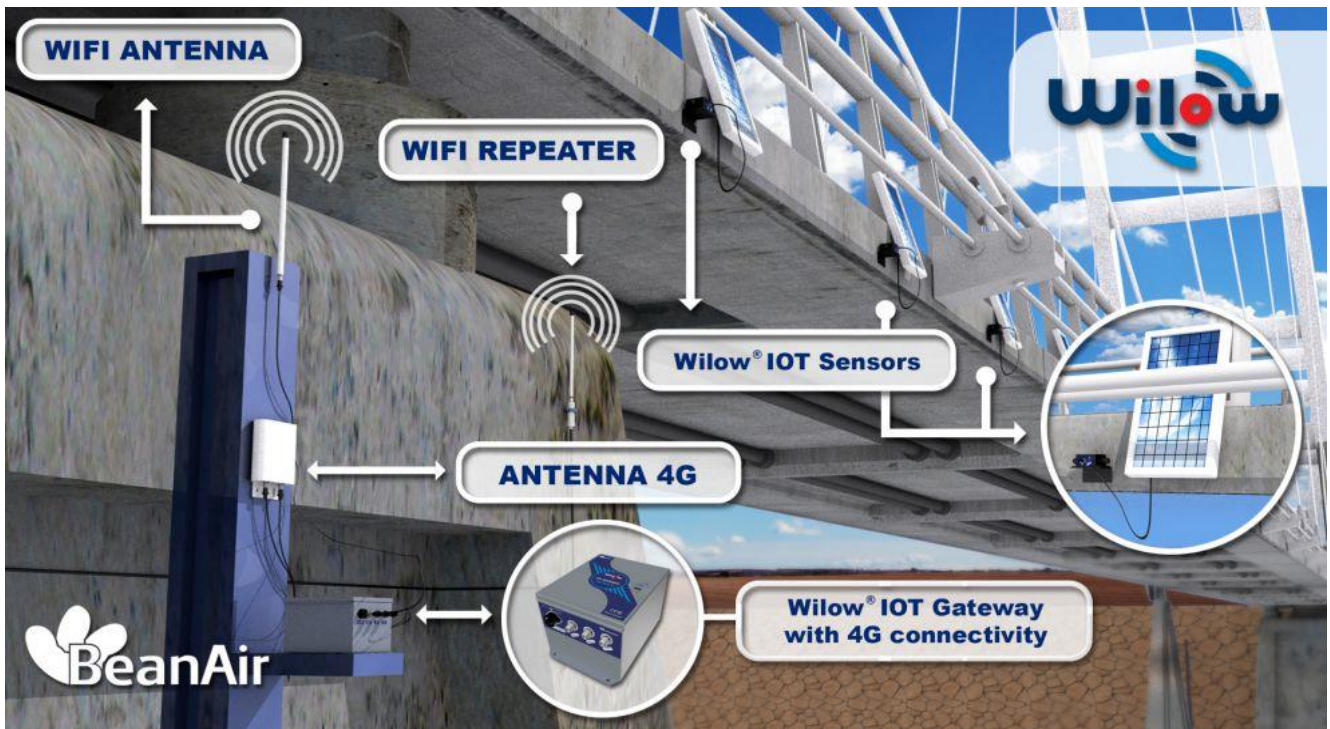


Version 1.4

WILOW®  
USER  
MANUAL

# WILOW® (WIFI LOW POWER) IOT GATEWAY USER GUIDE



 **BeanAir**  
Rethinking Sensing Technology



## DOCUMENT

Document ID	UM RF_07	Version	V1.3
External reference	UM-RF-09-ENG Wilow-IOT-Gateway	Date	08/05/2019
Author	Youssef Shahine		
		Project Code	
Document's name	Wilow® IoT Gateway		

## VALIDATION

Function	Destination	For validation	For info
Writer	Aymen Jegham	✓	
Reader	Mohamed-Yosri Jaouadi	✓	
Validation	Antje Jacob		✓

## DIFFUSION

Function	Destination	For action	For info
Reader n°1	Mohamed-Yosri Jaouadi., Software Architect	✓	
Reader n°2	Salah Riahi, Technical support engineer	✓	

## UPDATES

Version	Date	Author	Evolution & Status
1.0	12/01/2018	Aymen JEGHAM	<ul style="list-style-type: none"> <li>First version of the document</li> </ul>
1.1	25/06/2018	Youssef SHAHINE	<ul style="list-style-type: none"> <li>More information added about 3G/4G/LTE Router</li> <li>New section added about SIM Card provider</li> </ul>
1.2	08/08/2018	Aymen JEGHAM	<ul style="list-style-type: none"> <li>Public IP address and Dynamic DNS section added</li> <li>Port and public IP checking added</li> </ul>
1.3	21/02/2019	Youssef SHAHINE	<ul style="list-style-type: none"> <li>Firmware update on LTE Router</li> <li>Firmware update on Bullet M2 HP added</li> </ul>
1.3.1	08/05/2019	Mohamed Bechir Besbes	<ul style="list-style-type: none"> <li>Weblinks update</li> </ul>
V1.4	30/06/2019	Youssef SHAHINE	<ul style="list-style-type: none"> <li>Wiring code update due to Socket/Plug modifications for both Mains and Solar power supply</li> </ul>

## *Disclaimer*

The contents are confidential and any disclosure to persons other than the officers, employees, agents or subcontractors of the owner or licensee of this document, without the prior written consent of Beanair GmbH, is strictly prohibited.

Beanair makes every effort to ensure the quality of the information it makes available. Notwithstanding the foregoing, Beanair does not make any warranty as to the information contained herein, and does not accept any liability for any injury, loss or damage of any kind incurred by use of or reliance upon the information.

Beanair disclaims any and all responsibility for the application of the devices characterized in this document, and notes that the application of the device must comply with the safety standards of the applicable country, and where applicable, with the relevant wiring rules.

Beanair reserves the right to make modifications, additions and deletions to this document due to typographical errors, inaccurate information, or improvements to programs and/or equipment at any time and without notice.

Such changes will, nevertheless, be incorporated into new editions of this document.

Copyright: Transmittal, reproduction, dissemination and/or editing of this document as well as utilization of its contents and communication thereof to others without express authorization are prohibited. Offenders will be held liable for payment of damages. All rights are reserved.

Copyright © Beanair GmbH 2018



# Contents

- 1. TECHNICAL SUPPORT ..... 8
- 2. VISUAL SYMBOLS DEFINITION ..... 9
- 3. ACRONYMS AND ABBREVIATIONS..... 10
- 4. VISUAL SYMBOLS DEFINITION ..... 11
- 5. ACRONYMS AND ABBREVIATIONS..... 12
- 6. DOCUMENT ORGANISATION ..... 13
- 7. WILLOW® IOT GATEWAY PRODUCT PRESENTATION ..... 14
  - 7.1 Product overview ..... 14
  - 7.2 Outboxing your Wilow® IOT Gateway..... 15
  - 7.3 Accessories description ..... 16
  - 7.4 Wireless distribution System function description ..... 17
  - 7.5 Technical specifications..... 18
    - 7.5.1 Product reference..... 18
    - 7.5.2 WIFI Connectivity..... 19
    - 7.5.3 3G/4G/LTE Router ..... 19
    - 7.5.4 Environmental and Mechanical..... 20
      - 7.5.1 2.4GHz High Gain Antenna ..... 21
      - 7.5.2 Dual LTE Antenna ..... 21
      - 7.5.3 AC/DC power adapter with battery charger (UPS function) ..... 23
      - 7.5.4 Solar power supply with UPS battery ..... 26
      - 7.5.5 Included accessories..... 27
- 8. INSTALLATION GUIDELINE ..... 28
  - 8.1 How to Mount the Wilow® IOT Gateway..... 28
- 9. HOW TO SETUP A REMOTE ACCESS..... 29
  - 9.1 MQTT Architecture..... 29
  - 9.2 Which SIM card to use?..... 30
  - 9.3 Hardware description and system configuration..... 31

- 9.4 System configuration ..... 31
- 9.5 LTE Router configuration..... 32
  - 9.5.1 Pre-configured settings ..... 32
  - 9.5.2 SIM Card insertion ..... 32
  - 9.5.3 Logging to your router..... 33
  - 9.5.4 SIM card configuration ..... 35
  - 9.5.5 Checking your Mobile Status..... 37
  - 9.5.6 WiFi access point with WDS function, pre-configured settings (Ref: WILOW-IOT-GATEWAY-4G-WDS-MPWR) ..... 37
    - 9.5.1 WiFi access point pre-configured settings (Ref: WILOW-IOT-GATEWAY-4G -MPWR and (Ref: WILOW-IOT-GATEWAY-4G-SOLAR) ..... 38
    - 9.5.1 LAN configuration..... 38
    - 9.5.2 Public IP address and Dynamic DNS ..... 39
    - 9.5.3 MQTT Broker Configuration ..... 43
- 9.6 BeanDevice® Wilow® configuration ..... 44
  - 9.6.1 Authentication..... 46
  - 9.6.2 Keep alive ..... 46
  - 9.6.3 MQTT Status ..... 47
  - 9.6.4 Topic related to static measurement ..... 48
  - 9.6.5 Topic related to dynamic measurement ..... 48
  - 9.6.6 Subscribe ..... 48
- 9.7 Enabling the remote access at your office ..... 49
  - 9.7.1 BeanScape® RA configuration ..... 49
- 10. APPENDIX 1: WIFI AP WITH WDS FUNCTION - BULLET M2 HP CONFIGURATION (IF FACTORY SETTINGS ARE RESTORED)..... 52
  - 10.1 AirMax function..... 54
  - 10.2 Wireless Configuration..... 55
  - 10.3 Network configuration ..... 56
  - 10.4 Firmware update ..... 57
- 11. APPENDIX 2: LTE ROUTER CONFIGURATION (IF FACTORY SETTINGS ARE RESTORED) ..... 59
  - 11.1 Get an access to your LTE router ..... 59
  - 11.2 Internal wifi AP configuration ..... 61
    - 11.2.1 Case 1: Using Internal WIFI AP ..... 61
    - 11.2.2 Case 2: Using external WIFI AP with WDS function ..... 62
  - 11.3 Enable your MQTT Broker ..... 63

## List of Tables

**No table of figures entries found.**

## List of Figures

Figure 1: Remote access to Monitoring site .....	15
Figure 2: Outboxing your Wilow IOT Gateway .....	15
Figure 3 : Antenna connectors .....	16
Figure 4: WIFI cluster-tree network architecture with WDS function.....	17
Figure 5: Wifi star network architecture (without WDS function) .....	18
Figure 6: Dual LTE Antenna with u-clamp mounting kit .....	21
Figure 7 : Mains power supply – wiring code .....	24
Figure 8: Waterproof Plug .....	24
Figure 9 :MQTT architecture .....	29
Figure 10: Wilow® IOT Gateway enclosure .....	29
Figure 11 :Wilow® IoT Gateway (Ref: WILOW-IOT-GATEWAY-4G-WDS-MPWR).....	31
Figure 12 :Network configuration .....	32
Figure 13 :Inserting sim card .....	33
Figure 14 : Mobile status .....	37
Figure 15 :LAN configuration .....	39
Figure 16 :BeanDevice® Wilow® network settings configuration .....	44
Figure 17 :BeanDevice® Wilow® profile on BeanScape® .....	44
Figure 18 :MQTT configuration .....	45
Figure 19 :MQTT configuration window.....	45
Figure 20: A Screenshot of warning message.....	53
Figure 21: Airmax function should be disabled .....	54
Figure 22: Wireless Configuration - WIFI AP .....	55
Figure 23: WIFI Access Point should be disabled .....	63
Figure 24: MQTT Broker configuration.....	64

## 1. TECHNICAL SUPPORT

---

For general contact, technical support, to report documentation errors and to order manuals, contact **Beanair Technical Support Center** (BTSC) at:

[tech-support@Beanair.com](mailto:tech-support@Beanair.com)

For detailed information about where you can buy the Beanair equipment/software or for recommendations on accessories and components visit:

[www.Beanair.com](http://www.Beanair.com)

To register for product news and announcements or for product questions contact Beanair's Technical Support Center (BTSC).




Our aim is to make this user manual as helpful as possible. Keep us informed of your comments and suggestions for improvements.

Beanair appreciates feedback from the users of our information.



## 2. VISUAL SYMBOLS DEFINITION

---

<i>Symbols</i>	<i>Definition</i>
	<i><u>Caution or Warning</u> – Alerts the user with important information about Beanair wireless sensor networks (WSN), if this information is not followed, the equipment /software may fail or malfunction.</i>
	<i><u>Danger</u> – This information <b>MUST</b> be followed if not you may damage the equipment permanently or bodily injury may occur.</i>
	<i><u>Tip or Information</u> – Provides advice and suggestions that may be useful when installing Beanair Wireless Sensor Networks.</i>




### 3. ACRONYMS AND ABBREVIATIONS

---

<i>AES</i>	Advanced Encryption Standard
<i>CCA</i>	Clear Channel Assessment
<i>CSMA/CA</i>	Carrier Sense Multiple Access/Collision Avoidance
<i>GTS</i>	Guaranteed Time-Slot
<i>Ksps</i>	Kilo samples per second
<i>LLC</i>	Logical Link Control
<i>LQI</i>	Link quality indicator
<i>LDCDA</i>	Low duty cycle data acquisition
<i>MAC</i>	Media Access Control
<i>PAN</i>	Personal Area Network
<i>PER</i>	Packet error rate
<i>RF</i>	Radio Frequency
<i>SD</i>	Secure Digital
<i>WSN</i>	Wireless sensor Network

#### 4. VISUAL SYMBOLS DEFINITION

---

<i>Symbols</i>	<i>Definition</i>
	<p><i><u>Caution or Warning</u> – Alerts the user with important information about BeanAir wireless sensor networks (WSN), if this information is not followed, the equipment /software may fail or malfunction.</i></p>
	<p><i><u>Danger</u> – This information <b>MUST</b> be followed if not you may damage the equipment permanently or bodily injury may occur.</i></p>
	<p><i><u>Tip or Information</u> – Provides advice and suggestions that may be useful when installing BeanAir Wireless Sensor Networks.</i></p>

## 5. ACRONYMS AND ABBREVIATIONS

---

<b>AES</b>	Advanced Encryption Standard
<b>CCA</b>	Clear Channel Assessment
<b>CSMA/CA</b>	Carrier Sense Multiple Access/Collision Avoidance
<b>kSps</b>	Kilo samples per second
<b>LDCDA</b>	Low duty cycle data acquisition
<b>LLC</b>	Logical Link Control
<b>LQI</b>	Link quality indicator
<b>MAC</b>	Media Access Control
<b>NTP</b>	Net Time Protocol
<b>PAN</b>	Personal Area Network
<b>PER</b>	Packet error rate
<b>POE</b>	Power Over Ethernet
<b>RF</b>	Radio Frequency
<b>UPS</b>	Uninterruptible power supply
<b>USB OTG</b>	USB On The Go
<b>WDAQ</b>	Wireless DAQ
<b>WSN</b>	Wireless Sensor Networks

## 6. DOCUMENT ORGANISATION

---

WiLow IoT Gateway product description

- Details the IoT Gateway® product

IoT Gateway® installation guidelines

- Details the installation guidelines of the IoT Gateway®

IoT Gateway® supervision from the Beanscape®

- Details IoT Gateway® supervision from the BeanScape®

## 7. WILOW® IOT GATEWAY PRODUCT PRESENTATION

---



- ✓ *It is highly recommended to read all the user manual related to Beanair software & equipment (BeanScape® Wilow® and BeanDevice® WiLow®) before getting start your IoT Gateway®.*
- ✓ *Use only accessories supplied by Beanair (batteries, power supply unit, and antenna). Use of other materials may damage the IoT Gateway®;*
- ✓ *Only Beanair is qualified to make changes on the IoT Gateway®;*
- ✓ *Don't try to remove the adhesive label on the product; it contains important information such as the MAC address or sensor measurement range*

### 7.1 PRODUCT OVERVIEW

---

Wilow® IOT Gateway along with **BeanScape® RA** will provide you a ready to use one packaged solution for remote access monitoring using BeanDevice Wilow.

Communication between Wilow® IOT Gateway and Real time office monitoring site (using BeanScape® Wilow® RA) will be supported with 3G/4G channel.

In order to assure a continuous monitoring without interruption caused by network provider, it is recommended to use mobile broadband package or M2M sim card rather than using unlimited data plans which are available for smartphones (this is because providers monitor usage of unlimited plans and if they are being used in devices other than smartphone they will restrict access)

Data transmission is managed using MQTT lightweight protocol with the Wilow® IoT Gateway hosting an embedded MQTT broker.

Wilow® IoT Gateway is hosting an embedded MQTT Broker, and enables a remote access to the BeanScape® Wilow® RA.

