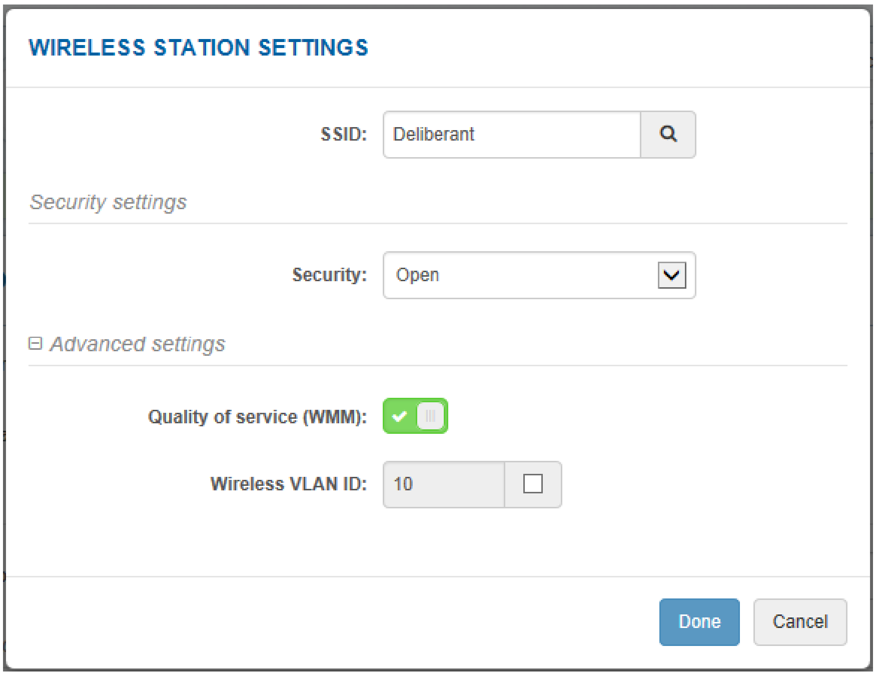


Wireless settings (station)

Network SSID	Security	Management	VLAN	Action
Deliberant	Open	Enabled	--	

Figure 18 - Wireless Settings

The wireless table allows configure main station parameters, such as SSID of the AP unit, Security, etc. Click on the edit icon and the wireless settings window will be displayed:



WIRELESS STATION SETTINGS

SSID: Deliberant

Security settings

Security: Open

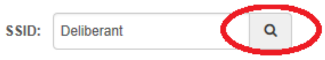
⊟ *Advanced settings*

Quality of service (WMM): ✓

Wireless VLAN ID: 10 □

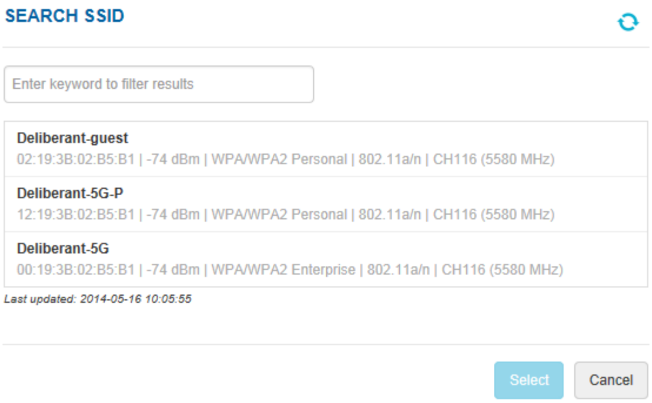
Figure 19 – Wireless AP Settings

SSID – specify the SSID of the wireless network device manually, or scan for iPoll 2 Access Points automatically:



SSID: Deliberant

If auto scan for SSID is used, the results will be displayed in the Search SSID table, thus simply click on the required AP and SSID will be selected:



SEARCH SSID

Enter keyword to filter results

Deliberant-guest
02:19:3B:02:B5:B1 | -74 dBm | WPA/WPA2 Personal | 802.11a/n | CH116 (5580 MHz)

Deliberant-5G-P
12:19:3B:02:B5:B1 | -74 dBm | WPA/WPA2 Personal | 802.11a/n | CH116 (5580 MHz)

Deliberant-5G
00:19:3B:02:B5:B1 | -74 dBm | WPA/WPA2 Enterprise | 802.11a/n | CH116 (5580 MHz)

Last updated: 2014-05-16 10:05:55

For detailed information about security settings refer at the respective sections *Wireless Security*.

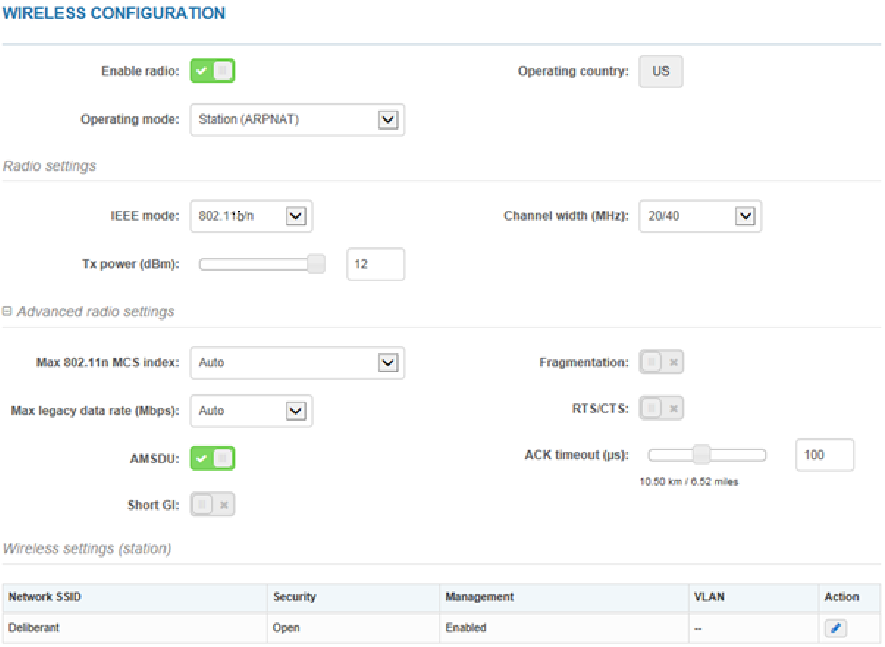
Advanced AP Settings

Quality of service (WMM) – enable to support quality of service for prioritizing traffic.

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

Wireless Mode: Station (ARPNAT)

Use Wireless Configuration to setup radio interface of the device.



