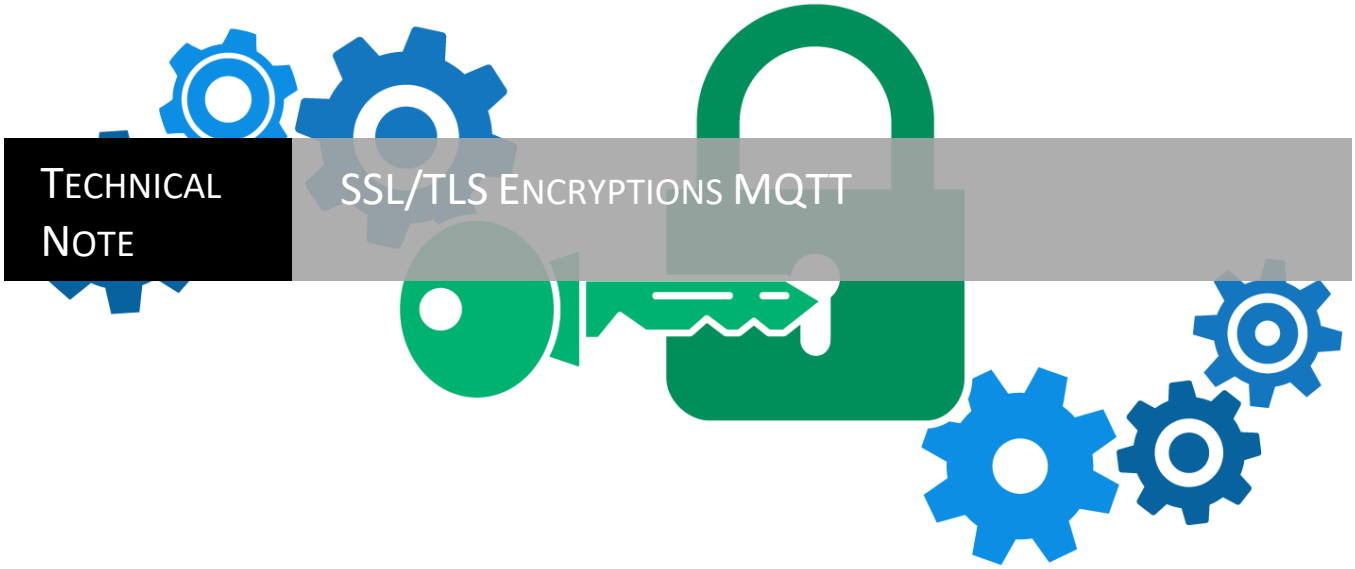
BeanDevice®

Version 1.0



TECHNICAL NOTE

SSL/TLS ENCRYPTIONS MQTT

BeanAir

Rethinking Sensing Technology

Wilow

DOCUMENT			
Document ID	TN_RF-021	**Version**	V1.0
External reference	TN_RF-021	**Date**	30/03/2020
Author	Achref CHAABENI, Test & validation Engineer		
		Project Code	
Document's name	TN-RF-021-SSL-TLS-Encryption-MQTT		

VALIDATION			
Fonction	**Destination**	**For validation**	**For info**
Writer		✓	
Reader		✓	
Validation			✓

DIFFUSION			
Fonction	**Destination**	**For action**	**For info**
Reader n°1	Antje Jacob, Production Manager	✓	
Reader n°2	Omar SKANDER, Embedded software engineer	✓	

UPDATES			
Version	**Date**	**Auteur**	**Evolution & Status**
1.0	30/03/2020	Achref CHAABENI	• First version of the document

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.

Contents

List of Tables

No table of figures entries found.