Wilow IOT Gateway is available in three versions:

- **WILOW-IOT-GATEWAY-4G-MPWR**, Mains Power supply
- **WILOW-IOT-GATEWAY-4G-WDS-MPWPR**, Mains power supply, WDS function
- **WILOW-IOT-GATEWAY-4G-SOLAR**, Solar Power Supply WILOW-IOT-GATEWAY-4G-SOLAR, with Solar Power Supply

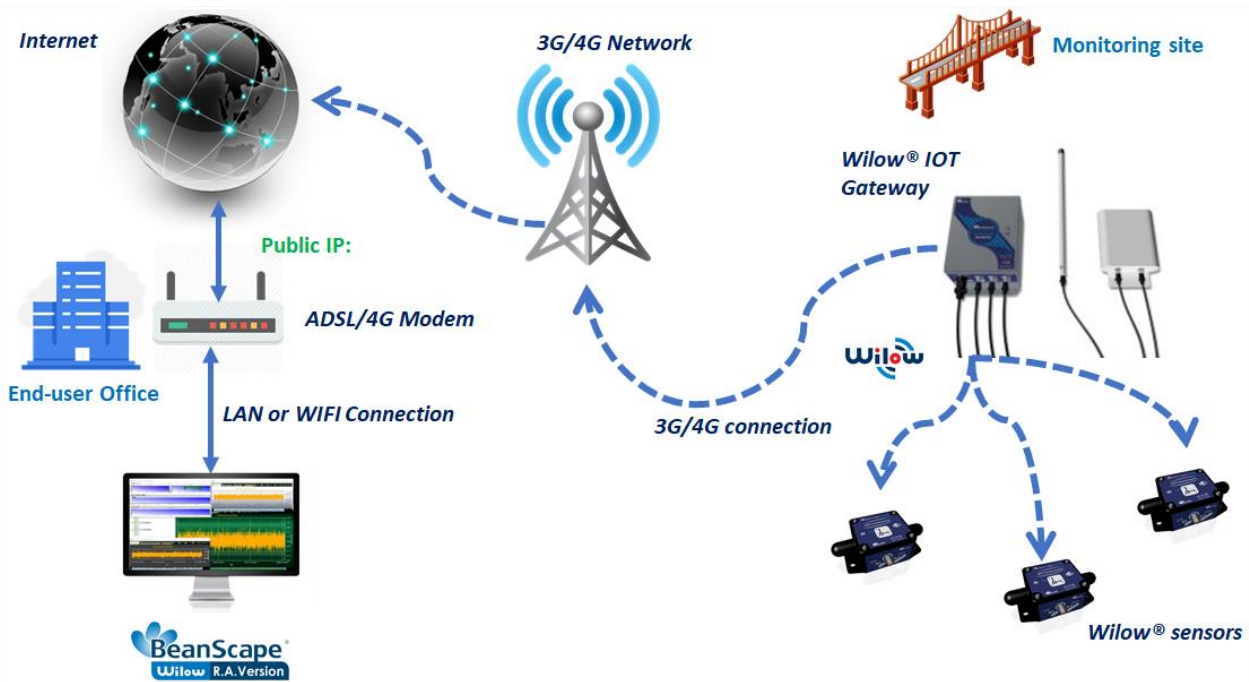


Figure 1: Remote access to Monitoring site

## 7.2 OUTBOXING YOUR WILLOW® IOT GATEWAY



Figure 2: Outboxing your Wilow IOT Gateway

### 7.3 ACCESSORIES DESCRIPTION

In addition to the WiLow® IoT gateway you will find inside the packet a list of accessories:

	Included accessories
4G Antenna	1 x 4G Antenna 12dBi - with pole mounting <b>Ref: WL-4G-HG-ANT-12DBI</b>
WIFI Antenna	1 x High Gain Wifi Antenna 9dBi - with pole mounting kit <b>Ref: HG-OMNI-OUT-7DBI</b>
External cable for WIFI Antenna	1 x N-Type cable, Cable Length: 1 meter <b>Ref: CBL-ANT-1M</b>
External cable for LTE Antenna	2 x N-Type cable, Cable Length: 1 meter <b>Ref: CBL-ANT-1M</b>
Waterproof Plug for AC Power Input	1 x Circular Connector Hirschmann CA 3LS, Waterproof IP67 <b>Ref: WL-CA3LS-PLUG</b>

Make sure to use the right connectors to connect your antennas and power supply :



**Figure 3 : Antenna connectors**

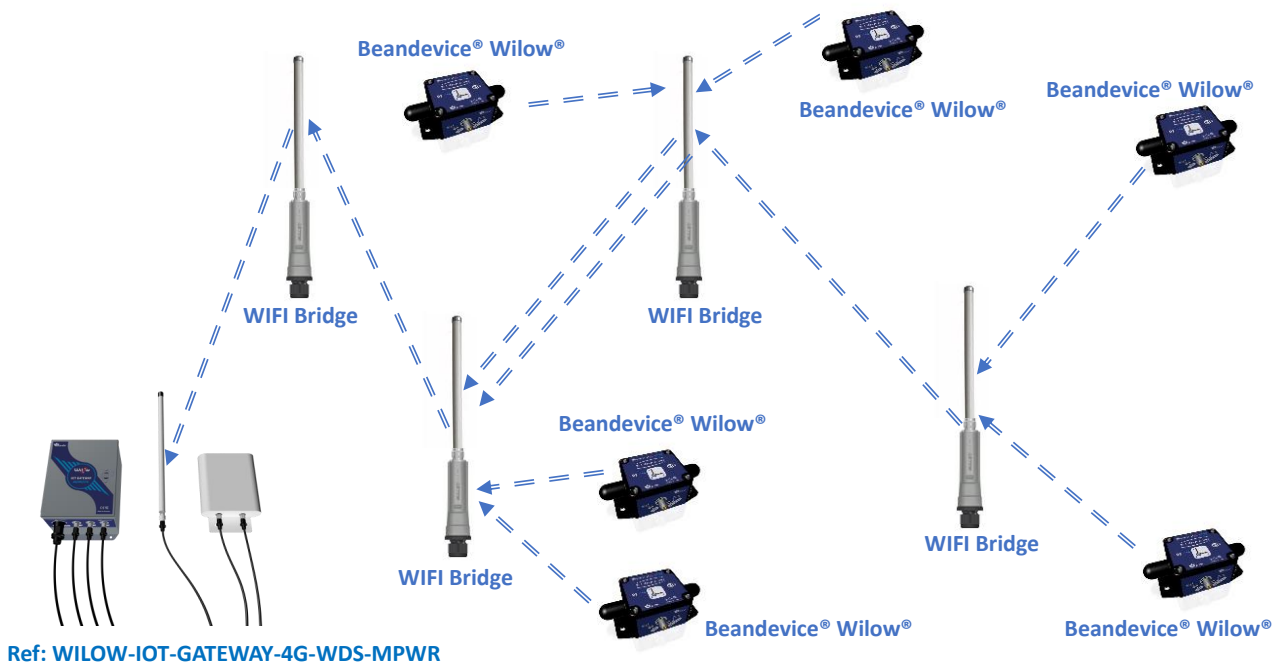


### 7.4 WIRELESS DISTRIBUTION SYSTEM FUNCTION DESCRIPTION

Wireless Distribution system is only available on the reference product: **ILOW-IOT-GATEWAY-4G-WDS-MPWPR**

Beanair is using Ubiquiti Bullet M2 HP Access point with WDS function. While there are some other manufacturers who use WDS that is compatible with Ubiquiti radios, WDS can vary depending on the manufacturer.

WDS is a way to enable layer-2 transparency across radio links. Because it preserves the MAC address from the traffic source, enabling WDS on bridged links is always recommended. WDS is not designed to interoperate between radio vendors, so by using two Ubiquiti radios, users can pass virtually all traffic across wireless links.



**Figure 4: WiFi cluster-tree network architecture with WDS function**

Without WDS function, users can setup a star wifi network without wifi cluster-tree network architecture:

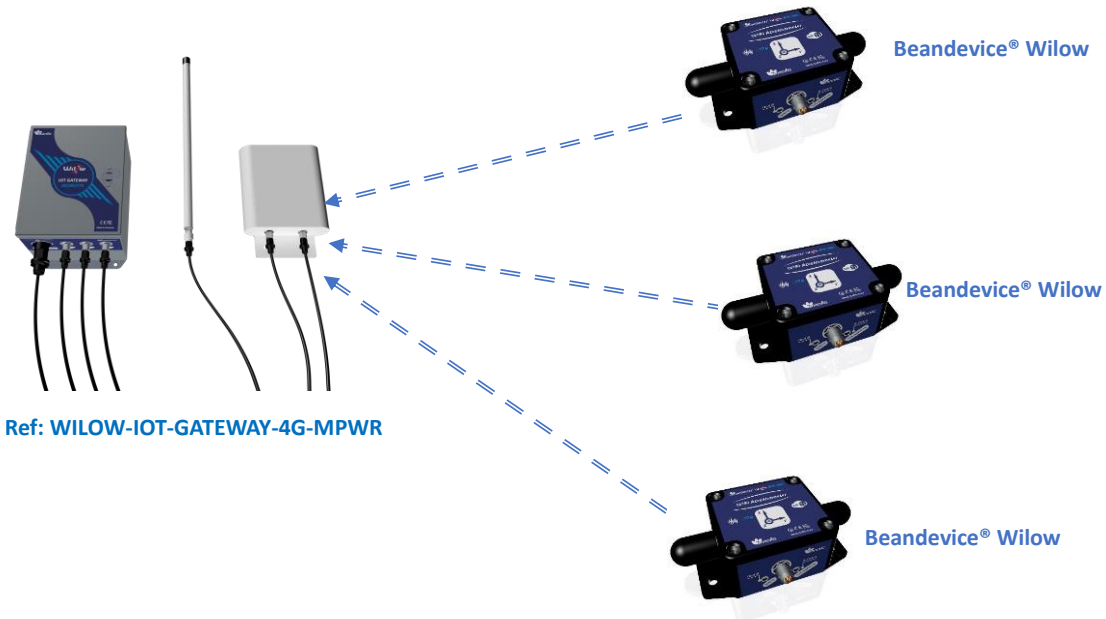


Figure 5: Wifi star network architecture (without WDS function)

## 7.5 TECHNICAL SPECIFICATIONS

### 7.5.1 Product reference

Product reference
WILOW-WIFI-IOT-GATEWAY-4G- <b>OPT1-PWR</b>
<b>OPT1:</b> Option for WDS function - wireless distribution system (not available if you choose Solar Power Supply)
<b>PWR</b> – External Power supply
<b>*MPWR:</b> Mains power supply with UPS Battery (Input: 90 to 264VAC)
<b>*SOLAR</b> - Solar Power supply
<b>Example 1:</b> WILOW-IOT-GATEWAY-4G-UP12, with UPS Battery 12Ah
<b>Example 2:</b> WILOW-IOT-GATEWAY-4G-WDS-UPS12, with WDS option and UPS Battery
<b>Example 3:</b> WILOW-IOT-GATEWAY-4G-SOLAR, with Solar Power Supply

**7.5.2 WIFI Connectivity**

	WIFI Connectivity specifications
Wireless Protocol	IEEE 802.11 b/g
WIFI configuration	Wireless AP, If <b>WDS option is selected</b> : Station and Bridge with WDS (Wireless Distribution System)
Operating frequency	2412-2462 MHz
Sensitivity	-74dBm to -90 dBm
DataRate	6 to 24 Mbps
Output power	If <b>WDS option is selected</b> : 28 dBm If <b>WDS option is not selected</b> : 20dBm
High Gain Ominidirectionnal WIFI Antenna	<b>Frequency range</b> 2400-2500MHz <b>Gain</b> : 9dBi, <b>VSWR</b> < 1.2 <b>Impedance</b> 50 Ohm, Polarization Vertical Beamwidth: Vertical plane 15°, Horizontal plane 360° <b>Dimensions</b> : 540x23 mm, <b>Weight</b> : 0.61 kg <b>Connector</b> : N female, <b>Wind load</b> : (170km/h) 11 N

**7.5.3 3G/4G/LTE Router**

	3G/4G Connectivity specifications
LTE	<ul style="list-style-type: none"> <li>■ LTE FDD: B1/B3/B5/B7/B8/B20</li> <li>■ LTE TDD: B38/B40/B41</li> <li>■ LTE CAT4 up to 70 Mbps DL</li> <li>■ LTE CAT4 up to 50 Mbps UL</li> <li>■ Class 3 (23dBm±2dB) for LTE FDD</li> <li>■ Class 3 (23dBm±2dB) for LTE TDD</li> </ul>
UMTS/DC-HSPA+	<ul style="list-style-type: none"> <li>■ 850/900/2100 MHz</li> <li>■ DC-HSPA+ mode: Max 42Mbps (DL) Max 5.76Mbps (UL)</li> <li>■ UMTS mode: 384 kbps DL, 384 kbps UL</li> <li>■ TD-SCDMA: Max 4.2Mbps (DL) Max 2.2Mbps (UL)</li> <li>■ Power Class 3 (24dBm +1/-3dB) for UMTS bands</li> <li>■ Class 3 (24dBm+1/-3dB) for TD-SCDMA</li> </ul>

GSM/GPRS/EDGE	<ul style="list-style-type: none"> <li>■ 900/1800 MHz</li> <li>■ GPRS/EDGE Multi-slot Class 12</li> <li>■ Power Class E2 (27dBm ±3dB) for GSM 900</li> <li>■ Power Class E2 (26dBm +3/-4dB) for DCS 1800</li> <li>■ Power Class 4 (33dBm ±2dB) for GSM 900</li> <li>■ Power Class 1 (30dBm ±2dB) for DCS 1800</li> </ul>
Omnidirectional 4G Antenna	<p><b>Omnidirectional 4G Antenna</b> (2x2 MIMO)                      Weather-resistant and UV-resistant plastic / PVC enclosure  <b>VSWR</b> &lt; 1.8  <b>Impedance:</b> 50 Ohm  <b>Beam width:</b> 360° Horizontal - 20° Vertical  <b>Gain :</b>                      8dBi @ 800 MHz                      12dBi @ 1800MHz                      12dBi @ 2600MHz  <b>Frequency:</b>                      791-862 MHz (2G, 4G)                      1700 - 2100 MHz (3G, 4G)                      2500 - 2700 (4G)  <b>Connectors:</b> 2 x N female  <b>Mounting Kit:</b> U-clamp for 30-50mm diameter handles</p>

**7.5.4 Environmental and Mechanical**

	Environmental and Mechanical
Casing	Steel enclosure with padlock adapter, Light gray color
Dimensions	25.4 cm x 20.3 cm x 15.24 cm
IP   NEMA Rating	IP66   Nema 6
Weight	9.3 kg
Mounting Process	Screw mounting
Operating Temperature	Battery Charging: -15°C to 50°C Battery Discharging: -20°C to 60°C
Norms & Radio Certifications	<ul style="list-style-type: none"> <li>. CE Labelling Directive R&amp;TTE (Radio) ETSI EN 300 328 (Europe)</li> <li>. FCC Part 15.247 (North America)</li> <li>. IC RS210</li> <li>. ROHS - Directive 2002/95/EC</li> </ul>

7.5.1 2.4GHz High Gain Antenna

9dBi 2.4GHz antenna specifications



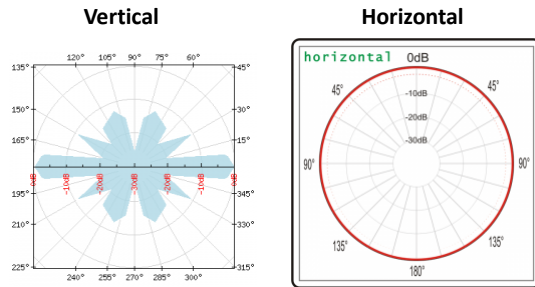
Electrical Parameters

Frequency range	2400-2500MHz
Gain	9dBi
VSWR	< 1.2
Impedance	50 Ohm
Polarization	Vertical
Vertical plane	15°
Horizontal plane	360°
Protection	shorted for DC

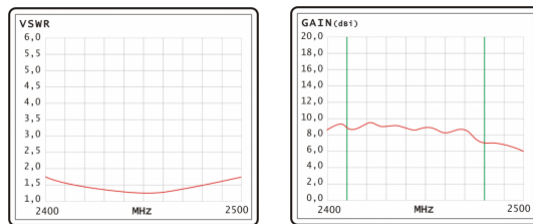
Mechanical Parameters

Dimensions	540x23 mm
Weight	0.61 kg
Connector	N female
Wind load (170km/h)	11 N

Patterns



VSWR and GAIN



Ref: HG-OMNI-OUT-9DBI

Antenna reference: HG-OMNI-OUT-9DBI

7.5.2 Dual LTE Antenna



Figure 6: Dual LTE Antenna with u-clamp mounting kit

The enclosure of this multiband 4G antennas is manufactured from robust, weather-resistant and UV-resistant plastic / PVC. This allows using this 4G antenna for in- and outdoor appliances even under extreme weather conditions.

The antenna is designed for mast/pole or wall handle installation. A mounting kit (u-clamp for 30-50mm diameter handles) is included.