WIRELESS CONFIGURATION

Enable radio: ✓ | Operating country: US

Operating mode: Station (ARPNAT)

Radio settings

IEEE mode: 802.11b/n | Channel width (MHz): 20/40

Tx power (dBm): 12

⊟ Advanced radio settings

Max 802.11n MCS index: Auto | Fragmentation: ✗

Max legacy data rate (Mbps): Auto | RTS/CTS: ✗

AMSDU: ✓ | ACK timeout (µs): 100

10.50 km / 6.52 miles

Short GI: ✗

Wireless settings (station)

Network SSID	Security	Management	VLAN	Action
Deliberant	Open	Enabled	--	✎

Figure 20 – Station Wireless Settings

Enable radio – use slide to enable or disable APC radio.

Operating country - displays APC 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 APC unit's installation, though can be updated if required.

IEEE mode – specify the wireless network mode.

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 width - The default channel bandwidth for 802.11 radio is 20MHz. The 802.11n allow channel bonding in such way the total channel width becomes 40MHz.

Advanced Radio Settings

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

Max 802.11n MCS index – choose the maximum rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. If there will be an interference encountered, the device will step down to the highest rate that allows data transmission.

Max legacy data rate – choose the maximum data rate in Mbps at which device should transmit packets. It will attempt to transmit data at the highest data rate set. If there will be an interference encountered, the device will step down to the highest rate that allows data transmission.

AMSDU – enable the AMSDU packet aggregation. If enabled, the maximum size of the 802.11 MAC frames will be increased.

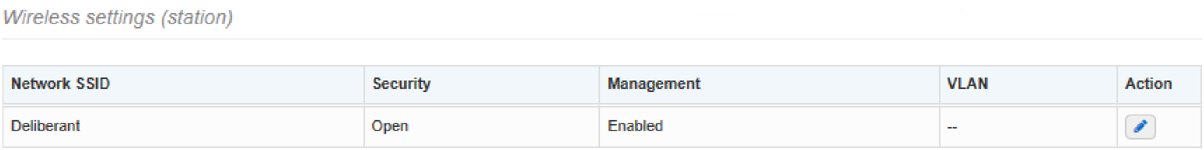
Short GI – enable short guard interval. If selected, then 400ns value will be used, else 800ns.

Fragmentation – specify the Fragmentation threshold using slider or enter the value manually [256-2346 bytes]. This is the maximum size for a packet before data is fragmented into multiple packets. Setting the Fragmentation threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

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.

ACK timeout – specify the ACK timeout using slider or enter the value manually. Ack timeout can be entered by defining the link distance or specifying time value. Too low value of the ACK timeout will give very low throughput. A high value may slow down the link in noisy environment. A low value is far worse than a value slightly too high. ACK Timeout value should be tuned to the optimal value for the maximum link throughput.

Wireless Settings (Station)

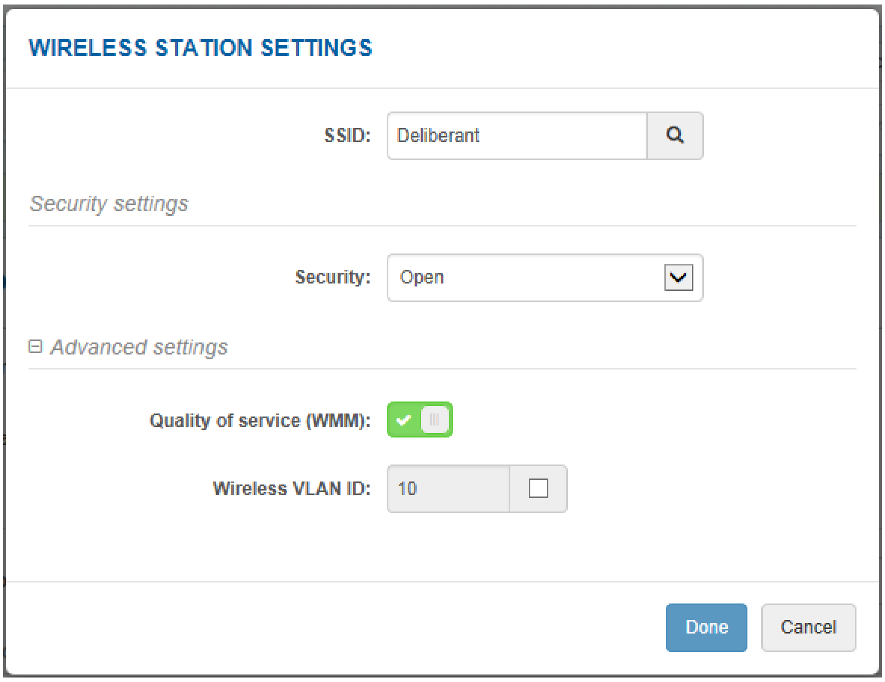


Wireless settings (station)

Network SSID	Security	Management	VLAN	Action
Deliberant	Open	Enabled	--	✎

Figure 21 - Wireless Settings

The wireless table allows configure main station parameters, such as SSID of the AP unit, Security, etc. Click on the edit icon ✎ and the wireless settings window will be displayed:



WIRELESS STATION SETTINGS

SSID: Deliberant

Security settings

Security: Open

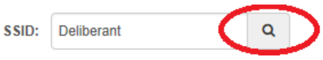
⊟ Advanced settings

Quality of service (WMM): ✓

Wireless VLAN ID: 10 □

Figure 22 – Wireless Station Settings

SSID – specify the SSID of the wireless network device manually, or scan for iPoll 2 Access Points automatically:



SSID: Deliberant

If auto scan for SSID is used, the results will be displayed in the Search SSID table, thus simply click on the required AP and SSID will be selected:

For detailed information about security settings refer at the respective sections *Wireless Security*.

Advanced AP Settings

Quality of service (WMM) – enable to support quality of service for prioritizing traffic.

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

Wireless Security

If APC acts as an Access Point (auto WDS) or Access Point (iPoll 2) 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.

The APC supports various authentication/encryption methods:

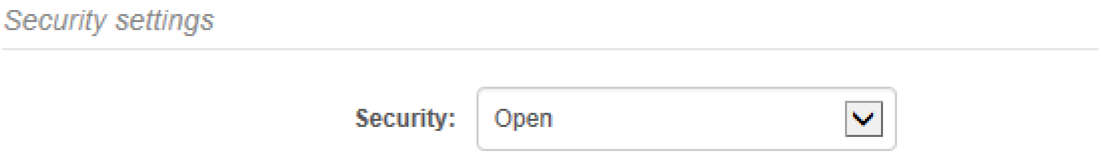
- **Open** – no encryption.
- **WEP** – encrypts the data portion of each packet exchanged on a wireless network using a 64-bit or 128-bit WEP encryption key.
- **Personal WPA/WPA2** – authorizes and identifies clients based on a secret key that changes automatically at regular intervals.
- **Enterprise WPA/WPA2** – RADIUS server based authentication (requires configured RADIUS server).