List of Figures

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

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

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

Symbols	*Definition*
	***Caution or Warning*** *– 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.*
	***Danger*** *– This information MUST be followed if not you may damage the equipment permanently or bodily injury may occur.*
	***Tip or Information*** *– Provides advice and suggestions that may be useful when installing Beanair Wireless Sensor Networks.*

3. ACRONYMS AND ABBREVIATIONS

SSL	Secure Socket Layer
TLS	Transport Layer security
CCA	Clear Channel Assessment
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
GTS	Guaranteed Time-Slot
kSps	Kilo samples per second
LLC	Logical Link Control
LQI	Link quality indicator
LDCDA	Low duty cycle data acquisition
MAC	Media Access Control
PAN	Personal Area Network
PER	Packet error rate
RF	Radio Frequency
SD	Secure Digital
WSN	Wireless sensor Network

4. DOCUMENT ORGANIZATION

MQTT configuration	• MQTT publisher configuration on your BeanDevice® Wilow®
SSL	• Descibes offline data analysis tool, only available on BeanDevice® Wilow® AX-3D

5. MQTT CONFIGURATION

To Start configure MQTT, select your BeanDevice® Wilow® and go to the BeanDevice® Wilow® menu and scroll down to MQTT

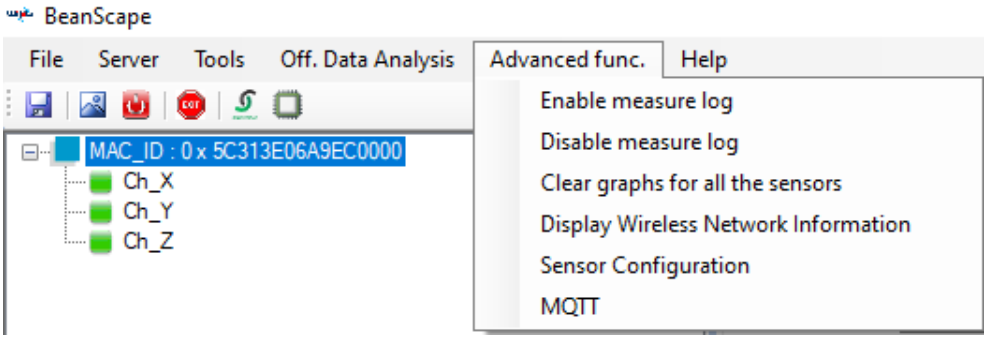


Figure 1: BeanDevice® Wilow® menu

MQTT Module window will pop up as follow:

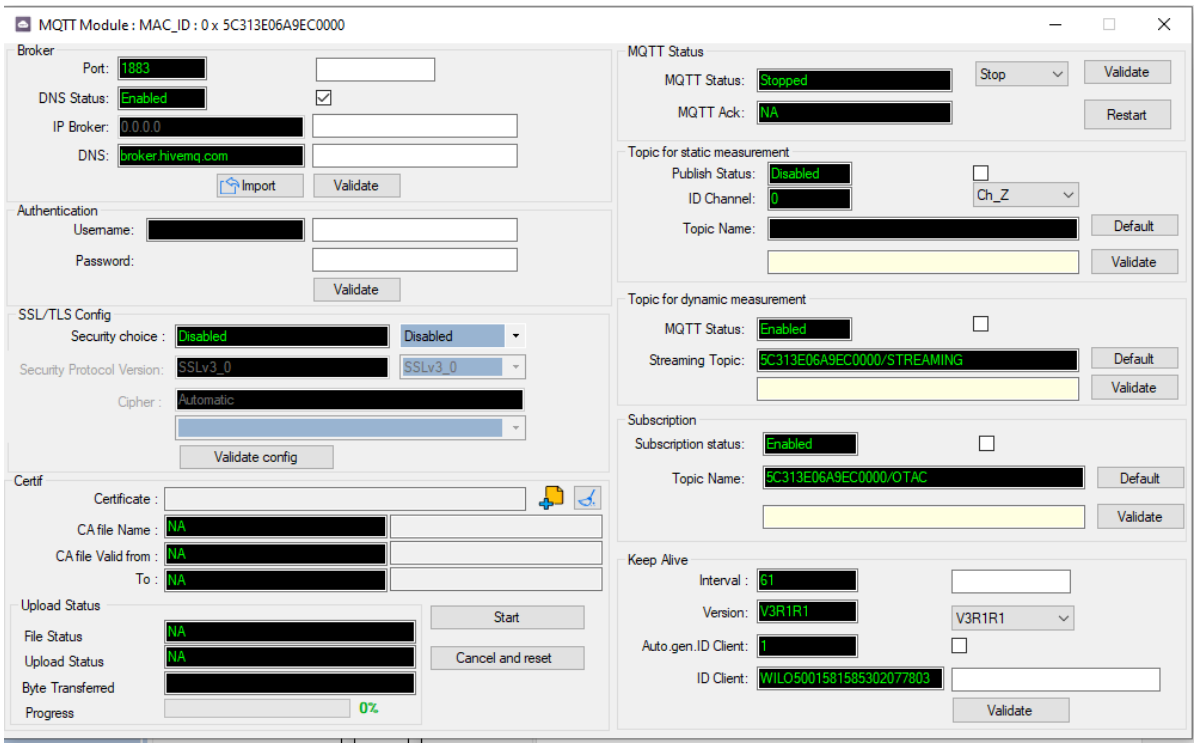


Figure 2: MQTT Module window

5.1 BROKER

The broker is responsible for distributing messages to the related clients based on the topic of a message and there are two categories of brokers:

- ✓ Brokers hosted on the web
- ✓ Brokers running on the internal network.

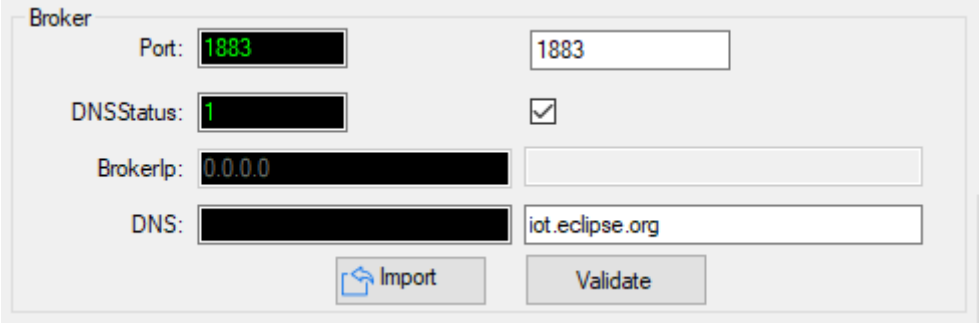


Figure 3: Broker frame

- ***Port***: TCP/IP port to use with MQTT. 1883 and 8883 are the reserved ports for use with MQTT
- ***DNSStatus***: check if you want to enter your broker DNS. DNSStaus is 1
- ***Brokerip***: enter your broker IP address after unchecking DNSStatus. DNSStatus is 0
- ***DNS***: domain name server of your Broker

5.2 KEEP ALIVE

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

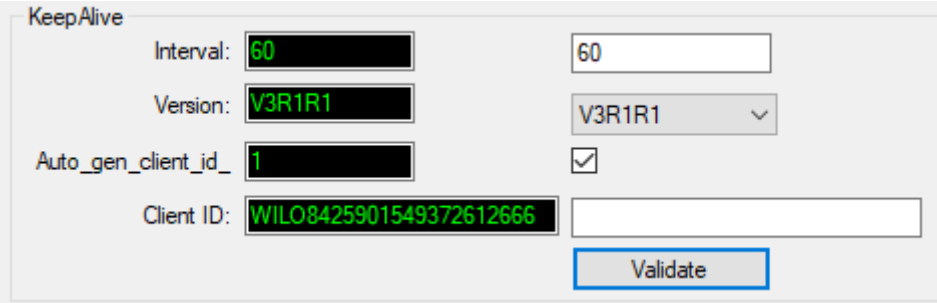


Figure 4: Keep alive frame

- ***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

5.3 AUTHENTIFICATION

MQTT broker can be configured to require client authentication using a valid username and password before a connection is permitted.

Figure 5: Authentication frame

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

5.4 SSL/TLS

SSL stands for Secure Sockets Layer and, in short, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems. The two systems can be a server and a client. It does this by making sure that any data transferred between two systems remain impossible to read. It uses encryption algorithms to scramble data in transit, preventing hackers from reading it as it is sent over the connection.

TLS (Transport Layer Security) is a secured version of SSL.