<b>Omnidirectionnal 4G Antenna</b>	Omnidirectional 4G Antenna (2x2 MIMO) Weather-resistant and UV-resistant plastic / PVC enclosure VSWR < 1.8 Impedance: 50 Ohm Beamwidth: 360° Horizontal - 20° Vertical Gain : 8dBi @ 800 MHz 12dBi @ 1800MHz 12dBi @ 2600MHz Frequency: 791-862 MHz (2G, 4G) 1700 - 2100 MHz (3G, 4G) 2500 - 2700 (4G) Connectors: 2 x N female Mounting Kit: U-clamp for 30-50mm diameter handles
------------------------------------	---

### 7.5.3 AC/DC power adapter with battery charger (UPS function)

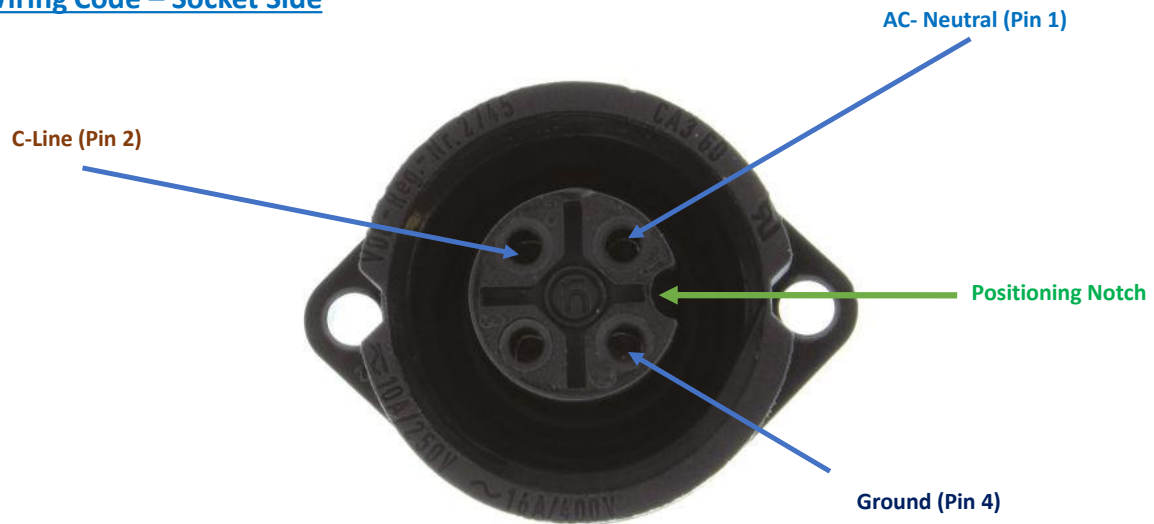
#### 7.5.3.1 Specifications

	AC power supply with UPS battery (-MPWR option is selected)
Battery	Valve Regulated Lead-Acid (VRLA) Capacity 12Ah
Battery protection	Overvoltage/Overload/Short circuit/Battery low/Battery reverse polarity
AC Voltage Range (Input)	90 to 264VAC
AC Range (Input)	0.75A/115VAC 0.5A/230VAC
Frequency Range	47 ~ 63Hz
Inrush current	Cold Start 20A/115VAC, 40A/230VAC
Safety and EMC	Safety standards: UL60950-1, TUV EN60950-1 approved Withstand Voltage: I/P-O/P:3KVAC I/P-FG:2KVAC O/P-FG:0.5KVAC Isolation Resistance TANCE: I/P-O/P, I/P-FG, O/P-FG:100M Ohms / 500VDC / 25°C/ 70% RH EMC emission: Compliance to EN55032 (CISPR32) Class B, EN61000-3-2,-3 EMC immunity: Compliance to EN61000-4-2,3,4,5,6,8,11, EN55024, light industry level, criteria A
Socket for AC power supply	Industrial and Waterproof Socket Circular Socket CA 3 GD - Hirschmann Rated Voltage: 400VA Rated Current:16A

### 7.5.3.2 Mains power supply (Hardware version before 15.05.2019)

The previous hardware version comes with a Female Socket and a Male Plug.:

#### Wiring Code – Socket Side



**Figure 7 : Mains power supply – wiring code**



**Figure 8: Waterproof Plug**

Plug Ref: 934124100, provider: Hirschmann

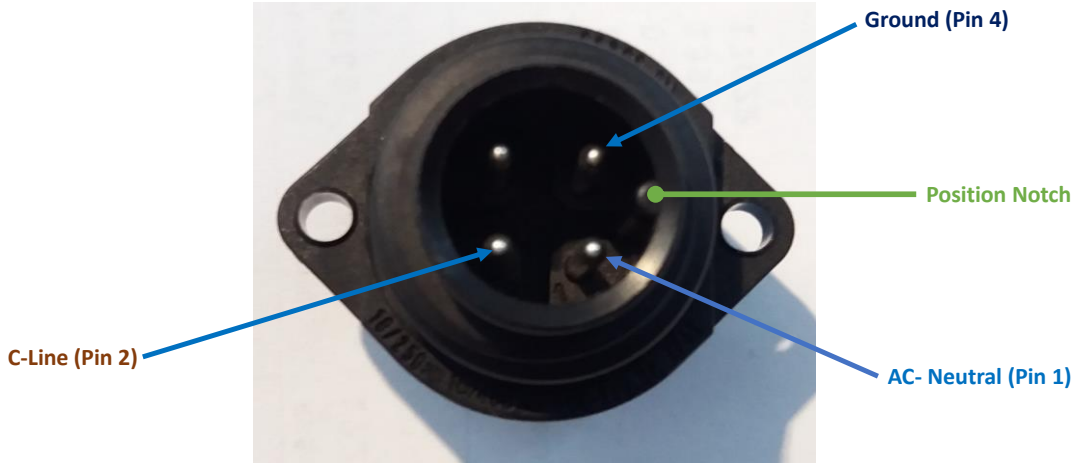


7.5.3.3 Mains power supply (Hardware version after 15.05.2019)

The new hardware version comes with a Male Socket and a Female Plug:

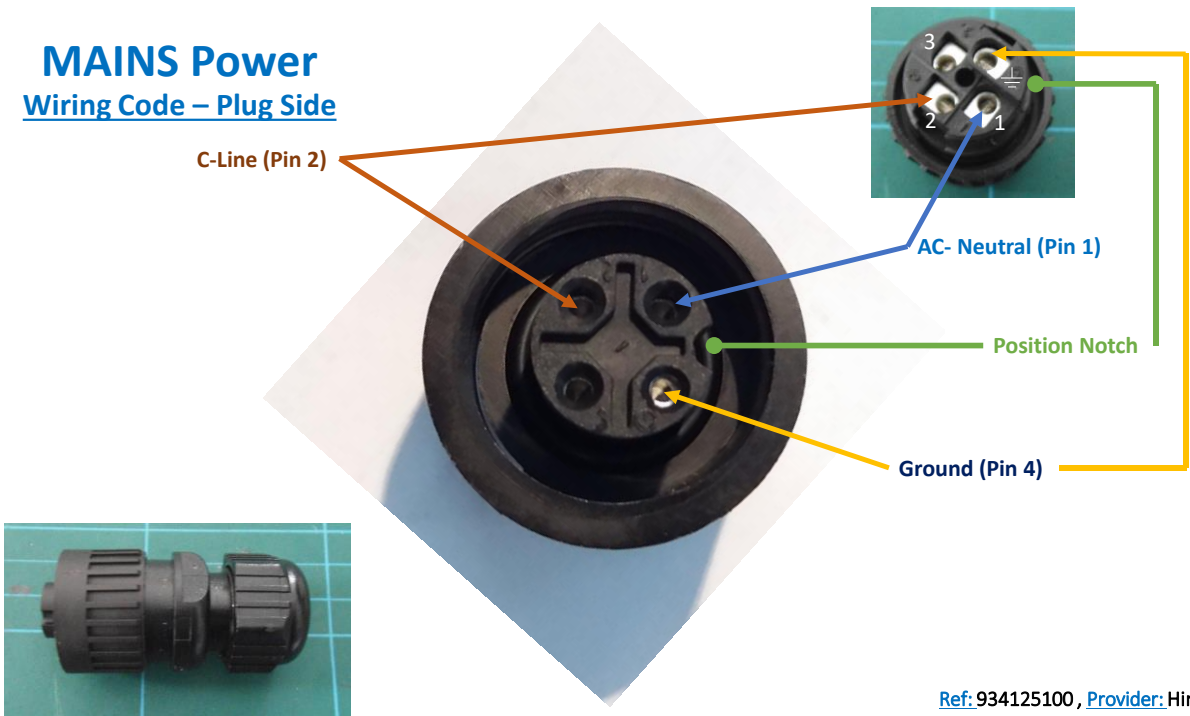
### MAINS Power

#### Wiring Code – Socket Side



### MAINS Power

#### Wiring Code – Plug Side



Ref: 934125100 , Provider: Hirschmann

**7.5.4 Solar power supply with UPS battery**

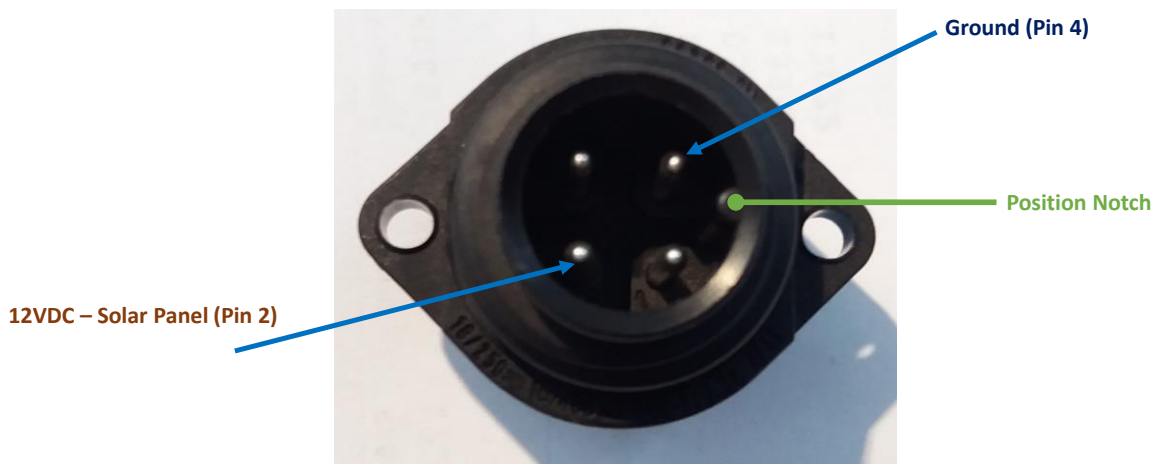
7.5.4.1 Specifications

	Solar Panel power supply with UPS Battery (-SOLAR option is selected)
Battery	Valve Regulated Lead-Acid (VRLA) Capacity 12Ah
Solar panel technology	Polycrystalline 100W, anodized aluminum frame. Surface protection with ESG solarglass. Dimensions (LxWxH): 1005 x 670 x 35mm
Solar charging controller	Maximum Input current: 10A Power consumption < 2.5mA , Led switch on Nominal voltage :12VDC Led displays: battery full and charging
Socket for Solar Panel Connection	Industrial and Waterproof Socket Circular Socket CA 3 GD - Hirschmann Rated Voltage: 400VA Rated Current: 16A

7.5.4.2 Wiring code ( Hardware version after 15.06.2019)

**SOLAR Power**

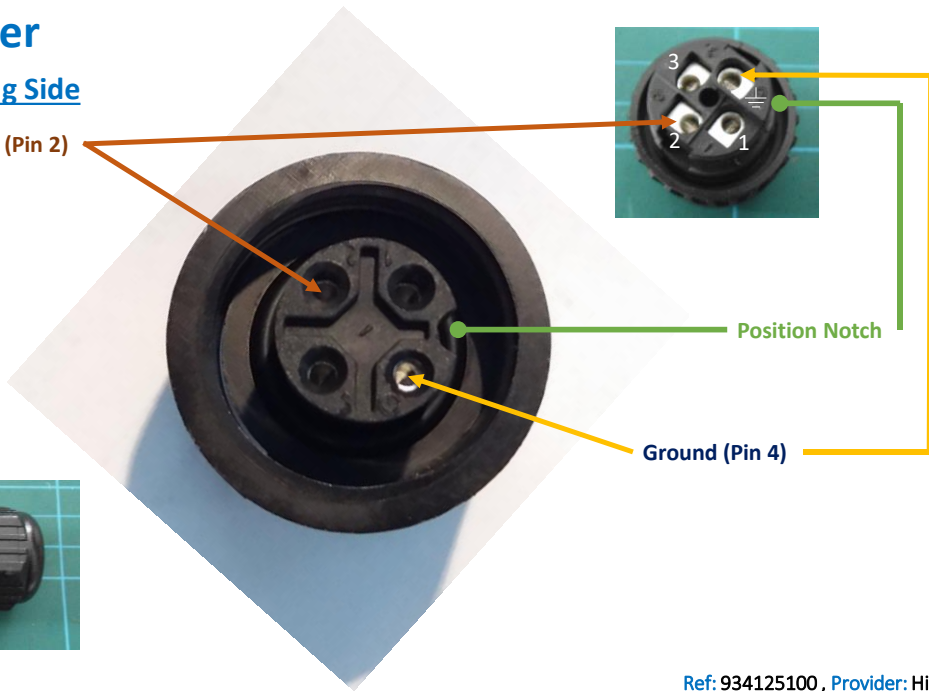
Wiring Code – Socket Side



## SOLAR Power

### Wiring Code – Plug Side

12VDC – Solar Panel (Pin 2)



Ref: 934125100, Provider: Hirschmann

### 7.5.5 Included accessories

	Included accessories
4G Antenna	1 x 4G Antenna 12dBi - with pole mounting Ref: <a href="#">HG-4G-OMNI-ANT-12DBI</a>
WIFI Antenna	1 x High Gain Wi-Fi Antenna 9dBi - with pole mounting kit Ref: <a href="#">HG-OMNI-OUT-7DBI</a>
External cable for WIFI Antenna	1 x N-Type cable, Cable Length: 1 meter Ref: <a href="#">CBL-ANT-1M</a>
External cable for LTE Antenna	2 x N-Type cable, Cable Length: 1 meter Ref: <a href="#">CBL-ANT-1M</a>
Waterproof Plug for AC Power Input	1 x Circular Connector Hirschmann CA 3LS, Waterproof IP67 Ref: <a href="#">PWR-CA3LS-PLUG</a>

## 8. INSTALLATION GUIDELINE

---

### 8.1 HOW TO MOUNT THE WILLOW® IOT GATEWAY

---

Your Wilow® IOT Gateway should be mounted on the vertical position with the antenna socket pointing to the ground.

Use a padlock to protect your Wilow® IOT Gateway casing against vandalism.



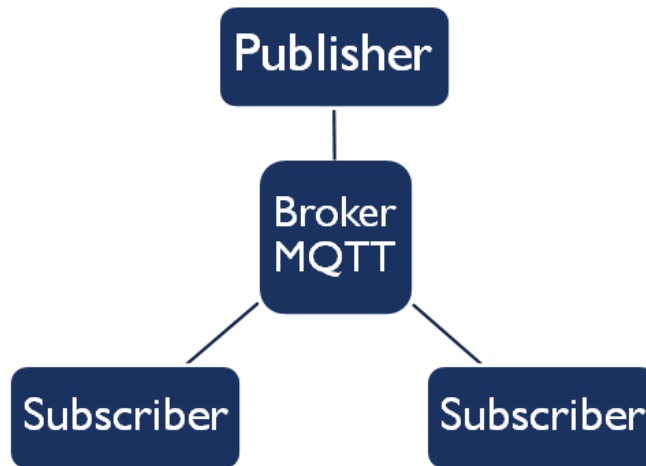
Use a Padlock to secure your Wilow® IOT Gateway

## 9. HOW TO SETUP A REMOTE ACCESS

---

### 9.1 MQTT ARCHITECTURE

---



*Figure 9 :MQTT architecture*

MQTT is based on publish & subscribe architecture. The **BeanDevice® Wilow®** will publish all the data through MQTT broker hosted on the Wilow® IOT Gateway. Thanks to the **BeanScope® RA** user can subscribe to any publishing BeanDevice® Wilow® to receive and collect real time data measurement from the devices also to configure the BeanDevice® Wilow®



*Figure 10: Wilow® IOT Gateway enclosure*

After opening the Wilow® IoT Gateway metallic enclosure, gently untighten the 3G/4G antenna connectors (displayed below) and use a screwdriver to open the router lid to insert your sim card.

## 9.2 WHICH SIM CARD TO USE?

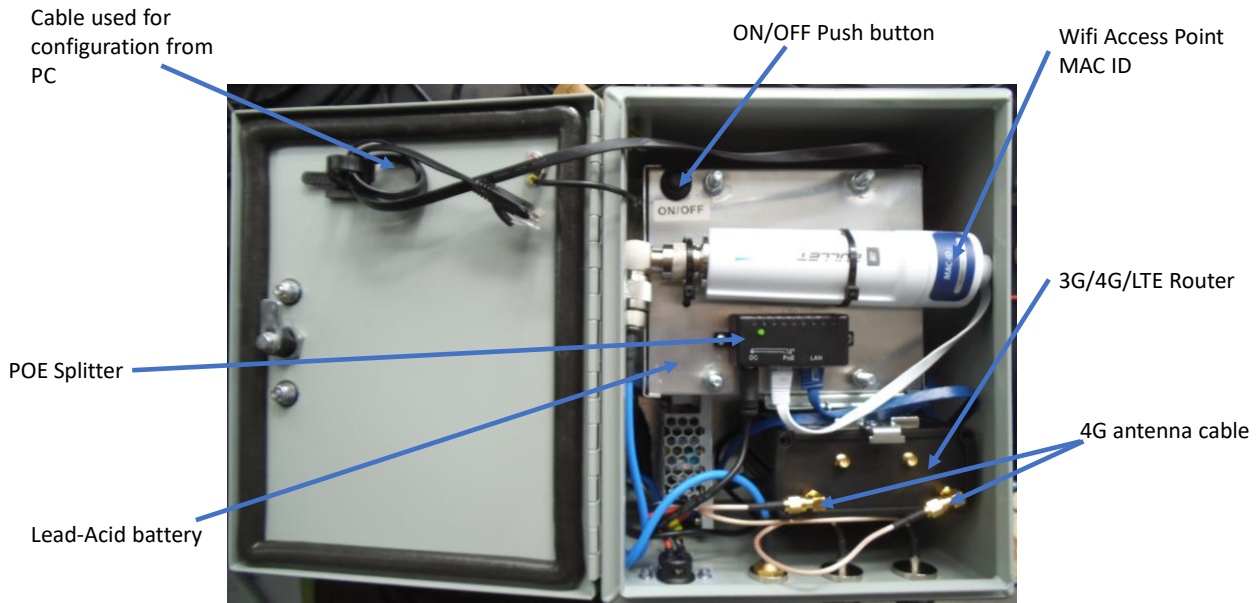
---

If you need to setup a remote access to the Wilow® IOT Gateway then please bear in mind that the 4G Data SIM cards available directly from EE, Vodafone, O2 and 3Mobile (including the MVNO partners of these primary networks eg. Tesco, Virgin, Network ID, BT etc.) Will only provide you connection with a PRIVATE IP Address so you will not be able to remotely connect to the router. This also means that you will not be able to use DYNDNS because the service provider has only given the 4G connection a PRIVATE IP address on their network.