Available security methods, according APC operating wireless mode is listed in the table below:

Security method	Access Point (autoWDS)	Access Point (iPoll 2)	Station (WDS/iPoll 2)	Station (ARPNAT)
Open	×	×	×	×
WEP 64bit/128bit			×	×
Personal WPA/WPA2	×	×	×	×
Enterprise WPA/WPA2	×	×	×	×

Open

By default there is no encryption enabled on the APC device:



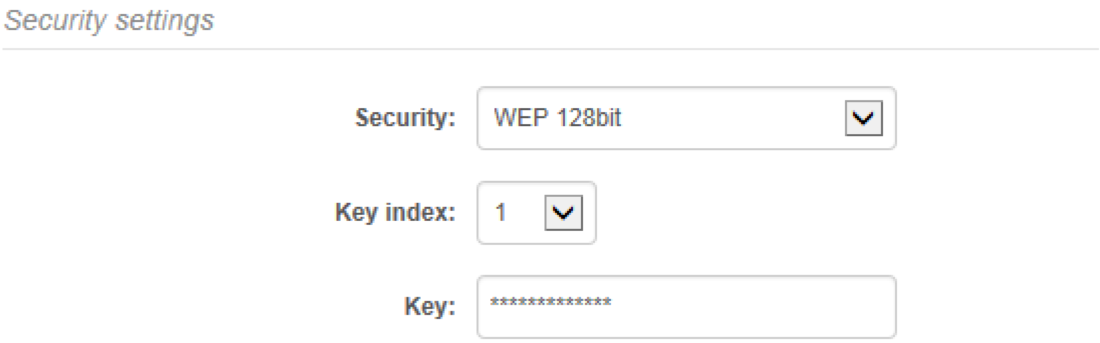
Security settings

Security: Open

Figure 23 – Wireless Security: Open with RADIUS MAC Authentication Enabled

WEP Encryption

WEP encryption can be either 64bit or 128bit.Select the required one and enter the rest parameters:



Security settings

Security: WEP 128bit

Key index: 1

Key: *************

Figure 24 –Wireless Security: WEP Security

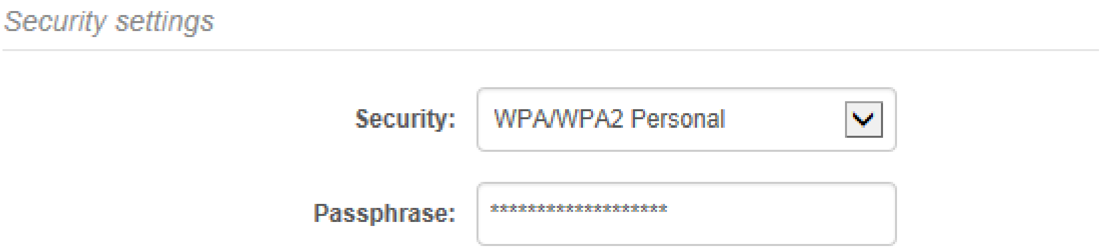
Key index - select the WEP key index [1-4]. Each number represents one of the four static keys of WEP. The selected key index will be used for frame encryption and decryption.

Key – specify the passkey, for the chosen WEP security:

- For **WEP 64bit** encryption – 5 HEX pairs (e.g. aa:bb:cc:dd:ee), or 5 ASCII characters (e.g. abcde);
- For **WEP 128bit** encryption – 13 HEX pairs (e.g. aa:bb:cc:dd:ee:ff:gg:hh:00:11:22:33:44), or 13 ASCII characters (e.g. abcdefghijklm);

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

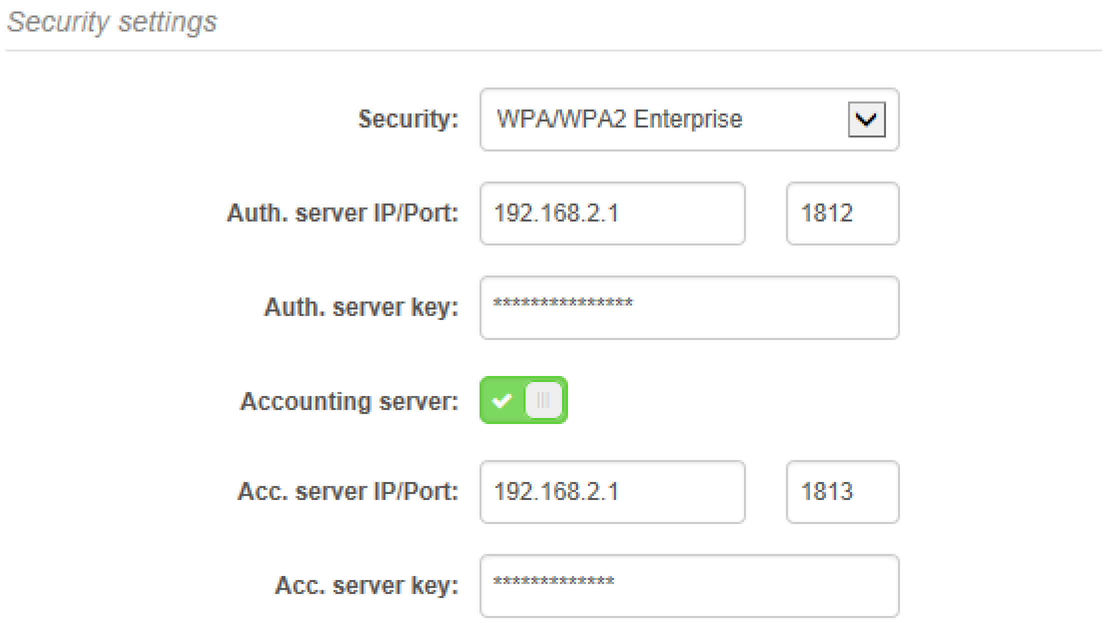
Passphrase: *******************

Figure 25 –Wireless Security: Personal WPA/WPA2 Security

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

WPA/WPA2 Enterprise for Access Points

APC 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: 192.168.2.1 1812

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

Accounting server: ✓

Acc. server IP/Port: 192.168.2.1 1813

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

Figure 26 –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.