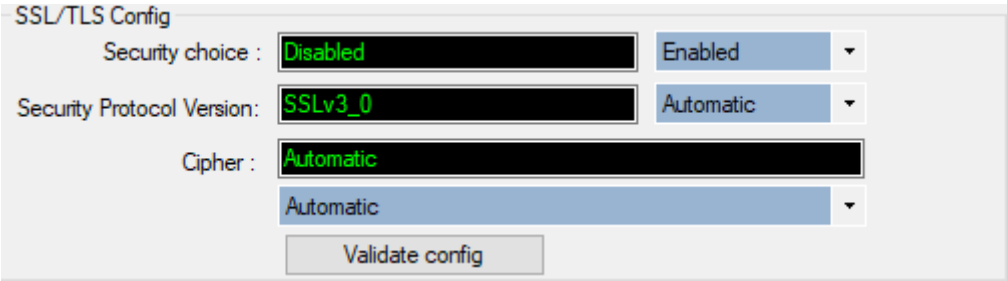


Figure 6 SSL/TLS

- ***Security choice:*** Enable or disable the security.
- ***Security Protocol Version:*** Choose the security protocol (Automatic choice is recommended).
- ***Cipher:*** Choose the cipher suit (Automatic choice is recommended).

5.5 CERTIF

We can choose the server root file from the local machine.

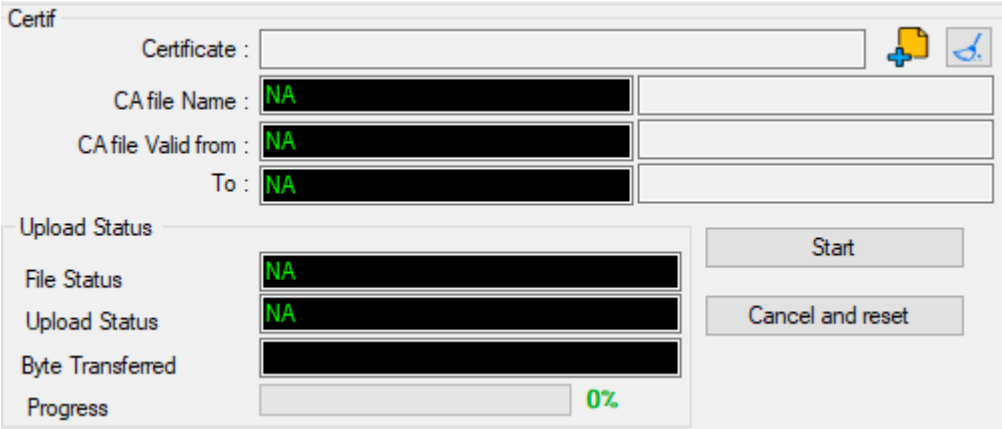


Figure 7 Certif

- ***Certificate:*** choose the certificate from local machine.
- ***CA file Name:*** enter the name of the file.
- ***CA file Valid from:*** choose the sender.
- ***To:*** choose the receiver (we can check the validity of the file on the Beanscape side before send it to avoid problems).
- ***Start:*** starting the process of the sending.
- ***Cancel and reset:*** cancelling the sending of the file and reset the informations.

5.6 MQTT STATUS

Here you can check your MQTT status:

- ✓ connected or stopped,
- ✓ connecting or disconnecting

And you can start your connection from here.

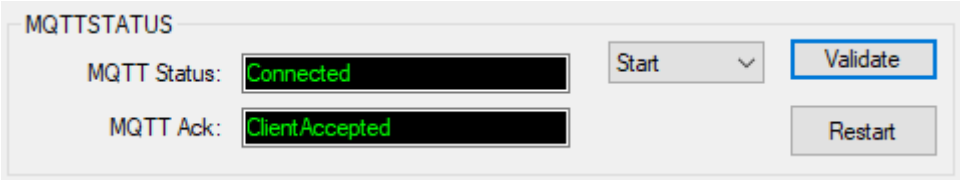


Figure 8: MQTT Status frame

- ***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
- ***Start/Stop:*** select and **Validate** to start or stop your MQTT Client connection
- ***Restart:*** restart your connection

5.7 TOPIC FOR STATIC MEASUREMENT

A topic is a string used by the broker to filter messages for each connected client. Using this Topic for static measurement you will receive LowDutyCycle & Alarm acquisition modes that are publishing to the MQTT broker,