For remote access and monitoring applications where you need to connect to the router and to your devices on the LAN we recommend a 4G Data SIM Card with fixed PUBLIC IP. A Fixed IP SIM card is a data SIM with fixed or static IP address. This provides a secure and reliable 2-way connection between you and your device from any location

- For UK customers: [Click on the following weblink](#)
- For German customers: [Click on the following weblink](#)
- Europe and North America : [Click on the following weblink](#)

### 9.3 HARDWARE DESCRIPTION AND SYSTEM CONFIGURATION



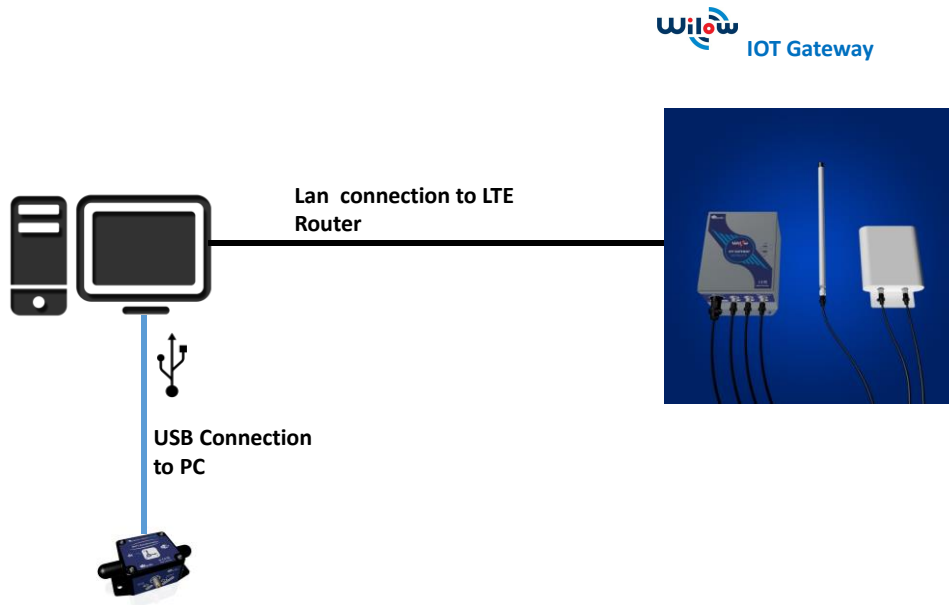
*Figure 11 :Wilow® IoT Gateway (Ref: WILLOW-IOT-GATEWAY-4G-WDS-MPWR)*

### 9.4 SYSTEM CONFIGURATION

Use the Ethernet cable inside the enclosure to connect to your PC running **BeanScape® Wilow® RA**, at the same time connecting your **BeanDevice® Wilow®** with the same PC using the provided USB cable.

Both LTE Router and WIFI Access point are tested and configured at our factory, therefore you don't need to spend time to configure all the different Network settings for a remote access.

However, if you decide to restore the factory settings, **Appendix 1** and **Appendix 2** describe how to re-configure these two devices.



**Figure 12 :Network configuration**

## 9.5 LTE ROUTER CONFIGURATION

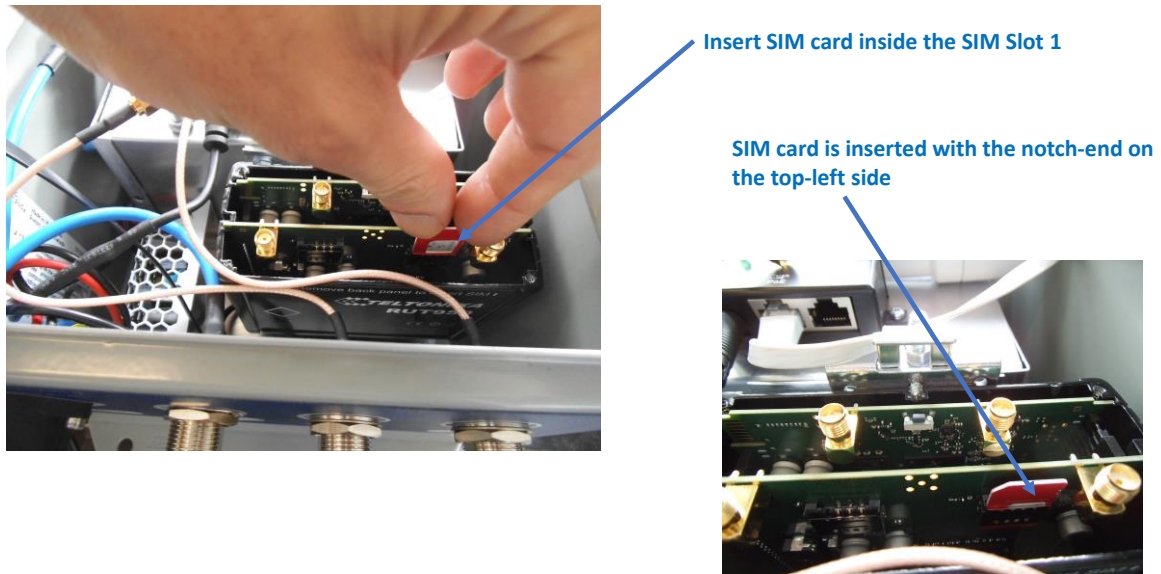
### 9.5.1 Pre-configured settings

<b>IP address</b>	192.168.1.243
<b>Login (lower case)</b>	admin
<b>Password (lower case)</b>	<b>Beanair2019</b>
<b>WIFI Access point</b>	<b>Disabled</b> , if you are using Wifi AP with WDS Function <b>Enabled</b> , if you are using internal Wifi AP (no WDS function)
<b>MQTT broker</b>	Enabled
<b>MQTT broker port</b>	1883
<b>Remote access</b>	Enabled

### 9.5.2 SIM Card insertion

Insert the SIM card provided by your ISP (Internet Service provider). The Correct SIM card orientation is shown on the following picture:





***Figure 13 :Inserting sim card***

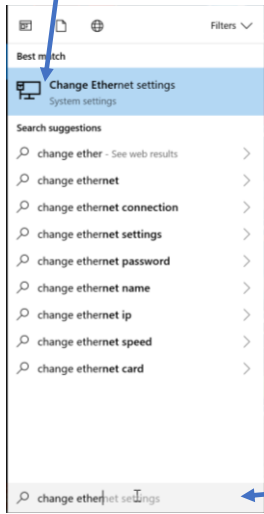
### 9.5.3 Logging to your router

Wilow® IOT Gateway comes with a private embedded MQTT broker enabling all the BeanDevice® on the LAN to use to stream and publish all the measurements to the internet .in order to use that we have to make sure it is well configured as follows:

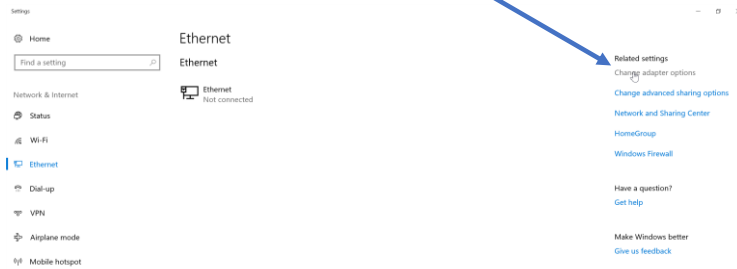
Use browser (Chrome, safari, or Firefox. Avoid internet explorer) to get access to the Gateway interface.

- use this default IP Address: 192.168.1.243
- **Username:** admin
- **Password:** Beanair2019

**2. Select Ethernet Settings**

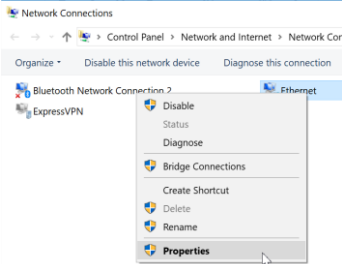


**3. A new window pop-up's , select Change adapter options**

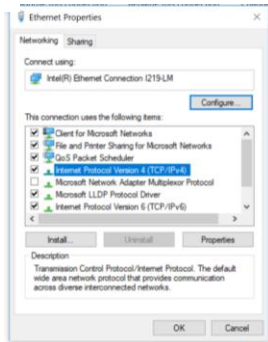


**1. Use the search tool, type in Change Ethernet Settings**

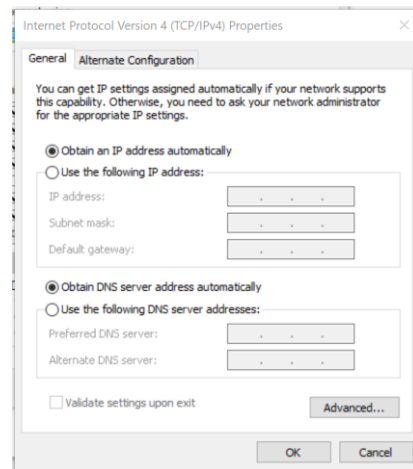
**4. right click on your Ethernet device which is connected to your 4G Router**



**5. Click on Properties, then select Internet Protocol Version 4 (TCP/IPv4) then click on Properties**

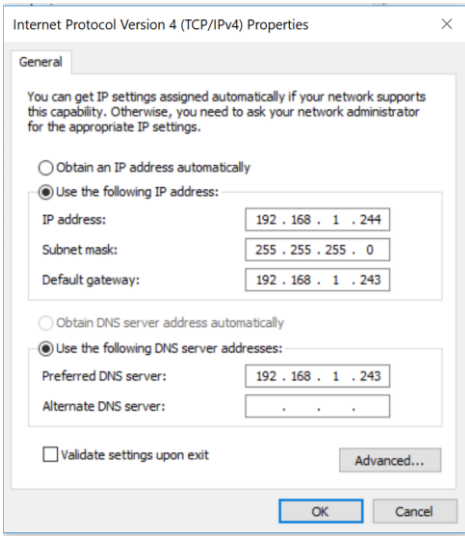


**6. By default DHCP is enabled on your PC, i.e. IP address can be automatically allocated**

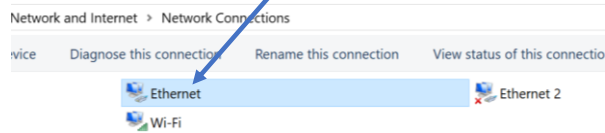


**7. Choose Manual IP configuration**

- First select an IP address. The 4G router is configured with the IP Address **192.168.1.243** . You can enter an IP in the form of 192.168.1.XXX, where XXX is a number in the range of **2-254**.
- Avoid to use the same IP address than your 4G Router which is **192.168.1.243**
- Enter 255.255.255.0 for your subnet mask
- The default gateway must come with the same IP address that your 4G Router **192.168.1.243**
- Finally enter primary DNS server IP , the same than your 4G Router IP **192.168.1.1**
- Click on OK validate your configuration



Your Ethernet Icon is displayed connected



**9.5.4 SIM card configuration**

For configuring your 4G/LTE Router go on Network then Click on Mobile

The connection type used when connecting to a network. It can either be PPP or QMI. PPP is considerably slower than QMI. **QMI is highly recommended**

**Access Point Name (APN)** is a configurable network identifier used by a mobile device when connecting to a GSM carrier.

Fill out this field only if your SIM card has PIN enabled

Fill out this field only if your SIM card has PIN enabled

Leave this field empty

No need to fill out this field

Leave this field empty

If enabled this function prevents the device from establishing mobile data connection while not in home network.

This box is checked by default

**Mobile Data On Demand**Enable No data timeout (sec) **Force LTE network**Enable Reregister Interval (sec) 

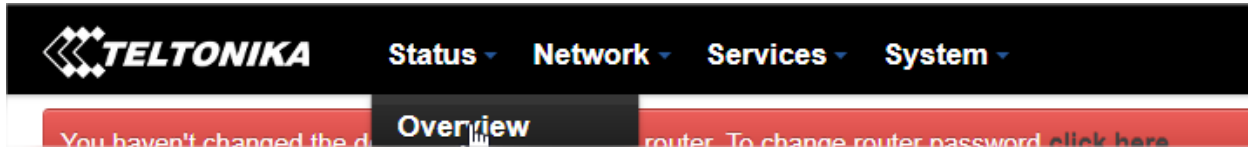
You can get the APN ID from your telecom operator provider



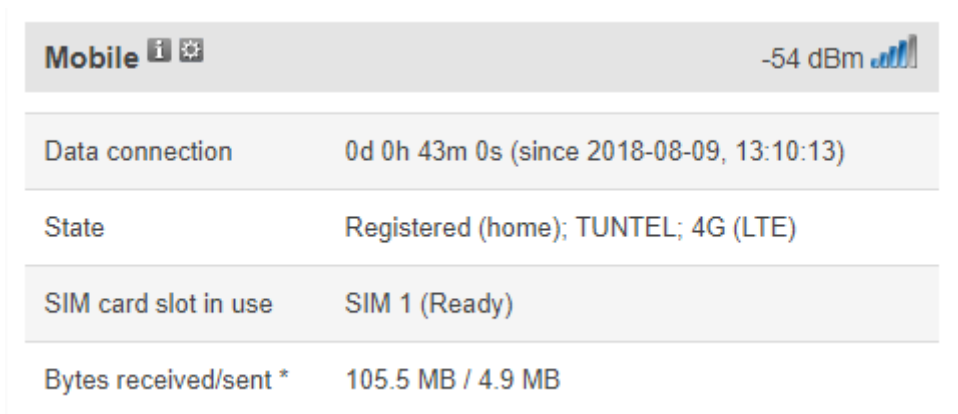
If an invalid PIN number was entered (i.e. the entered PIN does not match the one that was used to protect the SIM card), your SIM card will get blocked. To avoid such mishaps, it is highly advised to use an unprotected SIM. If you happen to insert a protected SIM and the PIN number is incorrect, your card won't get blocked immediately, although after a couple of reboots OR configuration saves it will.

### 9.5.5 Checking your Mobile Status

You can check on your Mobile status by clicking on the Status tab and then Overview.



You can view your data connection duration and quality of connectivity, whether you are registered and using 4G or not .you will also monitor the received and sent bytes.



**Figure 14 : Mobile status**

### 9.5.6 WiFi access point with WDS function, pre-configured settings (Ref: WILOW-IOT-GATEWAY-4G-WDS-MPWR)

Wilow® IOT Gateway (Ref: WILOW-IOT-GATEWAY-4G-WDS-MPWR) integrates a powerful WiFi Access point with WDS function from Ubiquiti (Bullet M2 HP). This access point is already configured with the following settings:

<b>AP IP address</b>	192.168.1.20
<b>AP Webserver Login</b>	ubnt
<b>AP Webserver PW</b>	Beanair2019
<b>WIFI SSID</b>	Beanair
<b>WIFI Password</b>	Beanair2019
<b>Encryption</b>	WPA2-AES
<b>WIFI RF Channel</b>	2437
<b>AirMax function</b>	disabled



If you need to change the WIFI AP with WDS function settings or if you need to reconfigure it after factory settings restoration go to the [Appendix 1](#)

### 9.5.1 WiFi access point pre-configured settings (Ref: WILOW-IOT-GATEWAY-4G -MPWR and (Ref: WILOW-IOT-GATEWAY-4G-SOLAR)

The LTE Router (RUT950) integrates a WIFI Access Point. This access point is already configured with the following settings:

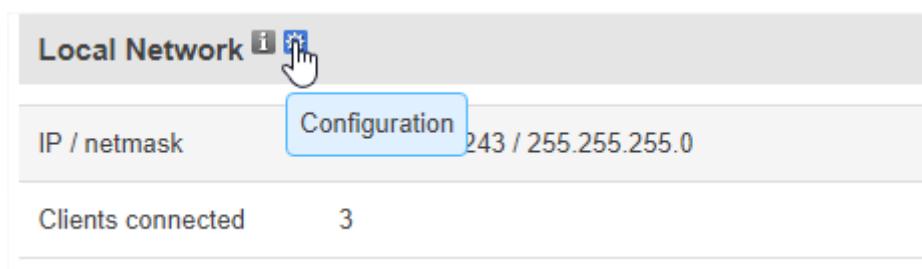
<b>WIFI SSID</b>	Beanair
<b>WIFI Password</b>	Beanair2019
<b>Encryption</b>	WPA2-PSK, Cipher: Auto
<b>WIFI RF Channel</b>	2437 (Channel 6)



If you need to change the WIFI AP settings or if you need to reconfigure it after factory settings restoration go to the [Appendix 2](#)

### 9.5.1 LAN configuration

LAN IP address should be 192.168.243 by default and if this is not the case for whatever reason, you will need to set it back to 192.168.1.243 in the configuration panel you can find in the overview page



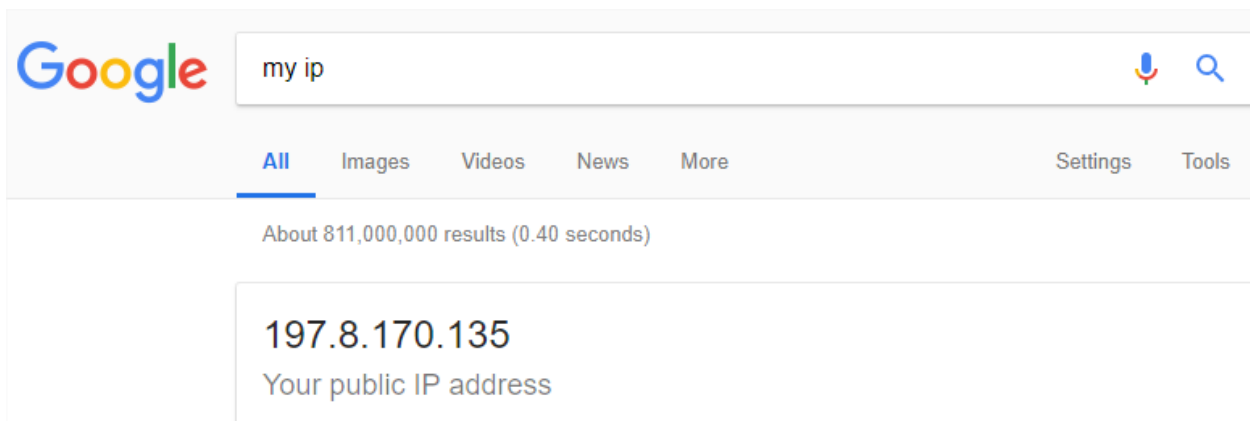
The screenshot shows the Teltonika web interface with the following structure:

- Header:** TELTONIKA logo, navigation menu (Status, Network, Services, System), and Logout button.
- Section:** LAN
- Configuration Panel:**
  - General Setup:** IP address (192.168.1.243), IP netmask (255.255.255.0), IP broadcast.
  - DHCP Server:**
    - DHCP: Enable
    - Start: 100
    - Limit: 143
    - Lease time: 12 Hours
    - Start IP address: 192.168.1.100
    - End IP address: 192.168.1.242

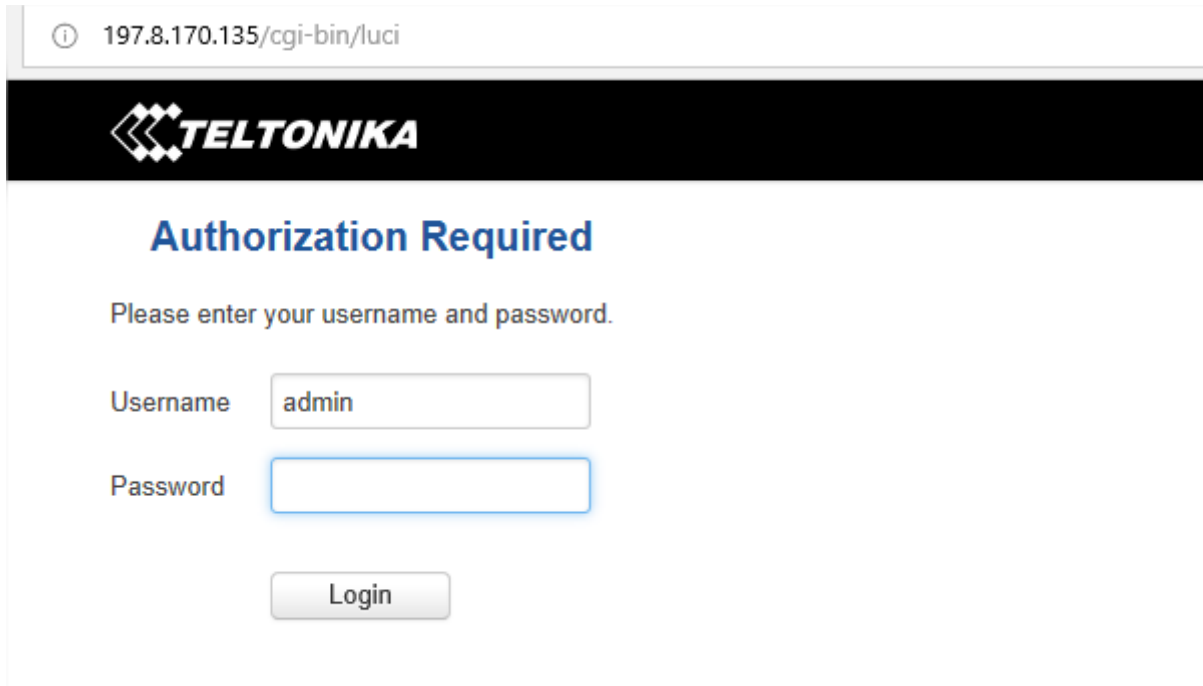
**Figure 15 :LAN configuration**

**9.5.2 Public IP address and Dynamic DNS**

It is recommended that you write down your PUBLIC IP address as we will use it to access this IoT Gateway from monitoring office. To discover your Public IP just type [my IP](#) in Google while connecting only using your Gateway data (make sure the Ethernet LAN cable is not connected)



To make sure your Public access is enabled you should try to access your IoT gateway from different network using that same IP address, you should see this.



197.8.170.135/cgi-bin/luci

**TELTONIKA**

### Authorization Required

Please enter your username and password.

Username

Password

Login



***Make sure to have a sim card with fixed public IP address, so if the router reboots, it doesn't change (you have to ask your provider for that)***

Still, if you don't have Fixed public IP address you can go for a dynamic DNS (free or paid as service) to:

- Have DNS for your IoT gateway (so instead of **197.8.170.135** you can have <http://www.muncheninstructsite.publicvm.com>)
- Keeps access to the IoT Gateway® available even with the Public IP is frequently changing.

To enable this method, you should have an account on one of Dynamic DNS providers (For example: DynDNS.net, noip.com, dnsexit.com,...etc.)



**Most of the time free DDNS service is only free for a period of time (For example 1 month).**

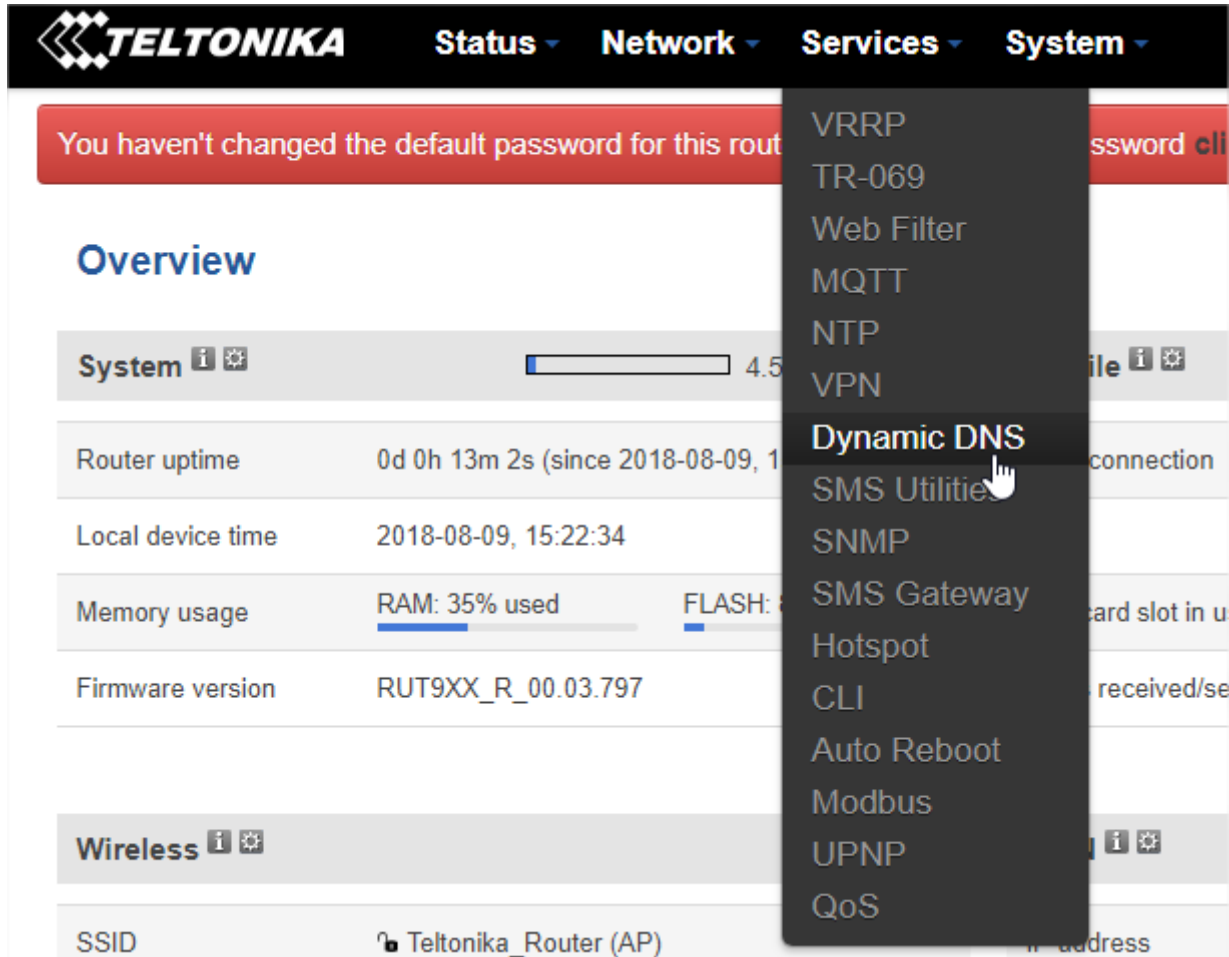
After signing up and creating a DDNS (for example: beanairtech.publicvm.com), this should be linked to our Public IP address **197.8.170.135**.



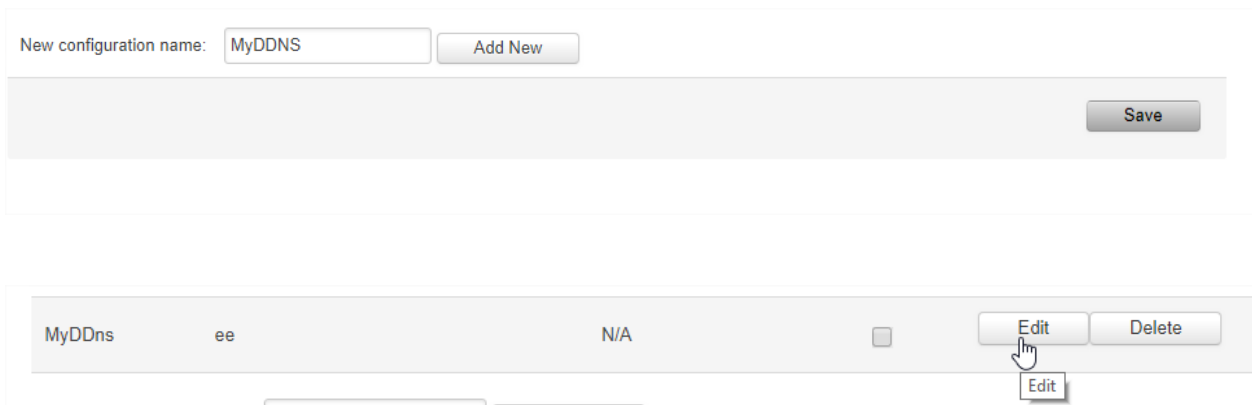
Host Records (A & AAAA)					<a href="#">Add Host</a>	<a href="#">? help</a>
Host	IP Address (IPv4 / IPv6)	FO	TTL ( hr : min )	Action		
beanairtech.publicvm.com.	197.8.170.135	off	00:02	<a href="#">Edit</a>	<a href="#">Delete</a>	

Next, in the IoT Gateway® side the DDNS client should be configured with the same account settings.

Go to Services tab → Dynamic DNS



Create a new DDNS configuration and then edit to access configuration page.



### Dynamic DNS

Dynamic DNS allows you to reach your router using a fixed hostname while having a dynamically changing IP address.

**DDNS**

Enable  ← Check to enable Dynamic DNS

Use HTTPS

Status 2018-08-09, 15:34:10 ← Time of last IP update

Service dnsexit.com ← DDNS Service used(dnsexit)

Hostname www.beanairtech.publicvm ← Hostname

User name beanairtech ← User name & Password

Password \*\*\*\*\* ← User name & Password

IP source Custom ← Switch to custom  
Private or custom IP source setting, will disable DNS rebinding protection

Network WAN ← Switch to WAN


IP renew interval (min) 10 ← Use default

Force IP renew (min) 472 ← Use default

[Back to Overview](#) [Save](#)

After saving, we can access our network using our DNS

beanairtech.publicvm.com/cgi-bin/luci



### Authorization Required

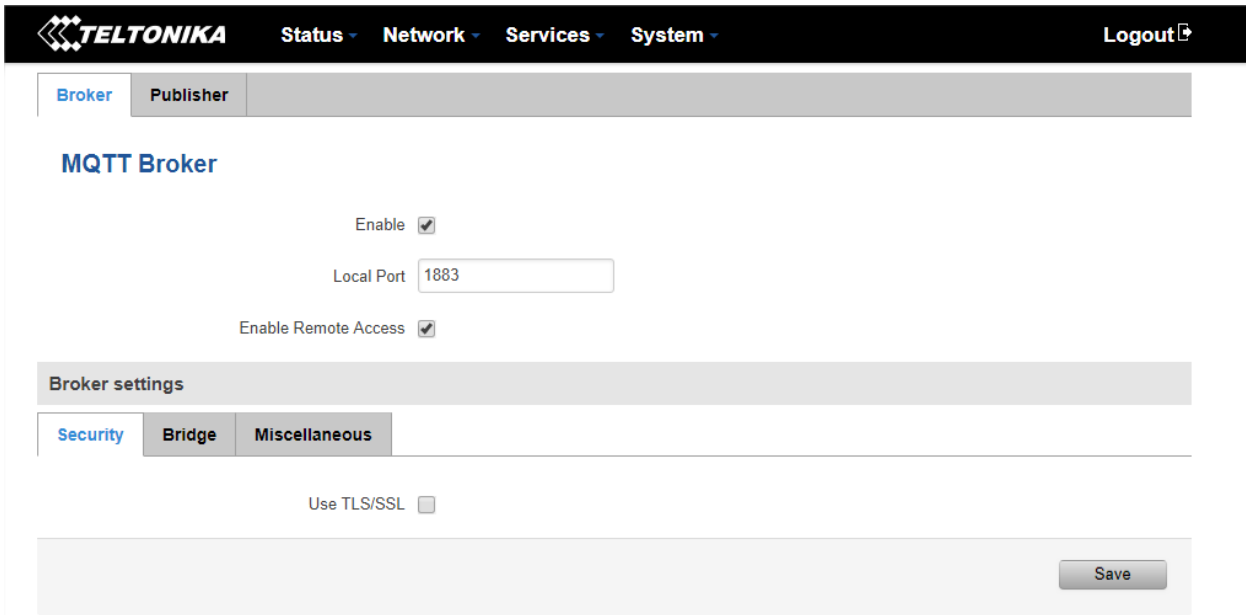
Please enter your username and password.

Username

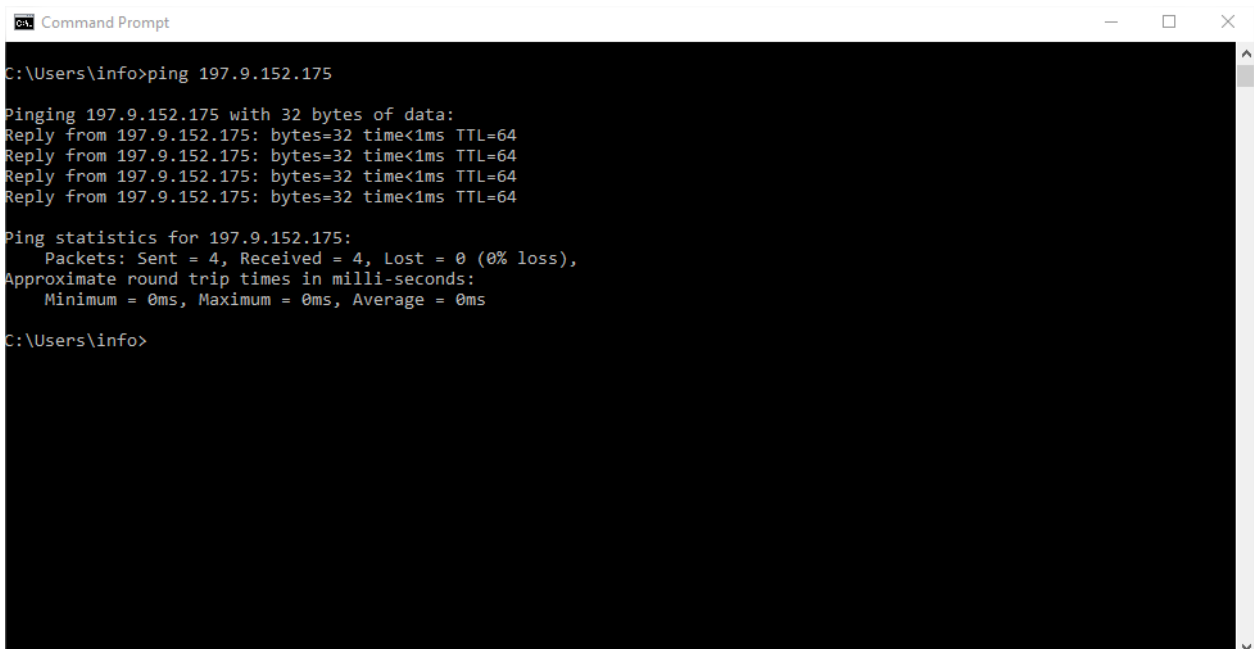
Password

[Login](#)

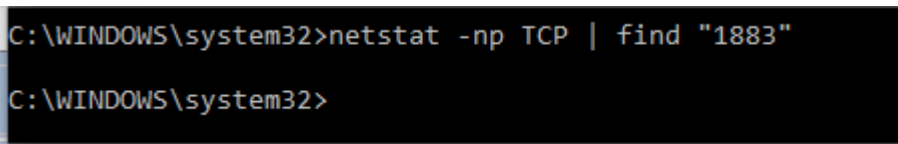
### 9.5.3 MQTT Broker Configuration



To make sure the MQTT broker in the Wilow® IOT Gateway® is working fine, try to ping to it (using its Public IP address you find in WAN) from a different network.



Also make sure PORT 1883 is not used by another application.