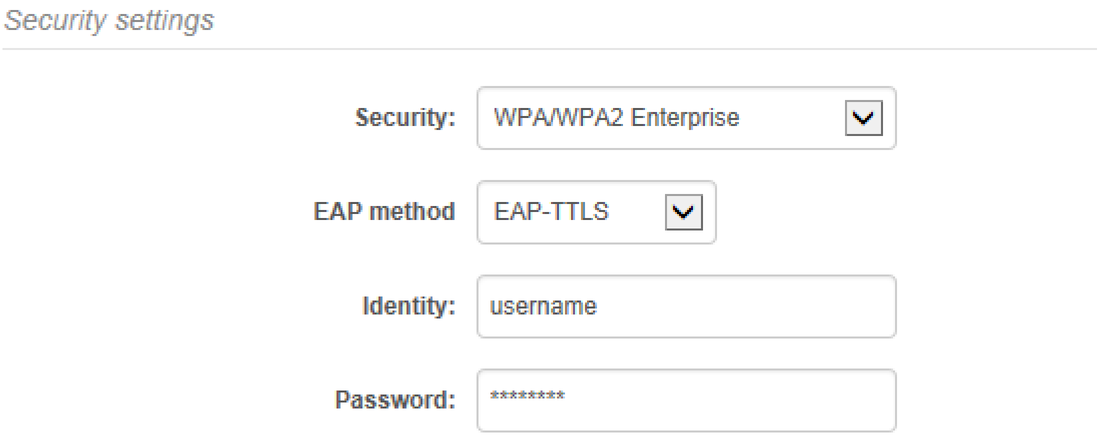
Accounting server – use slide to enable accounting RADIUS server, if required.

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.

WPA/WPA2 Enterprise for Stations

If APC is operating in Station wireless mode, Station will send requests to AP, which will redirect authentication parameters to required RADIUS server.



Security settings

Security: WPA/WPA2 Enterprise

EAP method EAP-TTLS

Identity: username

Password: ********

Figure 27 –Wireless Security: Enterprise WPA/WPA2 Security for Stations

EAP method – choose EAP method:

- **EAP-TTLS**
- **PEAP**

Identity – specify the identity of the authentication to the RADIUS server.

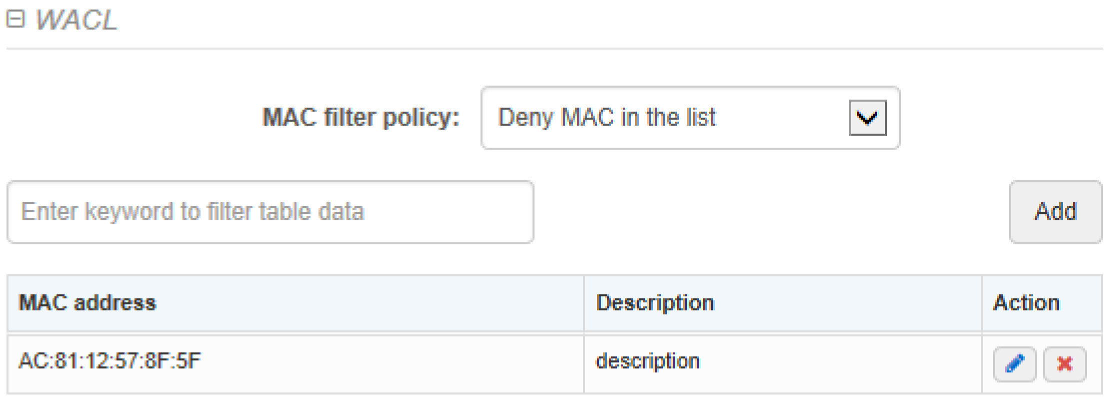
Password – specify the password of the authentication to the RADIUS server.

Identity and Password on the Station must match the identity and password running on the RADIUS server's user list.

Wireless ACL

Wireless ACL is active only in **Access Point (auto WDS)** and **Access Point (iPoll 2)** wireless modes.

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).



⊟ WACL

MAC filter policy: Deny MAC in the list

MAC address	Description	Action
AC:81:12:57:8F:5F	description	✎ ✖

Figure 28 – Wireless ACL Configuration

MAC filter policy – define the policy:

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

To add new rule, press the **Add** button.

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

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

Services Configuration

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

- Date & time
- Remote management
- SNMP
- Ping watchdog
- WNMS

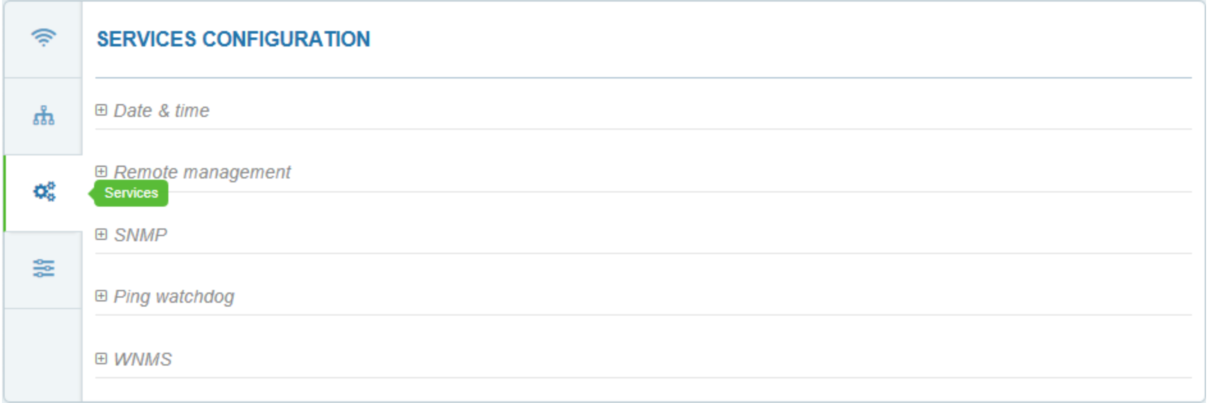
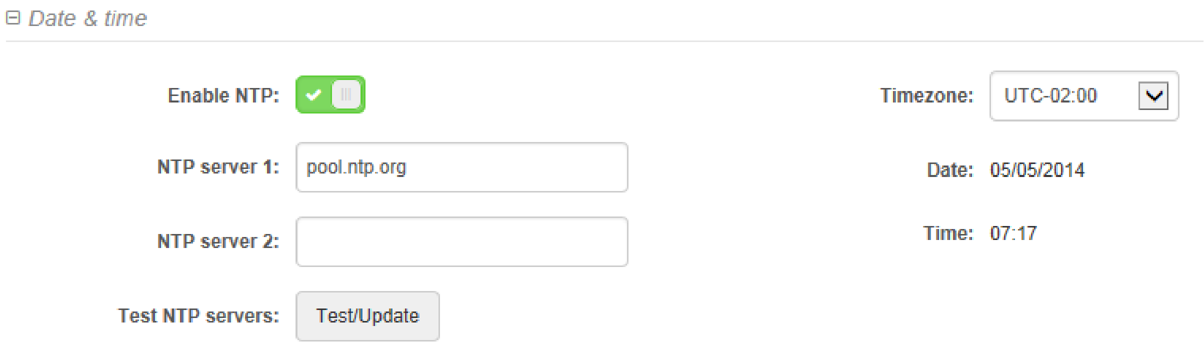


