

V1.4



TECHNICAL
NOTE

BEANGATEWAY®
REMOTE ACCESS MANAGEMENT



DOCUMENT

Document ID	RF-TN-15	Version	V1.4
External reference		Date	14/06/2022
Author	Fahd ESSID, Application/Support Engineer		
		Project Code	
Document's name	BeanGateway management on a LAN infrastructure		

VALIDATION

Fonction	Destination	For validation	For info
Writer	Fahd Essid	✓	
Reader	Damon Parsy	✓	
Validation	Antje Jacob		✓

DIFFUSION

Fonction	Destination	For action	For info
Reader n°1	Damon Parsy., Application engineer	✓	
Reader n°2	Antje Jacob, Embedded software engineer	✓	

UPDATES

Version	Date	Auteur	Evolution & Status
V1.0	30 /01/2019	Fahd ESSID	First version of the document
V1.1	25/04/2019	Fahd ESSID	Vocabulary update Port Forwarding update VPN/DDNS added Direct PPTP VPN added
V1.2	19/11/2019	YAHYA Bassem	VPN client Update
V1.3	13/04/2021	Seddik ATTIG	Screenshot update Update the FTP section
V1.3.1	16/11/2021	Seddik ATTIG	Links Updated
V1.4	14/06/2022	Seddik ATTIG	Port Forwarding configuration update

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.