## 9.6 BEANDEVICE® WILLOW® CONFIGURATION

- To setup the MQTT Publisher on your BeanDevice® Wilow®, it needs to be connected locally using TCP Connection first, once the BeanDevice® is connected to our WIFI network we can start configuring MQTT settings,
- After turning on your BeanDevice® Wilow® using the magnet go to BeanScope® supervision software Wilow® Wlan/LAN configuration window (Tools→ Wlan/LAN configuration), enter the default network settings and click on validate.



The WIFI AP on the Wilow® IoT Gateway comes with the following WIFI configuration:

- **Default SSID: beanair**
- **Password: beanair2019**
- **security type: WPA2**

Wifi configuration

Enabled

SSID : beanair

Password : beanair2018

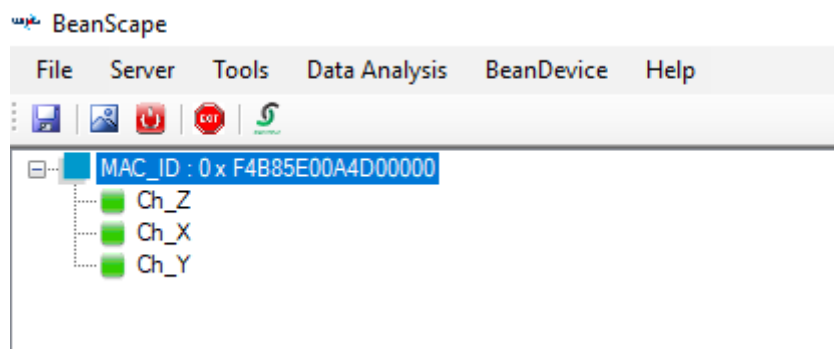
security type : WPA2

Validate

*Figure 16 :BeanDevice® Wilow® network settings configuration*



[See our Technical video Getting started with BeanDevice® Wilow®](#)



*Figure 17 :BeanDevice® Wilow® profile on BeanScope®*



For more information how to connect BeanDevice® Wilow® to Wi-Fi network. Please refer to the user manual at page 48

Next, start MQTT configuration panel on **BeanDevice®** tab

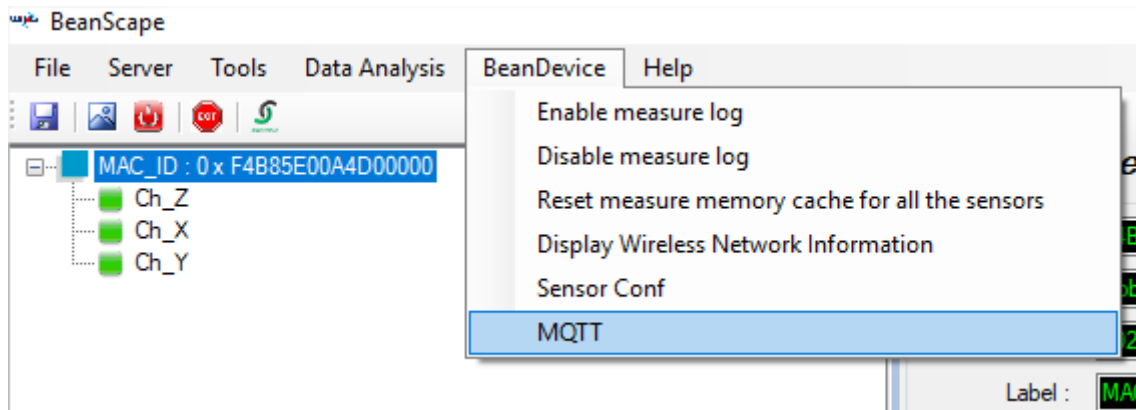


Figure 18 :MQTT configuration

MQTT configuration window will pop up:

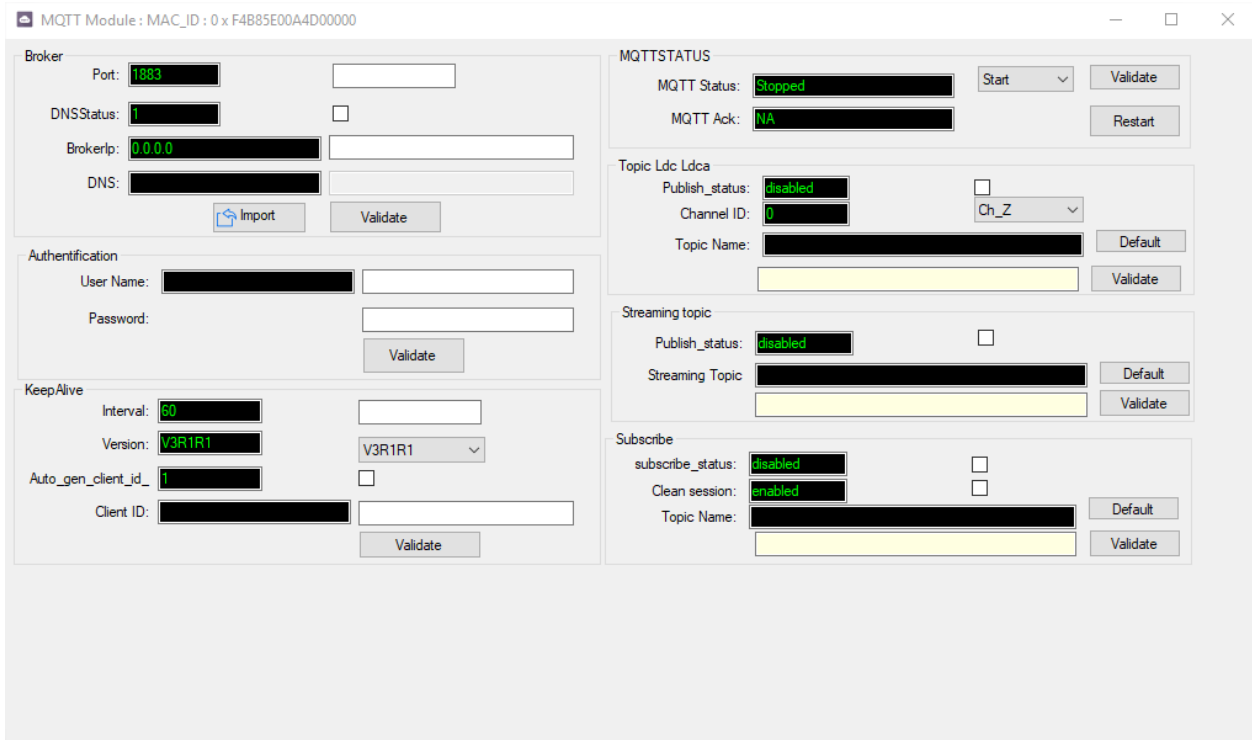


Figure 19 :MQTT configuration window

Follow this screenshot and fill in your Broker settings, then validate:



***Before validating, make sure the MQTT module is stopped; otherwise the configuration will not be accepted***

Broker

Port:

DNSStatus:

BrokerIp:

DNS:

- **Port:** TCP/IP port to use with MQTT .1883 is the reserved port to use.
- **DNSStatus:** check if you want to enter your broker DNS. For IoT Gateway we are using IP address
- **BrokerIp:** enter your broker IP address after unchecking DNSStatus .192.168.1.243
- **DNS:** domain name server of your Broker (not used here)

### 9.6.1 Authentication

MQTT broker can be configured to require client authentication using a valid username and password before a connection is permitted, (not used with IoT Gateway)

Authentication

User Name:

Password:

- **User Name:** specify your user name
- **Password:** enter your password

### 9.6.2 Keep alive

The keep alive functionality assures that the connection is still open and both broker and client are connected to one another

KeepAlive

Interval:

Version:

Auto\_gen\_client\_id\_

Client ID:

- **Interval:** The interval is the longest possible period of time, which broker and client can endure without sending a message.
- **Version:** MQTT protocol version
- **Auto\_gen\_client\_ID:** check for auto generate a Client ID
- **Client ID:** Enter your client ID

### 9.6.3 MQTT Status

Here you can check your MQTT different status, connected, stopped , connecting or disconnecting and can start your connection from here.

MQTTSTATUS

MQTT Status:

MQTT Ack:

- **MQTT Status:** shows the current status of the MQTT module:
  - **Connecting:** trying to establish a connection
  - **Connected:** connection established
  - **Disconnecting:** disconnecting the Client
  - **Stopped:** the connection is stopped
- **Password:** enter your password
- **Start/Stop:** select and **Validate** to start or stop your MQTT Client connection
- **Restart:** restart your connection

### 9.6.4 Topic related to static measurement

LDC topic is a string used by the broker to filter messages for each LowDutyCycle channel of the connected BeanDevice, enable each channel and set its name to default to avoid problems. Then validate

The screenshot shows a configuration window titled "Topic Ldc Ldca". It contains the following fields and controls:

- Publish\_status:** A dropdown menu showing "enabled".
- Channel ID:** A text input field containing "0".
- Topic Name:** A text input field containing "F4B85E00A4D00000/SENSOR/0".
- Ch\_Z:** A dropdown menu showing "Ch\_Z".
- Buttons:** "Default" and "Validate" buttons are located to the right of the Topic Name field.

- **Publish\_status:** check and **validate** to enable publishing
- **Channel ID :** channel identification
- **Topic Name:** Field to enter your topic's name

### 9.6.5 Topic related to dynamic measurement

Streaming topic is a string used by the broker to filter messages for streaming data from the connected BeanDevice. Enable and set its name to default then validate.

The screenshot shows a configuration window titled "Streaming topic". It contains the following fields and controls:

- Publish\_status:** A dropdown menu showing "enabled".
- Streaming Topic:** A text input field containing "F4B85E00A4D00000/STREAMING".
- Buttons:** "Default" and "Validate" buttons are located to the right of the Streaming Topic field.

- **Publish\_status:** check and **validate** to enable publishing
- **Streaming Topic:** Text field to enter your streaming topic's name

### 9.6.6 Subscribe

This Topic will be the string we will use to connect to the BeanDevice from remote BeanScope supervision software in order to send OTACs. By default this will be set to `MAC_ID/OTAC` .differentiating between BeanDevice using the unique MAC ID.

Enable subscribe and set your Topic to default and validate.



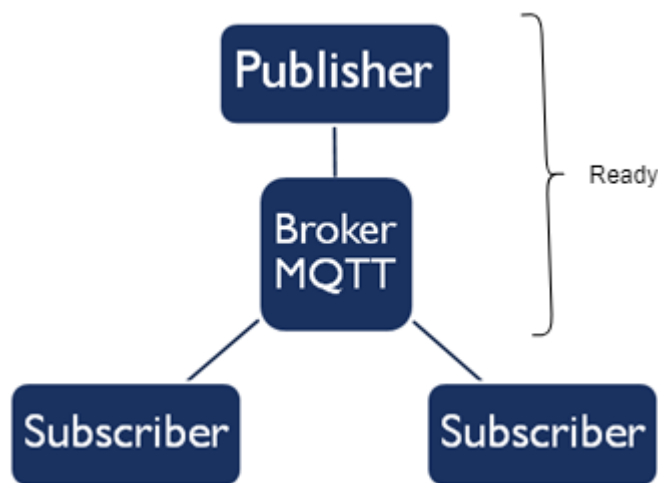
Subscribe

subscribe\_status:  enabled

Clean session:  disabled

Topic Name:

- **Subscribe\_status:** check and **validate** to enable subscribing
- **Clean session:** check and validate to enable, then the client does not have a persistent session and all information are lost when the client disconnects for any reason
- **Topic Name:** Field to enter your topic's name to subscribe to



The BeanDevice Wilow is now configured to publish its data through MQTT ,this can be checked in [MQTT conf](#) for each functional channel .

Custom display | Notes | Status | Measurement conditioning calibration | **MQTT Conf** | Log config. | /

Topic LDC / LDCA

Topic Name:

Retain Flag:  disabled

**Publishing:  enabled**

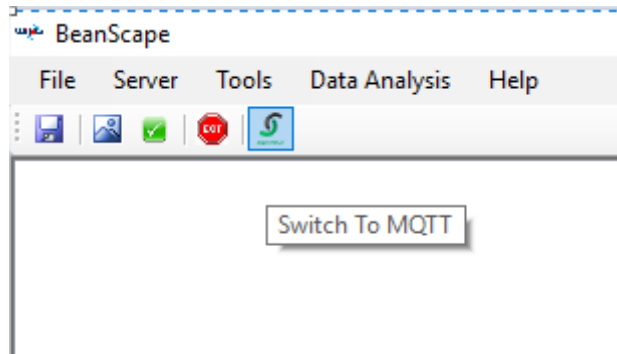
All you have to do now is to write down your Subscribe Topic name and save it as we will use it to connect to the BeanDevice willow from monitoring location.(For example: [F4B85E00A4D00000/OTAC](#))

## 9.7 ENABLING THE REMOTE ACCESS AT YOUR OFFICE

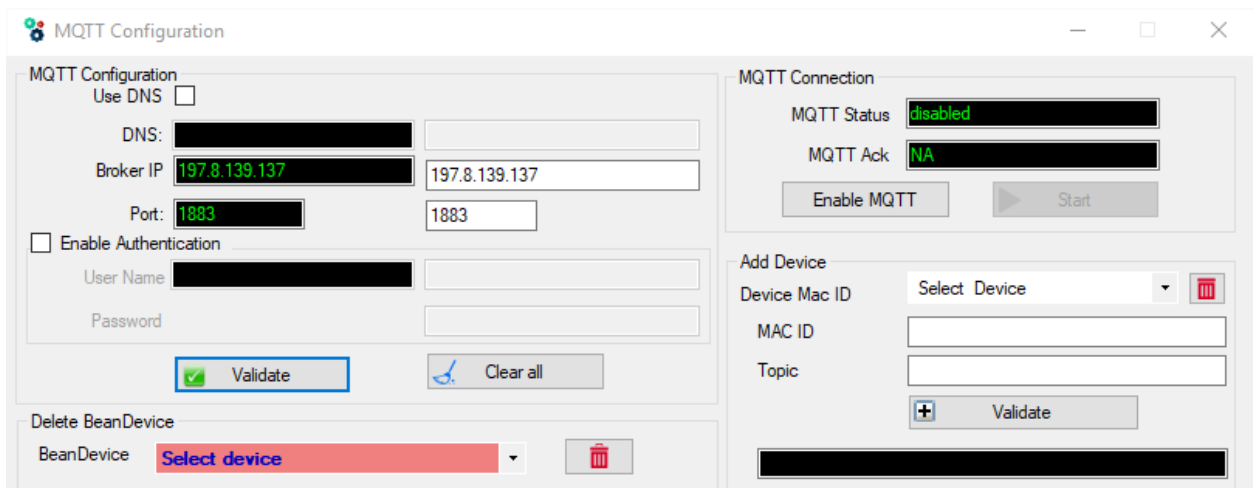
### 9.7.1 BeanScape® RA configuration

Using **BeanScape® RA** you will have the ability to subscribe remotely to any BeanDevice® publishing data, first you have to install and run your BeanScape RA at your monitoring office.

- You have to switch to MQTT using this button



- Next ,go to Tools tab →MQTT configuration and a new configuration window will pop up ,and we will establish a communication with our IoT Gateway ,

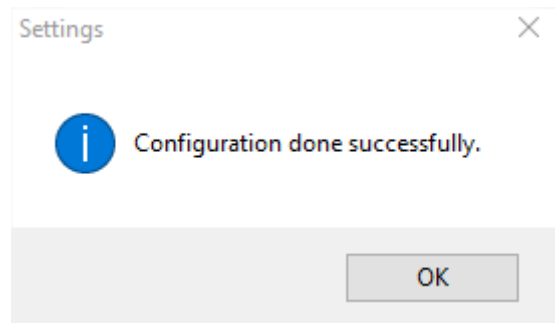


- In Broker IP you have to enter the IoT Gateway WAN IP Address, you can retrieve that from the interface we previously connected to .
- Port should be set to 1883 then validate

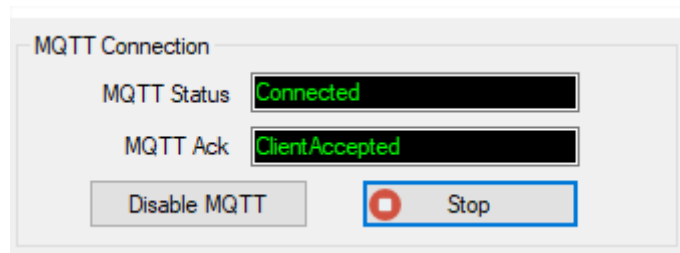


WAN IP address should be the same as the Public IP address you look at using What’s My IP site (using browser) during connection to the IoT gateway.

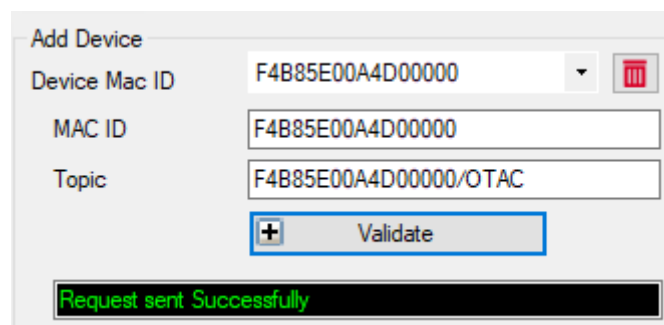
A successful configuration acknowledgement window will pop up .



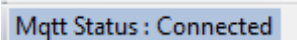
- On MQTT connection, enable MQTT and click on start, and the connection is successfully established as we can see on the status .



- Now, enter the BeanDevice Wilow MAC\_ID and Subscribe Topic we had previously setup for the BeanDevice .validate and the BeanDevice profile will be there .