Figure 29 - Services Menu

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: ✓
NTP server 1: pool.ntp.org
NTP server 2:
Test NTP servers: Test/Update
Timezone: UTC-02:00
Date: 05/05/2014
Time: 07:17

Figure 30 – Date&time: NTP Configuration

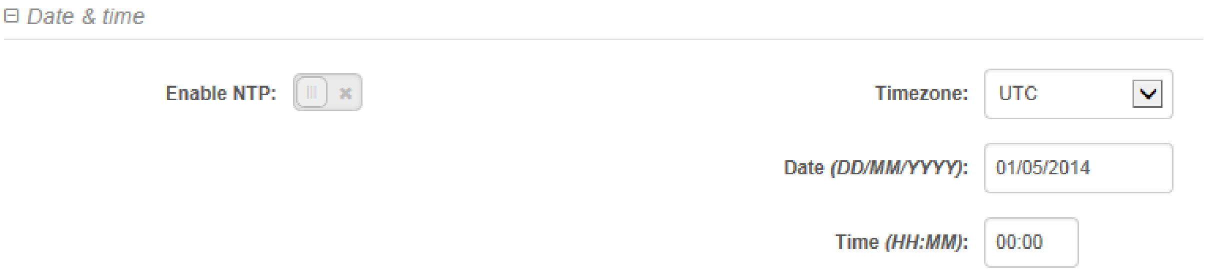
Enable NTP – select this option as enabled to configure NTP.

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 31 – Date&time: Manual Configuration

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

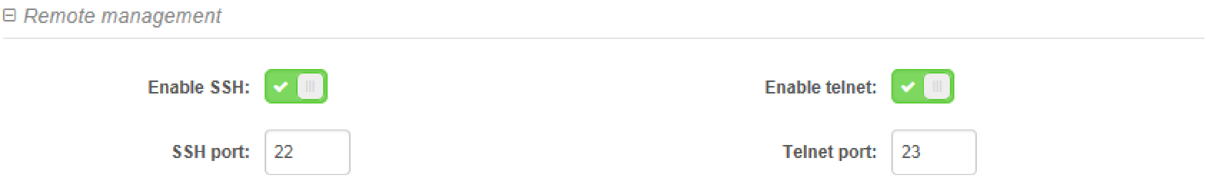
Timezone – select the timezone. Time zone should be specified as a difference between local time and UTC time.

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 APC via SSH and Telnet:



⊟ Remote management

Enable SSH: ✓

SSH port: 22

Enable telnet: ✓

Telnet port: 23

Figure 32 – Remote Management Configuration

Enable SSH – enable or disable SSH access to device.

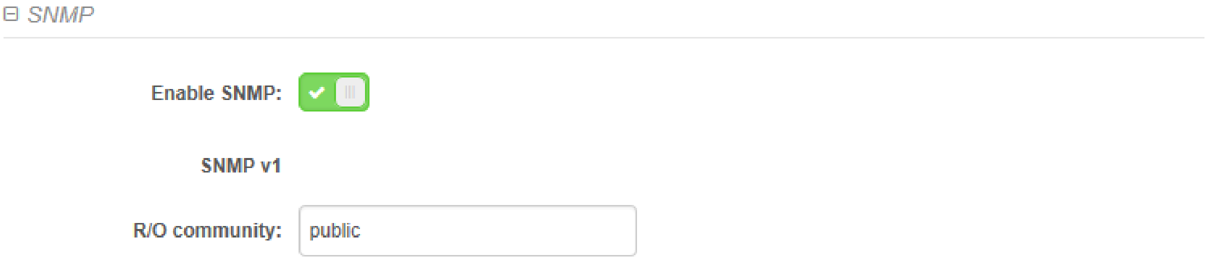
SSH port – specify the SSH service port. By default SSH port is 22.

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

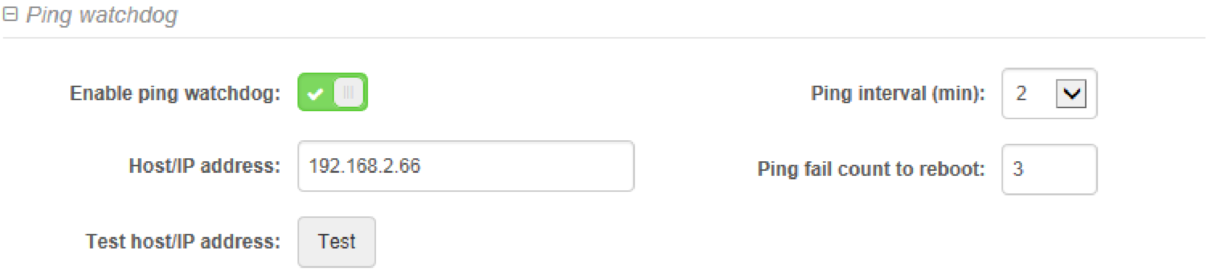
Figure 33 – SNMP Service Settings

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 an APC unit manager to read values, but denies any attempt to change values.

Ping watchdog

Enable Ping Watchdog for continuous monitoring of the APC unit network connection with the specified trusted host. If enabled, the APC unit will send Ping requests periodically to the host and in case there is no response within a specified time period, the Ping Watchdog will reboot the APC unit.



⊟ Ping watchdog

Enable ping watchdog: ✓

Host/IP address: 192.168.2.66

Ping interval (min): 2

Ping fail count to reboot: 3

Figure 34 –Ping Watchdog

Enable ping watchdog – click to enable Ping Watchdog function.

Host/IP address – specify the host where the Ping requests will be sent to.

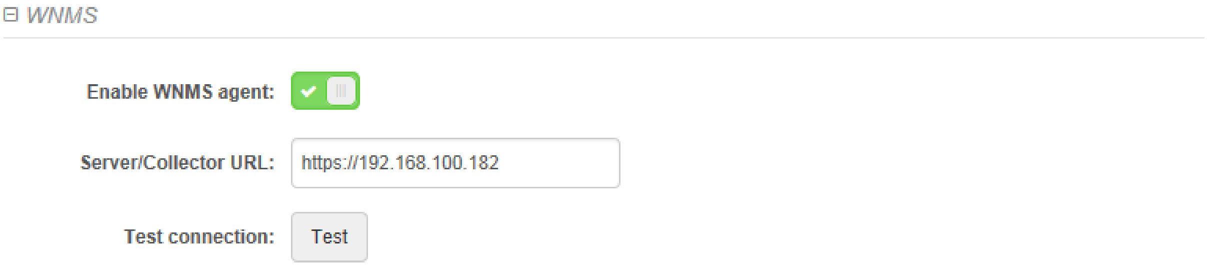
Test host/IP address - click this button to check if the specified host responses successfully.

Ping interval - specify the interval, in minutes, between Ping requests.