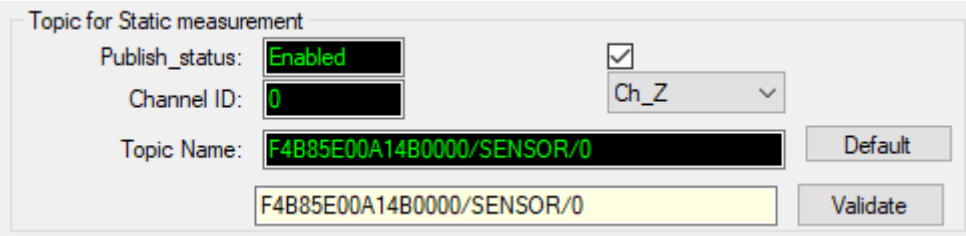


Figure 9: Topic for static measurement frame

- ***Publish_status:*** Check the check-button and **validate** to enable publishing
- ***Channel ID:*** channel identification
- ***Topic Name:*** Field to enter your topic's name

5.8 TOPIC FOR DYNAMIC MEASUREMENT

Using this Topic for Dynamic measurement you will receive Streaming, S.E.T & Shock detection acquisition modes that are publishing to the MQTT broker,

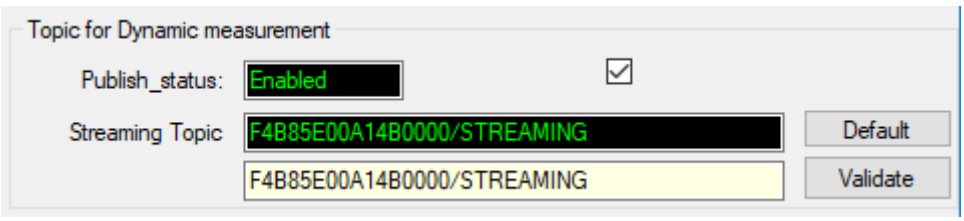


Figure 10: Topic for dynamic measurement frame

- ***Publish_status:*** check the check-button and **validate** to enable publishing
- ***Streaming Topic:*** Text field to enter your streaming topic's name

5.9 SUBSCRIBE

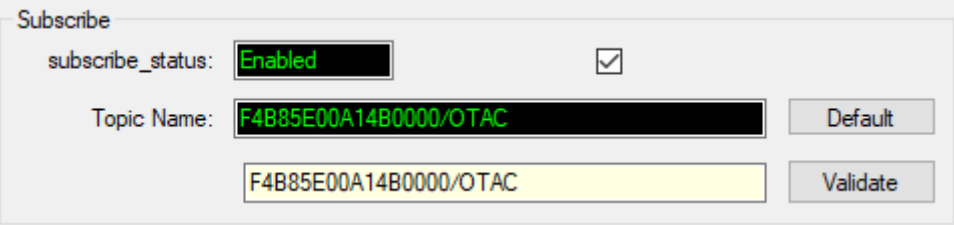


Figure 11: Subscribe

- ***Subscribe_status:*** check the check-button and **validate** to enable subscribing
- ***Topic Name:*** Field to enter your topic's name to subscribe to

6. SSL CONFIGURATION

6.1 INTRODUCTION ABOUT SSL

SSL stands for **S**ecure **S**ockets **L**ayer and, in short, it is a standard technology for keeping an internet connection more secure and safeguarding any sensitive data that is being sent between two systems, preventing others from reading and modifying any information transferred, including any potential details. The two system can be server and client (for example, an application with personal identifiable information or with payroll information).

It does this by making sure that any data transferred between users and sites, or between two systems remain impossible to read. It uses encryption algorithms to scramble data in transit, preventing hackers from reading it as it is sent over the connection. This information could be anything sensitive or personal which can include credit card numbers and other financial information, names and addresses.

TLS (**T**ransport **L**ayer **S**ecurity) is an updated, more secure version of SSL. We still refer to our security certificates as SSL because it is more commonly used term.

6.2 SSL ENCRYPTION FOR MQTT COMMUNICATION

- **Configuration on Beandevice® Wilow® Side**

For **SSL** encryption over MQTT, the Beandevice® Wilow® is considered as the client here, and the broker act as a server. First of all we need to download Root certificate CA of the server into the Beandevice® Wilow®.