Close the MQTT configuration window and make sure the server is started; the BeanDevice will be at your disposal, to read measurement,

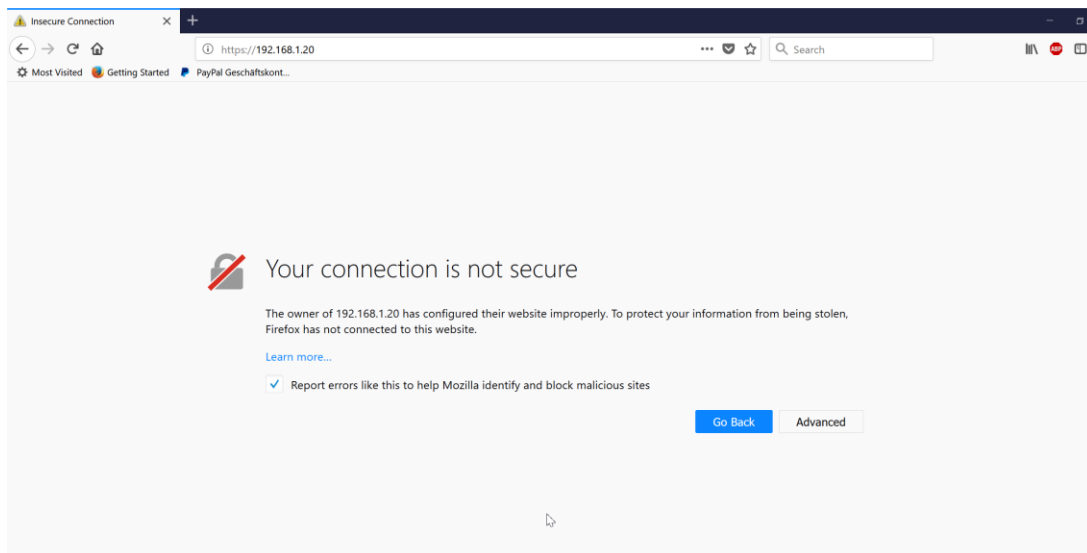


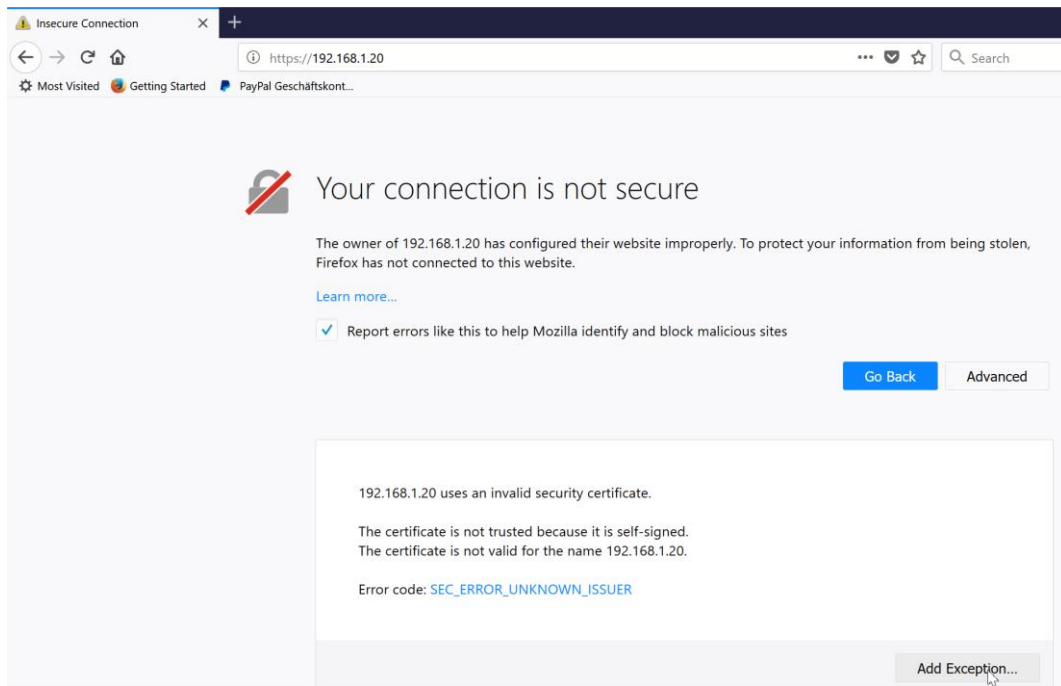
## 10.APPENDIX 1: WIFI AP WITH WDS FUNCTION - BULLET M2 HP CONFIGURATION (IF FACTORY SETTINGS ARE RESTORED)

Using the Ethernet connector, you will find inside, you connect to your PC to access the Wi-Fi access point configuration interface. By default its IP address is set to **192.168.1.20**, the username is **ubnt** and the password is **beanair**



*Warning message can be displayed by your browser, you should click on continue anyway*





***Figure 20: A Screenshot of warning message***

## 10.1 AIRMAX FUNCTION

After logging, you will have to configure these different settings on the access point:

- Select the first tab and disable **AirMax**

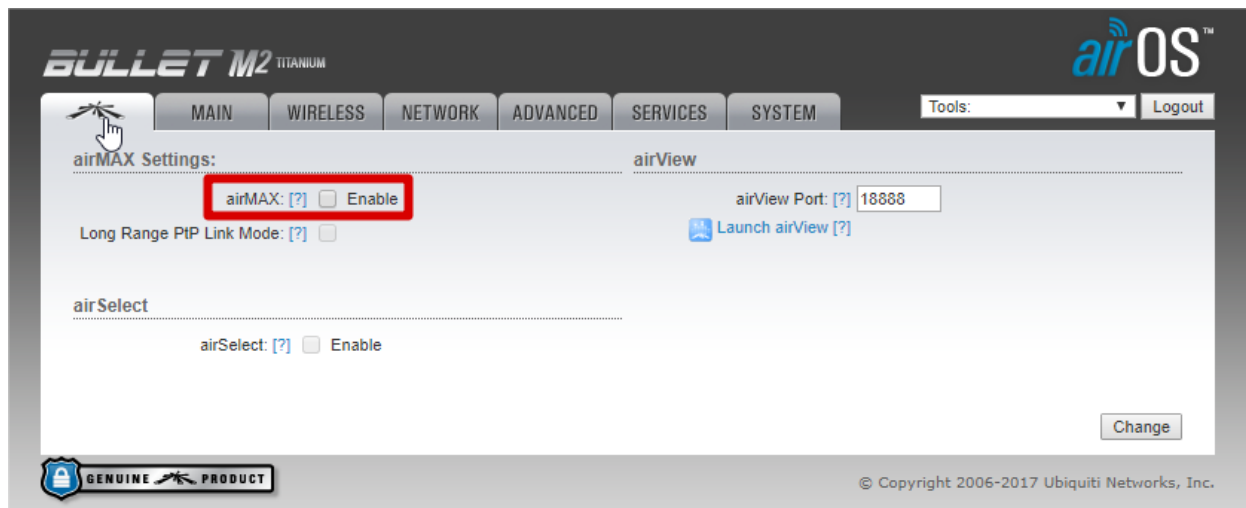


Figure 21: Airmax function should be disabled

## 10.2 WIRELESS CONFIGURATION

The screenshot shows the 'BULLET M2' wireless configuration interface. The top navigation bar includes 'MAIN', 'WIRELESS', 'NETWORK', 'ADVANCED', 'SERVICES', and 'SYSTEM'. The 'WIRELESS' tab is selected. The interface is divided into two main sections: 'Basic Wireless Settings' and 'Wireless Security'.

**Basic Wireless Settings:**

- Wireless Mode: **Access Point** (dropdown)
- WDS (Transparent Bridge Mode):  **Enable**
- SSID: **Beanair** (text input)  **Hide SSID**
- Country Code: **Germany** (dropdown)
- IEEE 802.11 Mode: **B/G/N mixed** (dropdown)
- Channel Width: **20 MHz** (dropdown)
- Frequency, MHz: **auto** (dropdown)
- Extension Channel: **None** (dropdown)
- Frequency List, MHz:  **Enable**
- Calculate EIRP Limit:  **Enable**
- Antenna Gain:  **dBi**  **Cable Loss: dB**
- Output Power:  **dBm**
- Data Rate Module: **Default** (dropdown)
- Max TX Rate, Mbps: **MCS 7 - 65/72.2** (dropdown)  **Auto**

**Wireless Security:**

- Security: **WPA2-AES** (dropdown)
- WPA Authentication: **PSK** (dropdown)
- WPA Preshared Key:   **Show**
- MAC ACL:  **Enable**

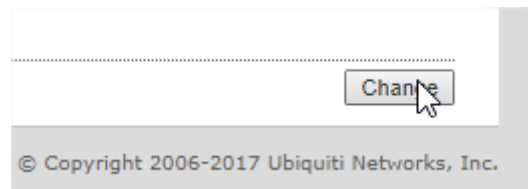
A 'Change' button is located at the bottom right of the configuration area. At the bottom left, there is a 'GENUINE PRODUCT' logo, and at the bottom right, the copyright notice: '© Copyright 2006-2019 Ubiquiti Networks, Inc.'

Figure 22: Wireless Configuration - WIFI AP

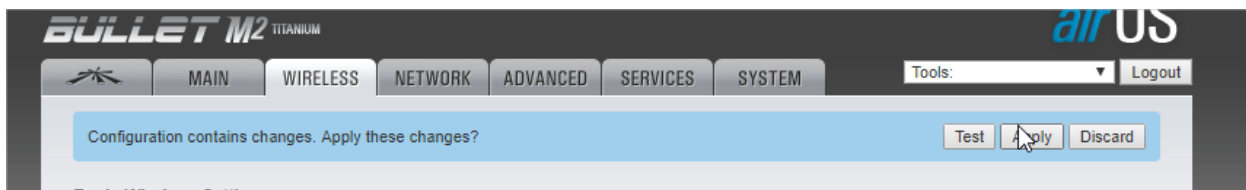
- Select the Wireless Mode as **Access Point**
- Check **WDS (Transparent Bridge Mode)**
- SSID is **Beanair**
- Select your country
- IEEE 802.11 Mode to **B/G/N mixed**
- Channel width to **20 MHz**
- Frequency to **2437 MHz (BeanDevice® Wilow® can't work on all the WIFI frequencies)**

- Extension channel to **None**
- Frequency List, MHz Is **Enabled**
- Calculate EIRP Limit is **Enabled**
- Leave the next 4 lines to default (as shown in the screenshot below)
- Set your security to **WPA2-AES** with WPA Authentication set to PSK
- WPA Preshared key is **beanair2019**
- MAC ACL is **disabled**

After all modifications set, click on change then apply



**Make sure to click on apply otherwise your configuration is not modified**



### 10.3 NETWORK CONFIGURATION

- Next, move to the Network Tab, make sure the network Mode is set to **Bridge** and IP address management is Static with IP Address defined at **192.168.1.20** with Gateway IP set to **192.168.1.1**



The screenshot displays the web interface for a Bullet M2 Titanium device. The top navigation bar includes tabs for MAIN, WIRELESS, NETWORK, ADVANCED, SERVICES, and SYSTEM. The NETWORK tab is active. The interface is titled 'airOS' and includes a 'Tools' dropdown and a 'Logout' button. The configuration is organized into three sections:

- Network Role:**
  - Network Mode: Bridge
  - Disable Network: None
- Configuration Mode:**
  - Configuration Mode: Simple
- Management Network Settings:**
  - Management IP Address: DHCP (selected) / Static
  - IP Address: 192.168.1.20
  - Netmask: 255.255.255.0
  - Gateway IP: 192.168.1.1
  - Primary DNS IP: (empty)
  - Secondary DNS IP: (empty)
  - MTU: 1500
  - Management VLAN:  Enable
  - Auto IP Aliasing:  Enable
  - STP:  Enable
  - IPv6:  Enable

A 'Change' button is located at the bottom right of the configuration area.

After all modifications set, click on change then apply ,the access point is now well configured and ready to use ,you can continue with your deployment setup.

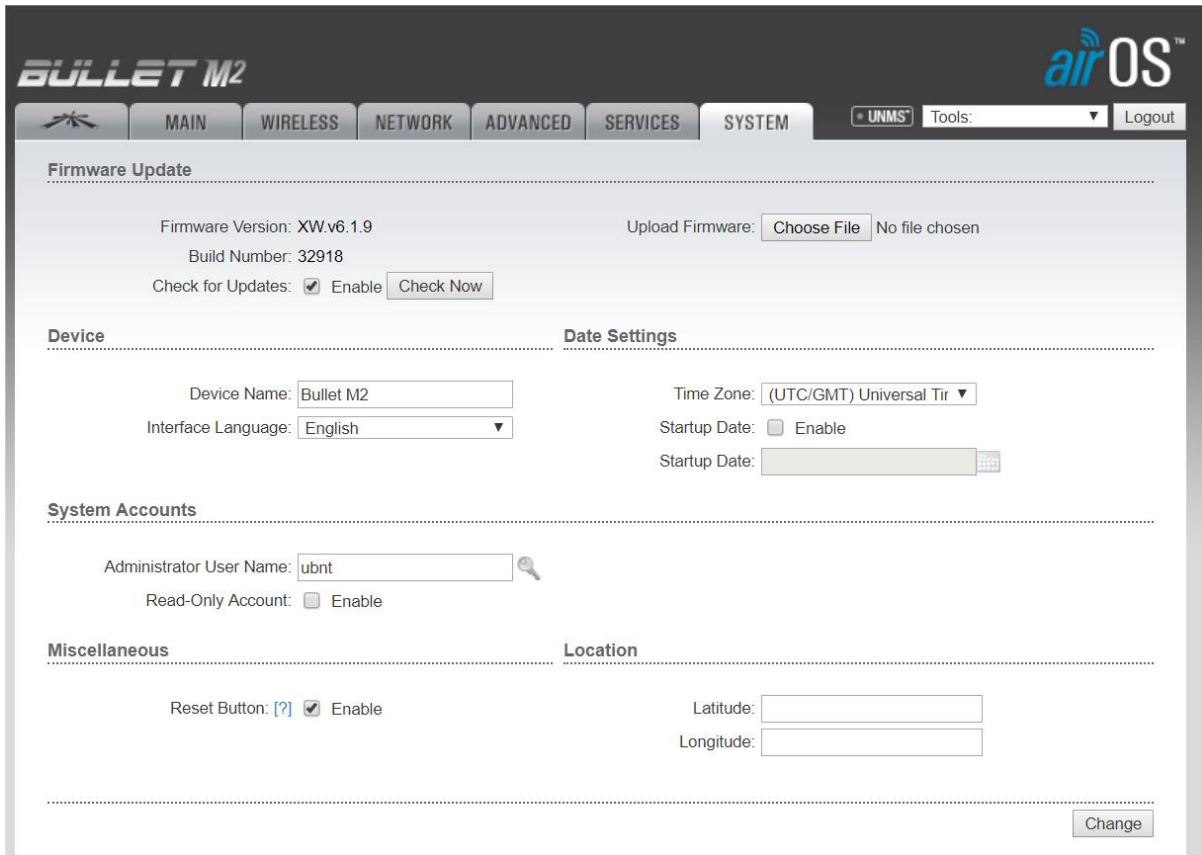
## 10.4 FIRMWARE UPDATE

Go on **System**, then click on choose File to select the latest Bullet M2 HP firmware coming with the following format:

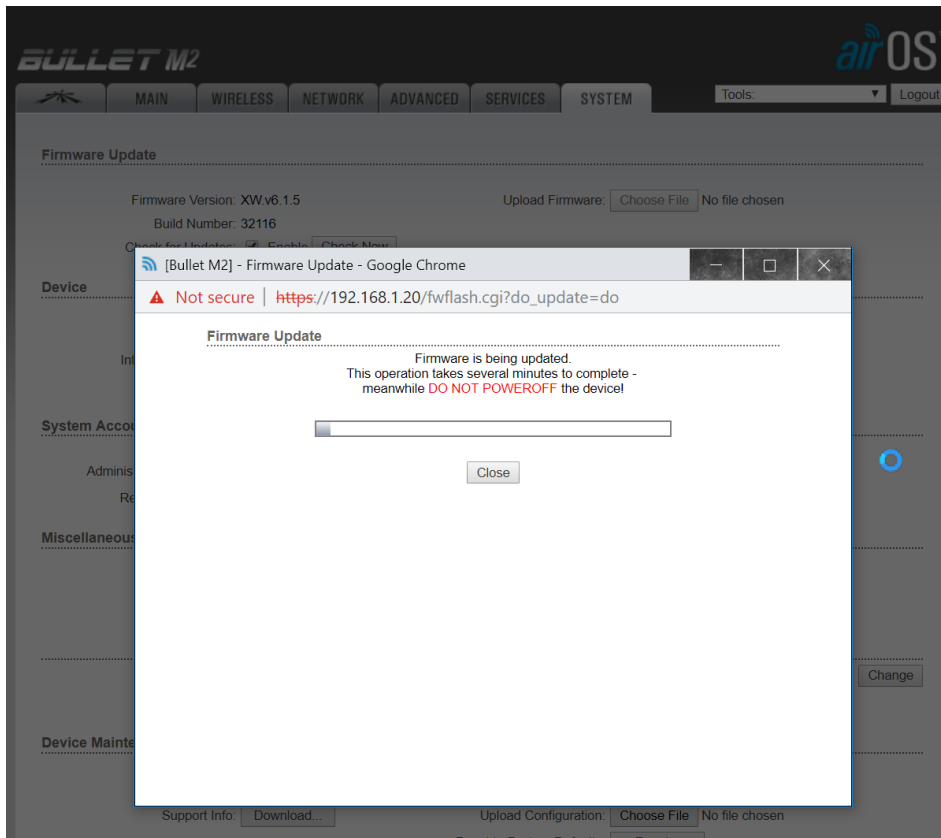
**XW.vVERSION.XXXX.XXXX.XXXX.bin**

You can find Buller M2 HP Firmware:

- Ubiquiti website – download page
- Beanair® website – Wilow® Firmware



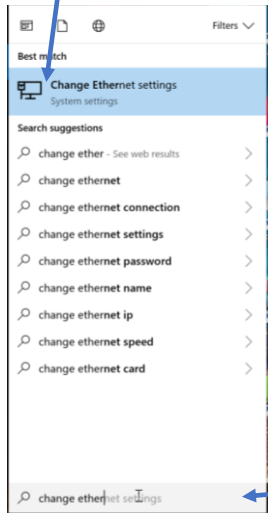
Then firmware update can restart:



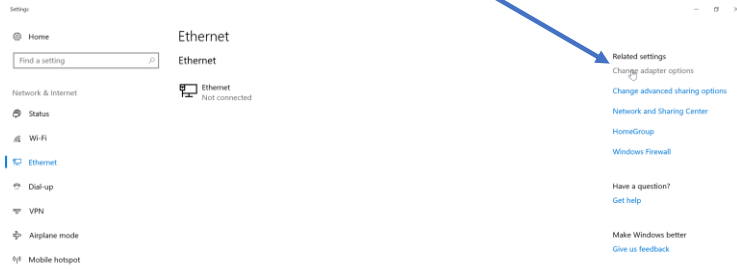
## 11. APPENDIX 2: LTE ROUTER CONFIGURATION (IF FACTORY SETTINGS ARE RESTORED)

### 11.1 GET AN ACCESS TO YOUR LTE ROUTER

2. Select **Ethernet Settings**

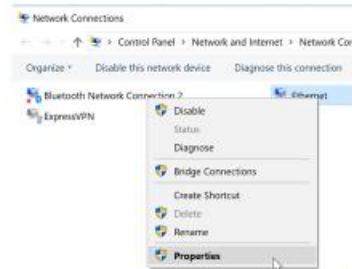


3. A new window pop-up's , select **Change adapter options**

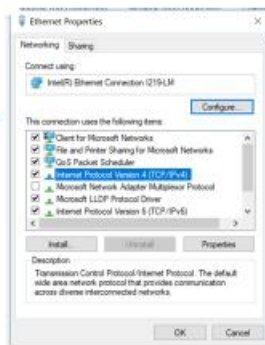


1. Use the search tool, type in **Change Ethernet Settings**

4. right click on your Ethernet device which is connected to your 4G Router

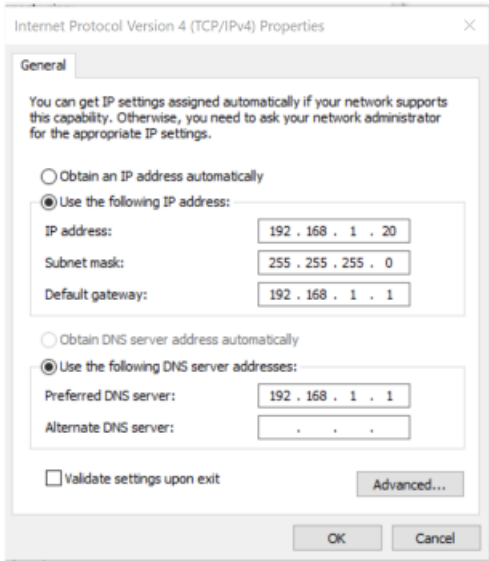


5. Click on **Properties**, then select **Internet Protocol Version 4 (TCP/IPv4)** then click on **Properties**



6. By default DHCP is enabled on your PC, i.e. IP address can be automatically allocated

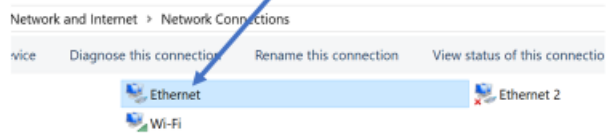




**7. Choose Manual IP configuration**

- First select an IP address. The 4G router is configured with the default IP Address **192.168.1.1** . You can enter an IP in the form of 192.168.1.XXX, where XXX is a number in the range of **2-254**.  
Avoid to use the same IP address than your 4G Router which is **192.168.1.1**
- Enter 255.255.255.0 for your subnet mask
- The default gateway must come with the same IP address that your 4G Router **192.168.1.1**
- Finally enter primary DNS server IP , the same than your 4G Router IP **192.168.1.1**
- Click on OK validate your configuration

Your Ethernet Icon is displayed connected



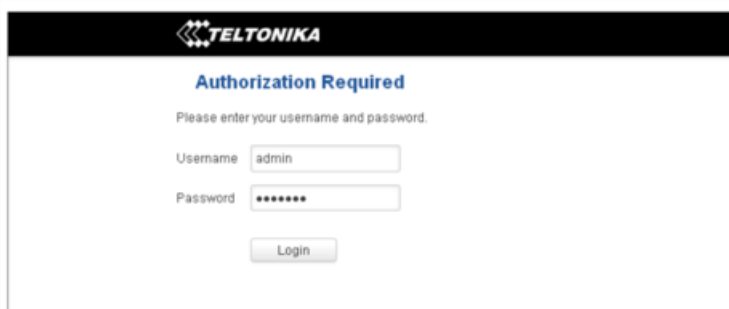
8. Now that your PC's Ethernet network settings are configured, launch your browser (Mozilla or Chrome, Adblocker should be disabled) and enter your Router's IP into the the address field: 192.168.1.1



9. Enter username and password, by default these settings are:

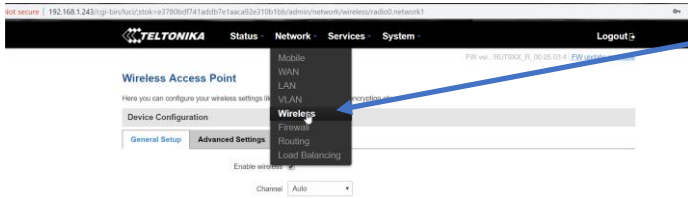
**Username: admin**  
**Password: admin01**

then click on login, you will get logged into your 4G Router

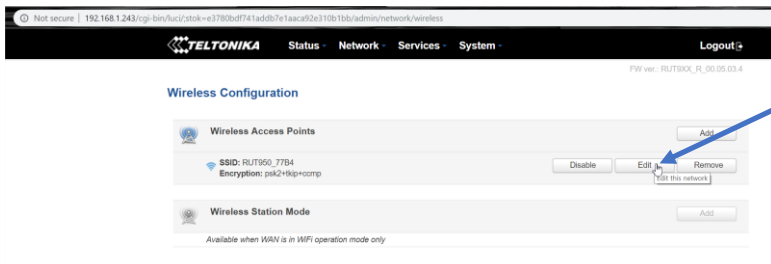


## 11.2 INTERNAL WIFI AP CONFIGURATION

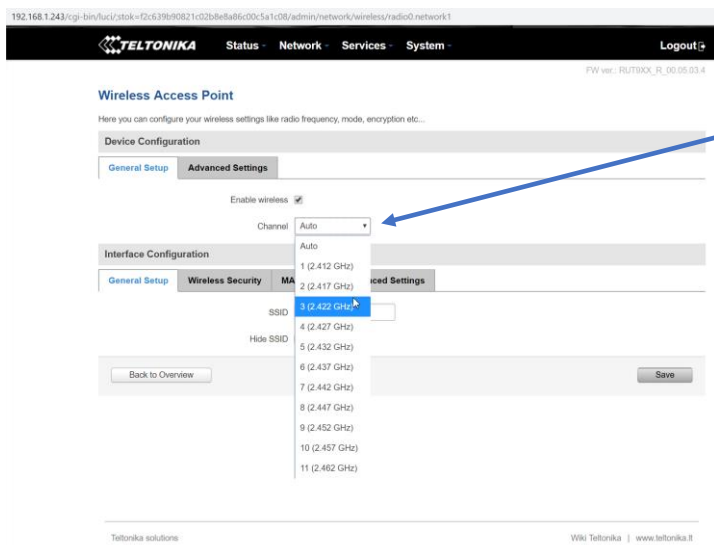
### 11.2.1 Case 1: Using Internal WIFI AP



1. Click on Network then wireless



2. Edit to configure your SSID and Password

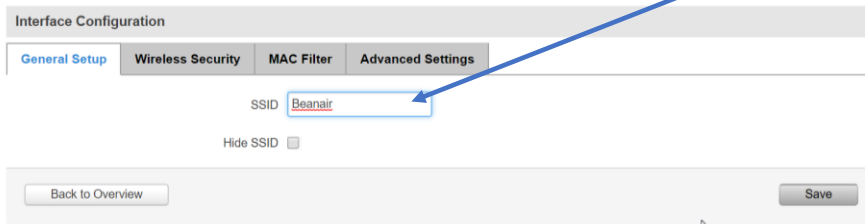


3. Select your WIFI channel between 1 and 11

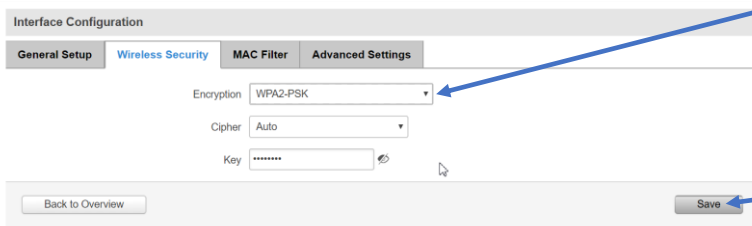


As Wilow® device comes with both CE and FCC certifications. It's compatible with North America WIFI, it will not work on Channels 12,13 and 14

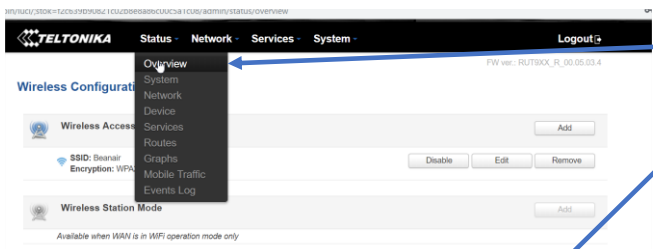
4. Choose your SSID , Example : Beanair



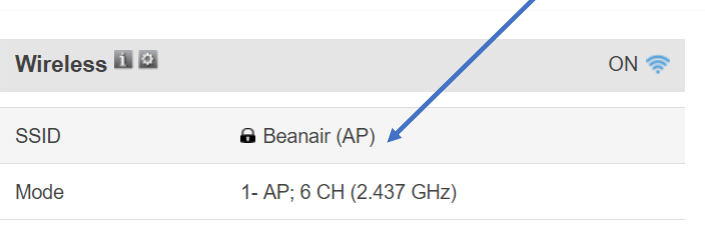
5. Choose the encryption WPA2-PSK  
Cipher : Auto  
Key: choose a strong key that you can remember , example: Beanair2019



6. Click on save



7. Click on Status the Overview,  
you can check your WIFI Network  
status



### 11.2.2 Case 2: Using external WIFI AP with WDS function

If you are using External WIFI AP with WDS function, Disable the Wi-Fi Access point function on your LTE Router

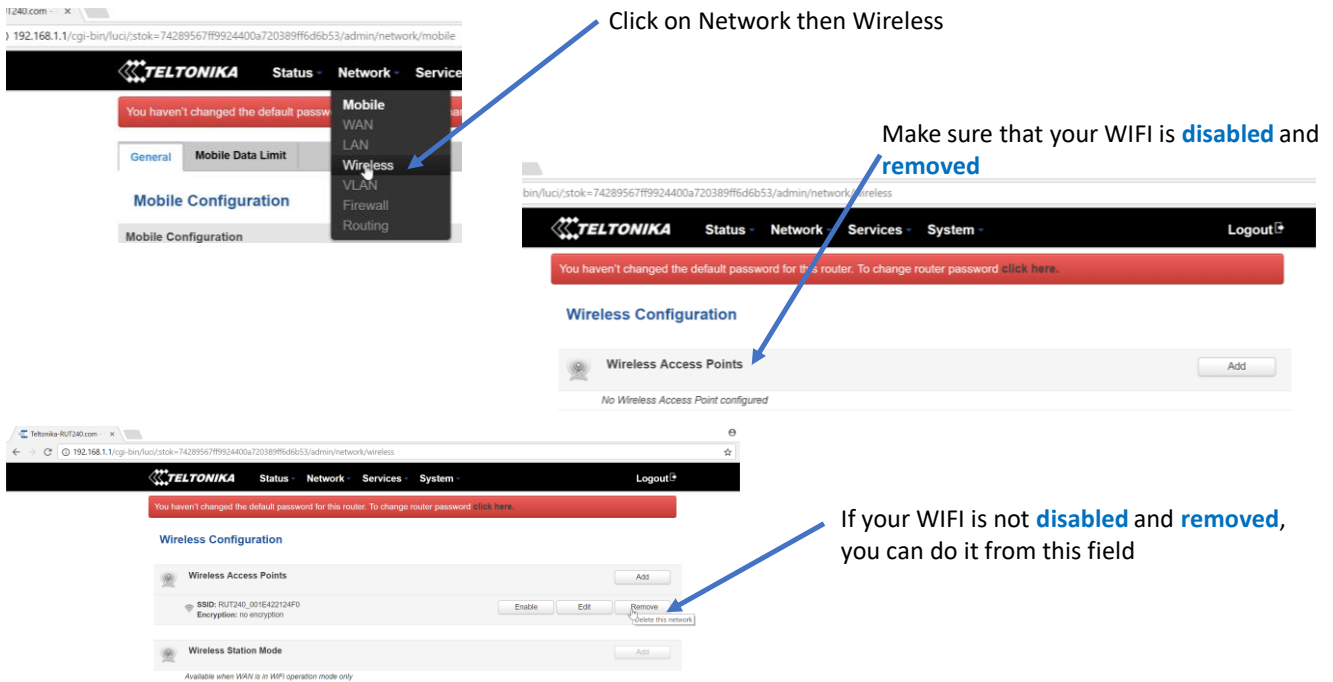
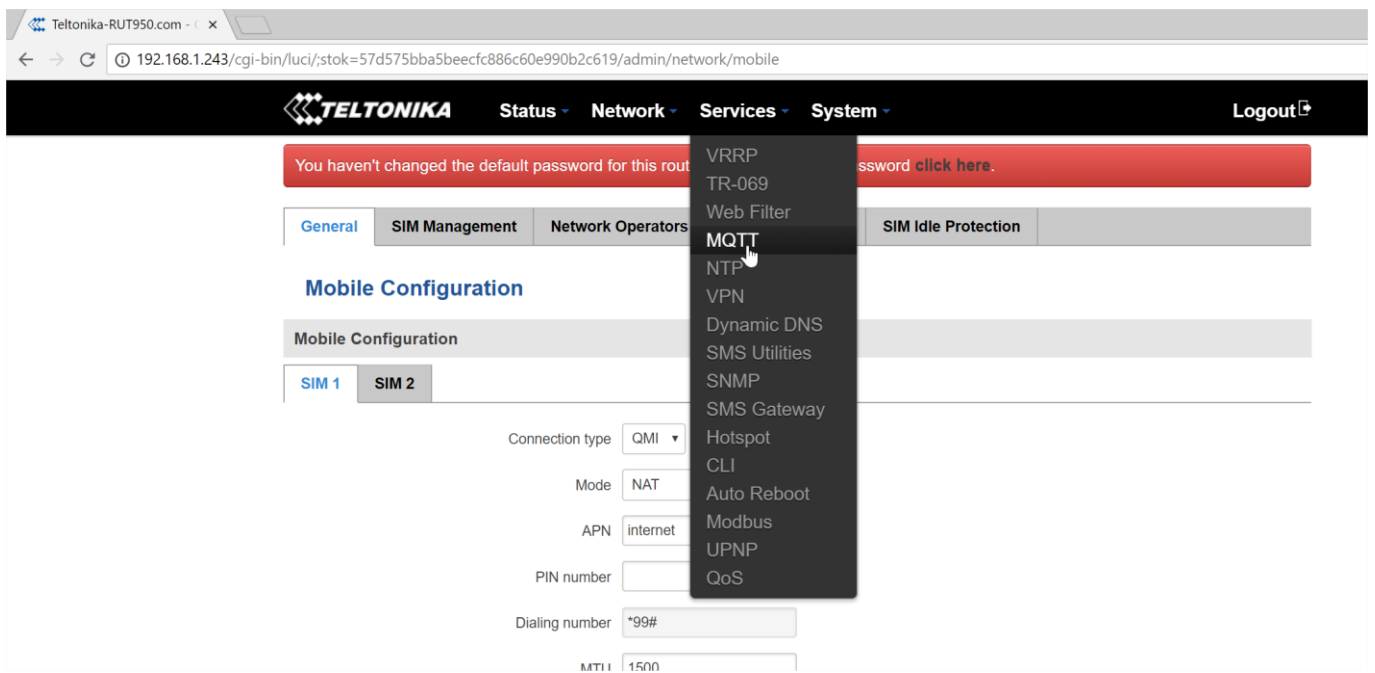


Figure 23: WIFI Access Point should be disabled

### 11.3 ENABLE YOUR MQTT BROKER

Click on **Services** Tab then **MQTT**



Click on **Enable MQTT Broker**, use the Local Port **1883** and click on **Enable Remote Access**

in/luci/stok=57d575bba5beecfc886c60e990b2c619/admin/services/mqtt

**TELTONIKA** Status ▾ Network ▾ Services ▾ System ▾ Logout ↗

You haven't changed the default password for this router. To change router password [click here](#).

Broker Publisher

### MQTT Broker

Enable

Local Port

Enable Remote Access

Broker settings

Security Bridge Miscellaneous

Use TLS/SSL

Save

Figure 24: MQTT Broker configuration



**SCIGATE AUTOMATION (S) PTE LTD**

No.1 Bukit Batok Street 22 #01-01 Singapore 659592

Tel: (65) 6561 0488

Fax: (65) 6562 0588

Email: sales@scigate.com.sg

Web: www.scigate.com.sg

Business Hours: Monday - Friday 8.30am - 6.15pm