Ping fail count to reboot - specify the count of failed Ping replies. After specified count of Ping failures, the APC unit will reboot itself automatically.

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 an WNMS client service running on every device.



⊟ *WNMS*

Enable WNMS agent: ✓

Server/Collector URL: https://192.168.100.182

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 APC settings and perform main system actions (reboot, restore configuration, etc.). The section is divided into further five sections:

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

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

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

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

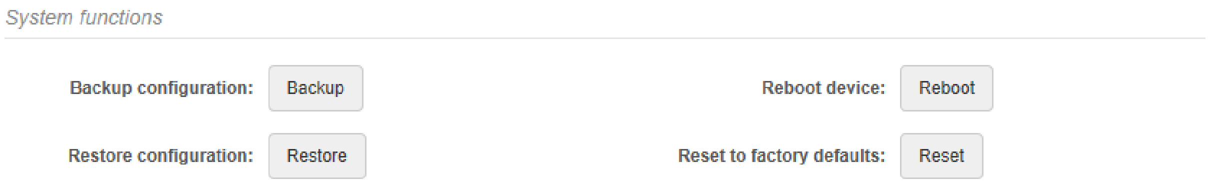


Figure 35 - System Functions

New configuration will be effective after the *Apply* button is activated and system reboot cycle is completed. Previous system configuration is deleted after *Apply* button is activated. It is highly recommended to backup the system configuration before uploading the new configuration.

Restore configuration – click to upload an existing configuration file to the device.

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.

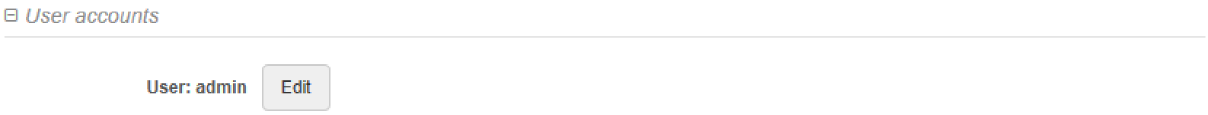
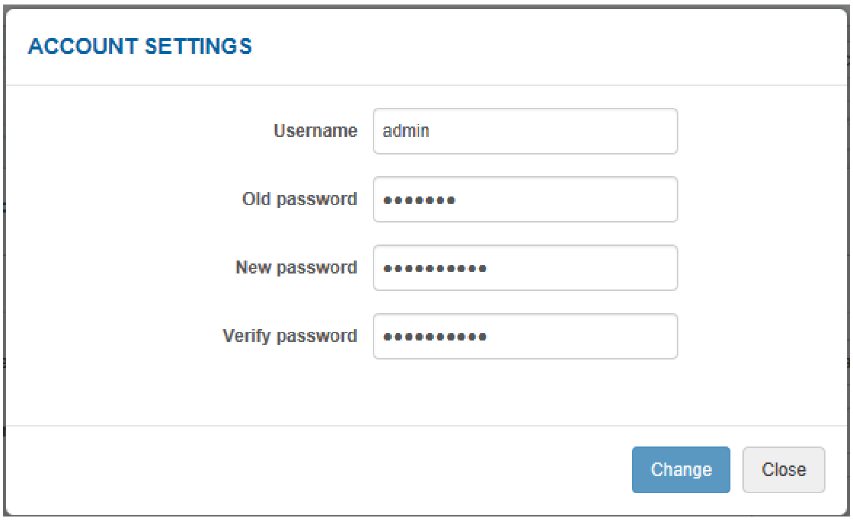


Figure 36 – User Accounts

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 37 – User Account Settings

Username – change the administrator's username.

Old password – enter the old administrator password.

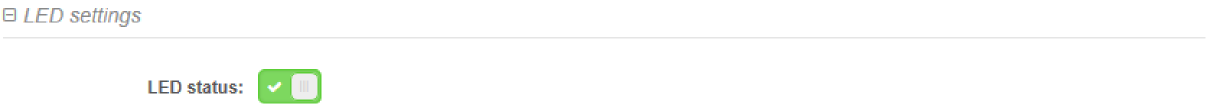
New password – enter the new administrator password for user authentication.

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.

LED settings

The APC has possibility to control LEDs:



⊟ *LED settings*

LED status: ✓

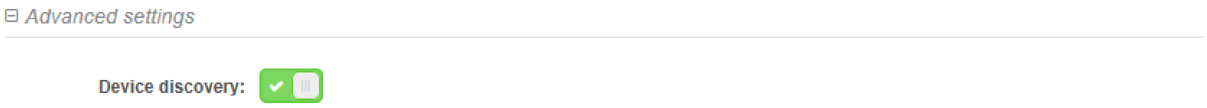
Figure 38 – Device LED Control

LED status – use the slide to disable or enable LED signals.

Advanced settings

Device discovery function is available only on **Station (WDS/iPoll2)** and **Station (ARPNAT)** wireless modes.

Enable this feature to allow the APC unit discovery within reach of a single multicast packet.



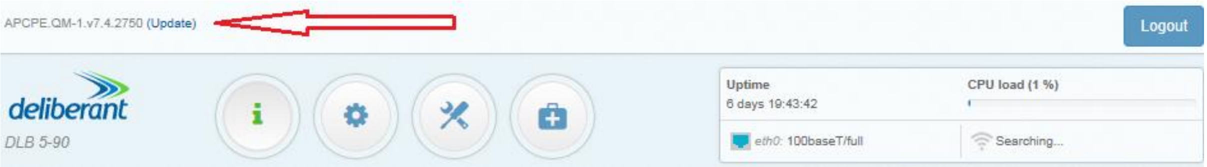
Device discovery: ✓

Figure 39 – Device discovery

Device discovery – select to enable APC discovery function.

Firmware Upgrade

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

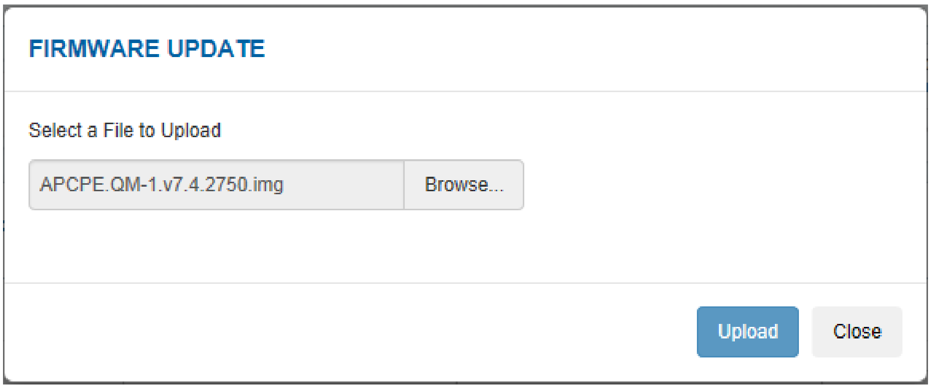


APCPE.QM-1.v7.4.2750 (Update)