The Root certificate CA must be a binary file (*.der format)

To convert any type of certificate to a binary file, we can use OpenSSL with the following command:

```
OpenSSL
OpenSSL> x509 -outform der -in "NonBinary_Certificate".crt -out "Binary_Certificate".der
```

Figure 12 OpenSSL command

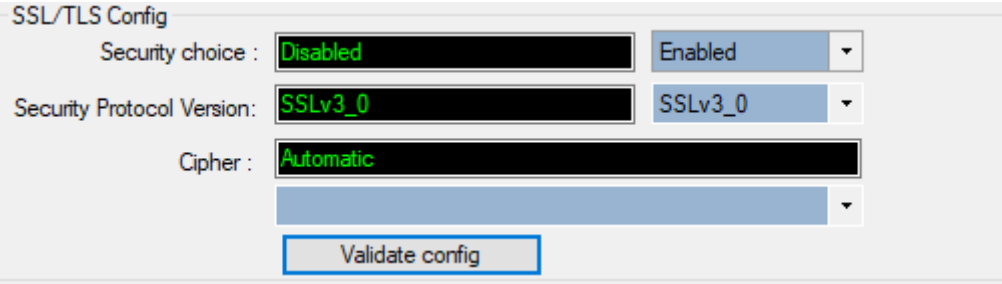


Figure 13 SSL/TLS configuration

On Beanscape® Wilow®, we need to enable the Security choice at first, then configure the secure socket, choose the Security protocol and the cypher in "**SSL/TLS config**" window.

It is highly recommended to choose the Automatic choice for both protocol and cypher then let the server and client choose the most appropriate configuration from the available parameters for both sides during the handshake process

After that in "certif" window we choose the server root file from the local machine and the most important thing is to verify the certificate validity (CA file valid from \ Ca file valid to) so we have put a filter (Beanscape side) to check the validity before we sent the file to avoid problems.

Finally, we click start to send the file.

Beanscape® Wilow® side

To configure the MQTT on the Beanscape side, we need to click on tools then choose MQTT configuration option:

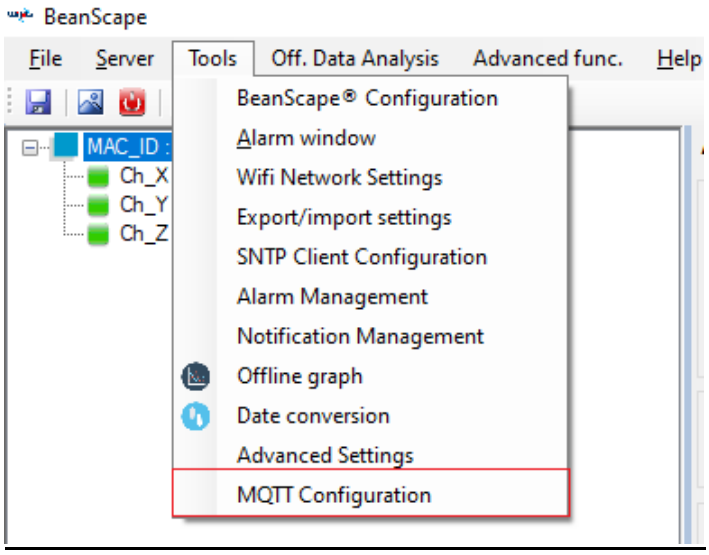


Figure 14 MQTT configuration

For MQTT communication, Beanscape® Wilow® is also seen as a client from the broker side, like the BeanDevice® Wilow® the server root certificate is needed and then configure the secure socket options.