Figure 40 – 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:



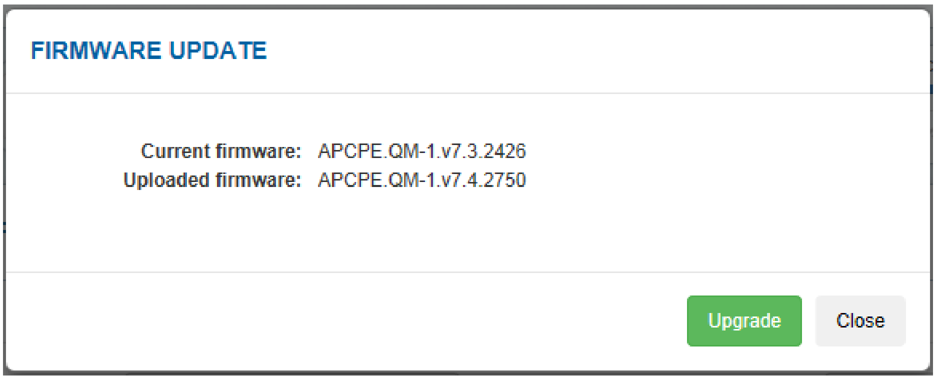
FIRMWARE UPDATE

Select a File to Upload

APCPE.QM-1.v7.4.2750.img

Figure 41 – 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 **Upload** button:


FIRMWARE UPDATE

Current firmware: APCPE.QM-1.v7.3.2426
Uploaded firmware: APCPE.QM-1.v7.4.2750

Figure 42 –Firmware Upgrade

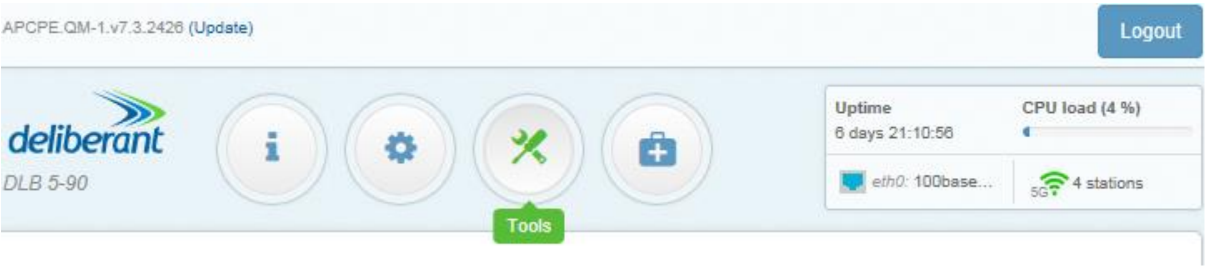
Current version – displays version of the current firmware.

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



APCPE.QM-1.v7.3.2426 (Update)

Logout

deliberant

DLB 5-90

Tools

Uptime
6 days 21:10:56

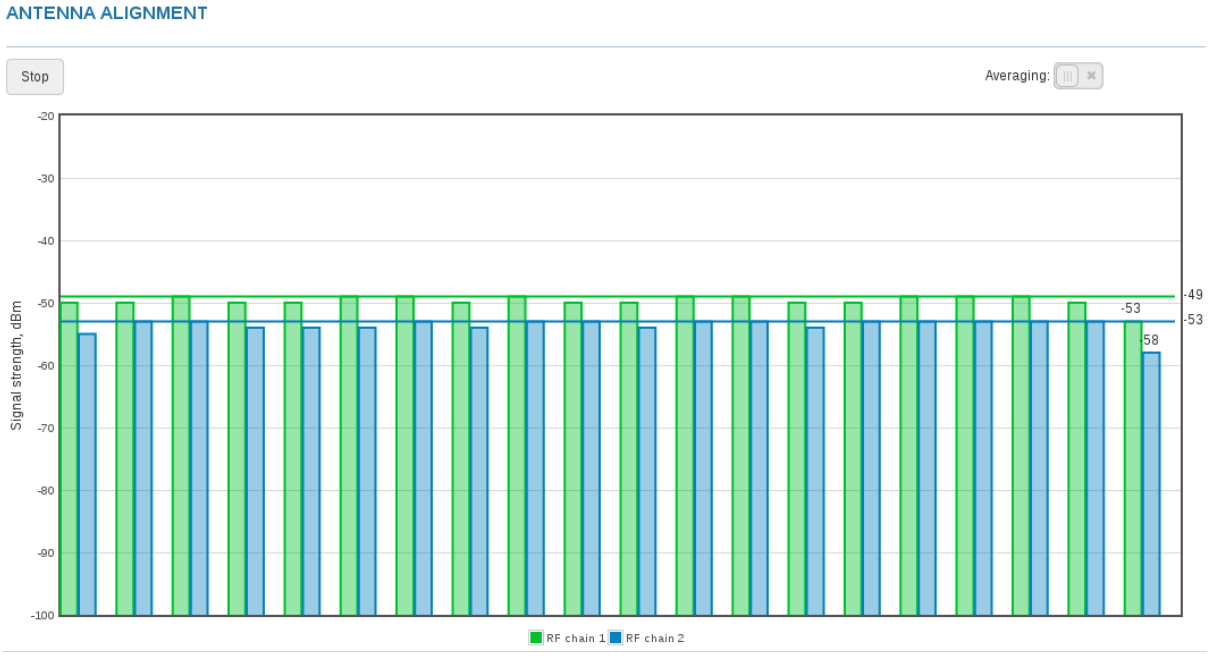
CPU load (4 %)

eth0: 100base...

5G 4 stations

Antenna Alignment

The Antenna Alignment tool measures signal quality between the Station and AP. For best results during the antenna alignment test, turn off all wireless networking devices within range of the device except the device(s) with which you are trying to align the antenna. Watch the constantly updated display as you adjust the antenna.



ANTENNA ALIGNMENT

Stop

Averaging: ☐

Figure 43 – Antenna Alignment

Start – press this button to start antenna alignment.

Stop – press this button to stop antenna alignment.

Averaging – if this option enabled, the graph will display the average Signal Strength of both antennas.

Site Survey

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

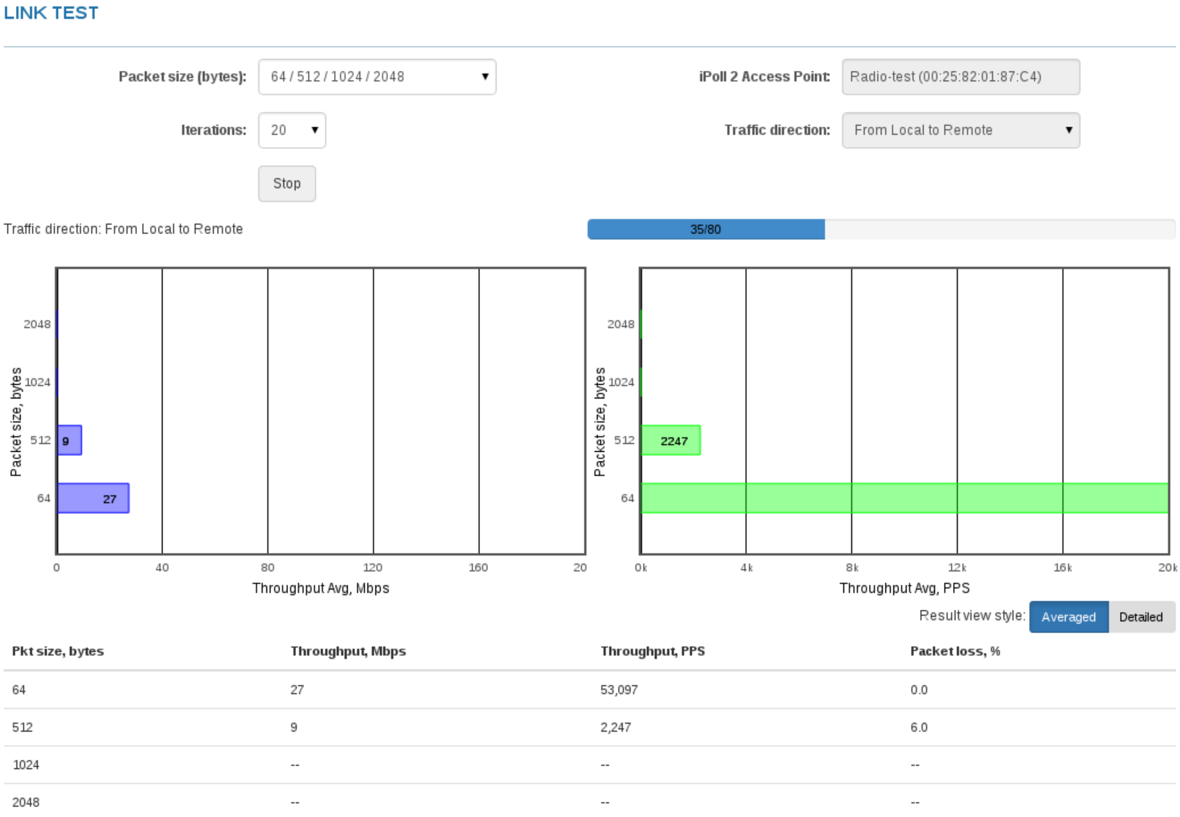
To perform the Site Survey test currently, click the **Start scan**:

Last updated – displays when the last scan was performed.

Link Test

It is recommended to ensure that there is no traffic on the link before running the Link Test as results may not be completely accurate.

Use the Link test tool to check the quality of the established **iPoll 2** link. This tool tests the throughput at selected packet sizes and iterations.



LINK TEST

Packet size (bytes): 64 / 512 / 1024 / 2048

iPoll 2 Access Point: Radio-test (00:25:82:01:87:C4)

Iterations: 20

Traffic direction: From Local to Remote

Traffic direction: From Local to Remote

35/80

Pkt size, bytes	Throughput, Mbps	Throughput, PPS	Packet loss, %
64	27	53,097	0.0
512	9	2,247	6.0
1024	--	--	--
2048	--	--	--

Figure 44 – Linktest Results

Packet size - select packet sizes in bytes at which the test will be performed.

Iterations - select number of test iterations.

iPoll 2 Access Point – displays the Access Point information (iPoll 2 station side).

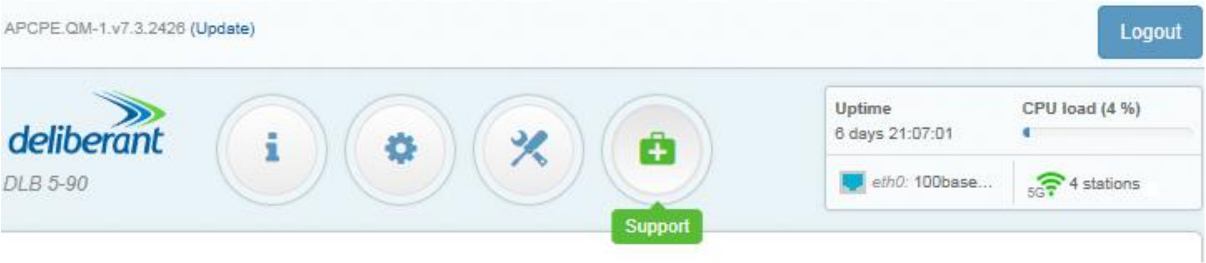
iPoll 2 station – select the Station the Link Test will be performed with (iPoll 2 Access Point side).

Traffic direction – select the traffic direction for the performing test.

Start – click to start the throughput test.

Stop – click to stop the throughput test.

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.

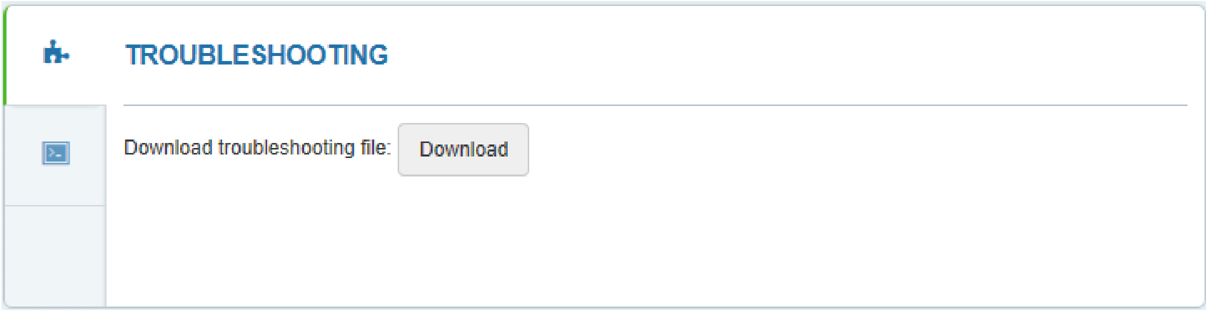


Figure 45 – Troubleshooting File Download

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.

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

Antennas:

Only below approved antennas can be used for this modular installation:
Type1: Manufacture: ExtraLink, Model: 2400A-12, Gain: 12dBi, Number: 2

Type2: Manufacture: Shenzhen fengliyuan, Model: FS-2400F, Gain: 3dBi, Number: 2