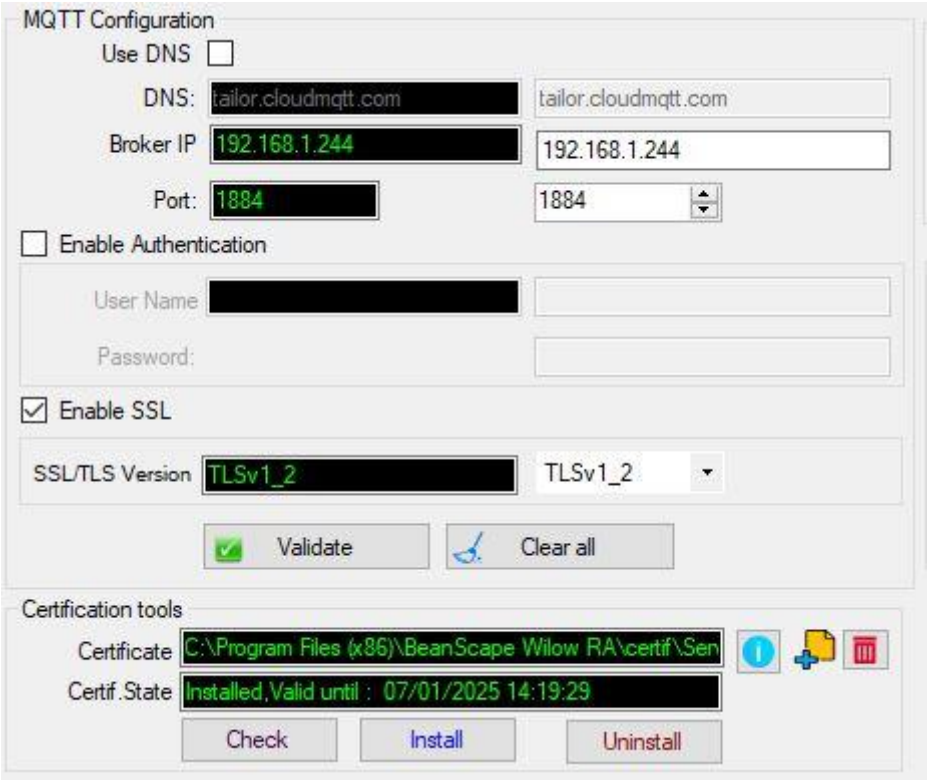


Figure 15 MQTT configuration window

On Beanscape® Wilow®, you can check if your certificate is already installed, if not, click on “install”.

6.3 SSL FOR OTAOP COMMUNICATION

- **Configuration on Beandevice® Wilow® Side**

In this case, the device is the server here and Beanscape is the client. So for server, we need to have two main files: Private key file and server certificate file.

✓ For the private key file, it will be installed only one time into the device (no need to change it over the time, only for extreme security reason).

✓ For the server certificate file is also binary file (*.der format).

These two files are supplied by BeanAir’s team.

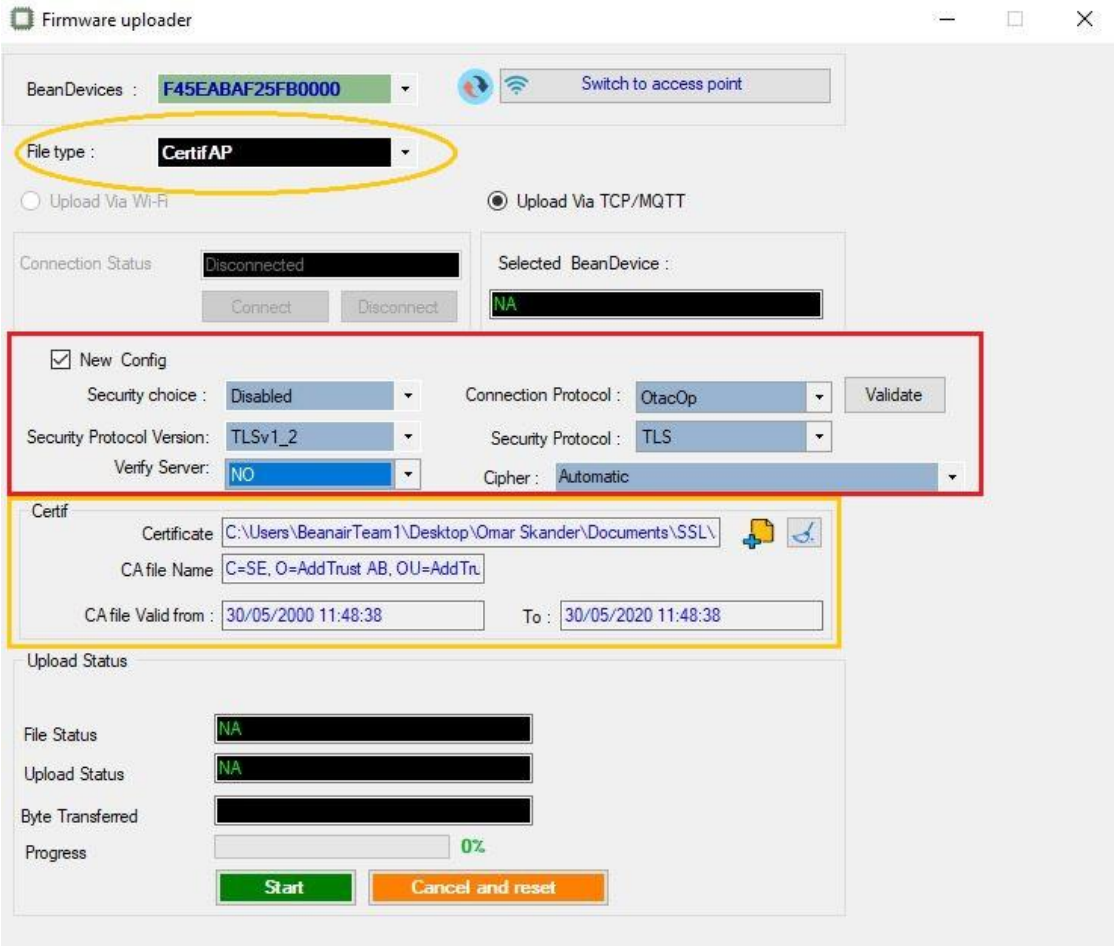


Figure 16 firmware uploader

On Beanscape®, we select the access point (AP) certificate as an option for file to be uploaded to the device, after that we choose the file from the local machine and click start to send file.

Please note it is preferred to not change any configurations related to the secure socket options.

- **Beanscape® Wilow® side**

  The Beanscape® Wilow® is a client in this case, so it needs only the Root certificate file of the device, this file is saved inside Beanscape folders.

6.4 SSL FOR BEANSCAPE® WILOW®

- **Configuration on Beandevice® Wilow® Side**

This is a secure communication for our standard communication between Beanscape and all the devices, the principals are the same here, Beanscape is the server and the devices are clients.

As the device is a client it needs only the Root Certificate of the server, also it must be a binary file before we downloaded into the devices.

- **Beanscape® Wilow® side**

  Like mentioned before, the Beanscape® Wilow® is operating as a server here, so it needs two main things:

  ✓ the server certificate which will be installed inside Beanscape folders.

  ✓ the private key will be also installed in Beanscape folders.

6.5 EXAMPLE OF MQTT BROKER ON TELTONIKA ROUTER (RUT240/RUT950)

For the MQTT communication between Beanscape® Wilow® and the BeanDevice® Wilow®, we can use the hosted broker on Teltonika Router RUT240/RUT950.

Like any kind of MQTT Broker, the router is acting as a server and both Beanscape® Wilow® and BeanDevice® Wilow® are acting as a client.

On the Teltonika broker configuration, we need to follow those steps:

- Enable the broker and specify the port ID ;

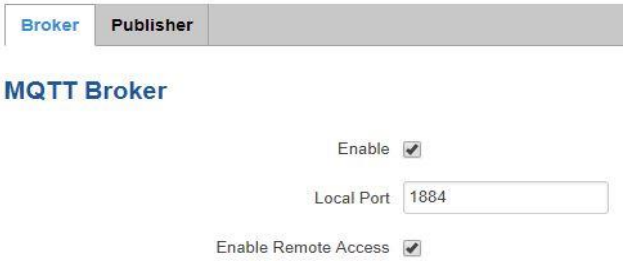


Figure 17 MQTT Broker

- Enable TLS/SSL option and update the 3 files:

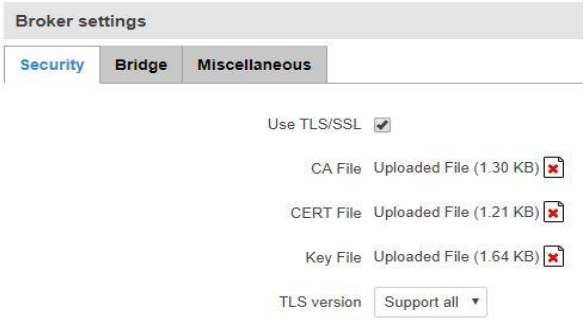


Figure 18 Broker Settings

- ✓ **CA File**: the root CA file of the client, the server may request the client certificate to verify it.
- ✓ **CERT file**: the server certificate
- ✓ **Key File:** the server private key.