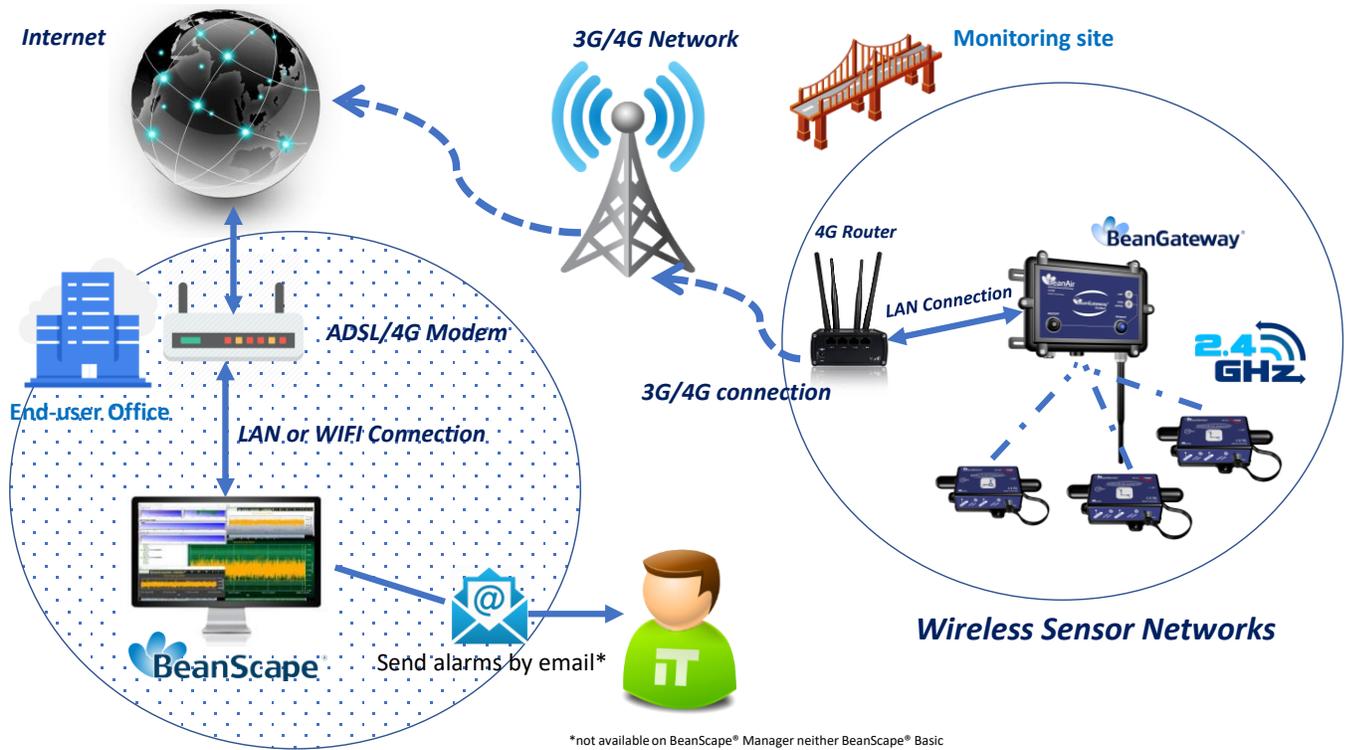
Copyright © Beanair GmbH 2022



- 1. Connection to a 3G/4G Router 6
 - 1.1 Available Remote Access Techniques 7
 - 1.2 Material requirement 7
- 2. How to setup a remote access based on Port Forwarding rules 8
 - 2.1 Step 1: At your office, configure Your Firewall For Remote Access..... 9
 - 2.2 Step 2: At your office, Configure IP forwarding rules 9
 - 2.2.1 Example with ADSL MODEM (NAT ROUTER Configuration) 9
 - 2.2.2 Example of 4G Router (SIM CARD Provider Olivia wireless) 11
 - 2.3 Step 3: At your office, configure the port number on your BeanScape® 18
 - 2.1 Step 4 : BeanGateway® Configuration on the monitoring site 18
 - 2.1.1 Sim card configuration 19
 - 2.1.2 Make sure the DHCP is enabled on your LTE router 20
 - 2.1.3 BeanGateway® 2.4GHz configuration with Public IP of your Office PC 21
- 3. Alternatives of Port Forwarding..... 25
- 4. VPN/DDNS Acces for dynamic IPs 26
 - 4.1 Dynamic DNS..... 26
 - 4.2 PPTP VPN..... 31
 - 4.2.1 PPTP VPN Configuration..... 31
 - 4.2.2 Distant VPN Client Configuration..... 32
 - 4.3 Connecting the BeanGateway to the VPN 37
 - 4.4 BeanScape at the Office 38
 - 4.5 Data Consumption 39
- 5. Direct VPN Access with distant Public Fixed IP 41
 - 5.1 PPTP VPN Configuration 41
 - 5.2 Distant VPN Client Configuration..... 43
 - 5.3 CONNECTING THE BEANGATEWAY TO THE VPN 48**
 - 5.4 BEANSCAPE AT THE OFFICE 48**

5.5	DATA CONSUMPTION	49
6.	FTP Synchronization.....	51
6.1	using BeanScape FTP Feature	51
6.2	Using Third Party FTP Software	54
7.	Troubleshooting.....	57
7.1	How can I Get the IP Configuration on my PC?.....	57
7.2	How can I modify my PC network interface configuration?	57

1. CONNECTION TO A 3G/4G ROUTER



[See "Remote access to a Wireless Sensor Network" Youtube video](#)

1.1 AVAILABLE REMOTE ACCESS TECHNIQUES

The remote access allows you to remotely access to the distant BeanGateway® in the distant site.

The settings can be done using one of the 3 remote access techniques presented by BeanAir®:

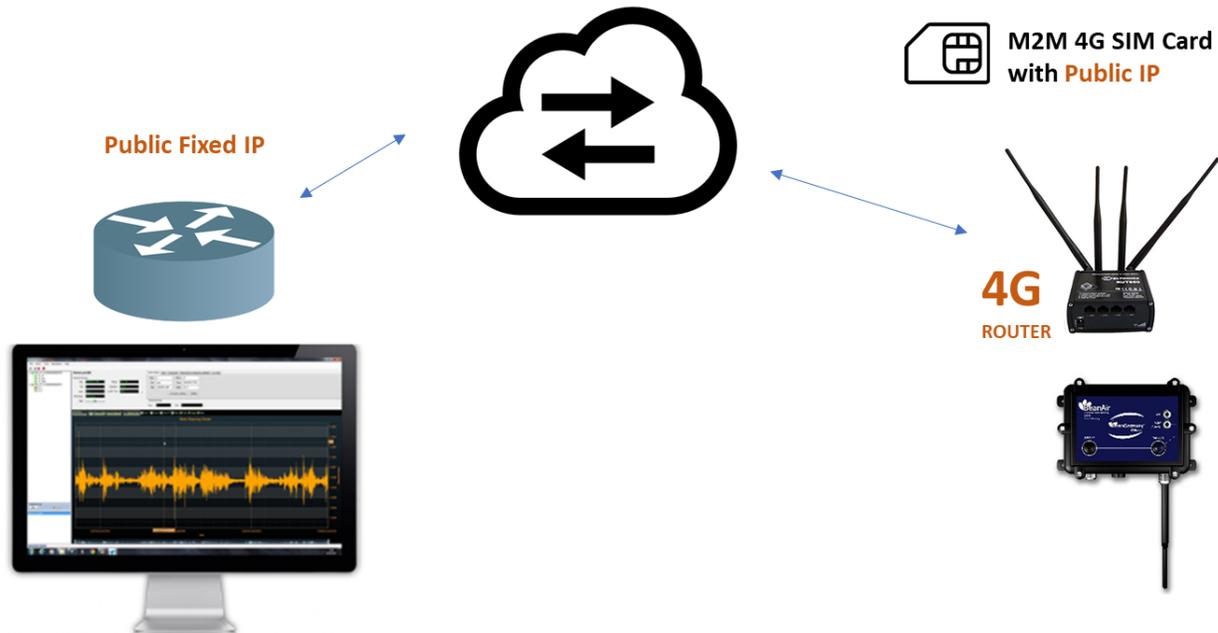
- Port Forwarding
- VPN/DDNS Access
- Direct VPN

User can also synchronize the Log files with an FTP distant folder using an FTP client.

1.2 MATERIAL REQUIREMENT

<i>BeanGateway® version</i>	<i>BeanGateway® Ethernet</i>
<i>4G/3G Gateway</i>	<p><u>TECHNOLOGY</u></p> <ul style="list-style-type: none"> • HSUPA with fallback to: LTE, HSDPA, UMTS, EDGE <p><u>Bands</u></p> <p>Tri-Band UMTS/HSDPA/HSUPA 850, 1900, 2100 MHz Or Quad-Band UMTS/HSDPA/HSUPA 850, 900, 1900, 2100 MHz</p> <p><u>HOST INTERFACES</u></p> <p>Ethernet: 10/100 BASE-T RJ-45</p> <p><u>APPLICATION INTERFACES</u></p> <p>TCP/IP, UDP/IP, DHCP, HTTP, SNMP, SMTP, SMS, MSCI</p>
<i>ADSL Modem</i>	ADSL Modem with NAT Configuration software

2. HOW TO SETUP A REMOTE ACCESS BASED ON PORT FORWARDING RULES



Before to start to configure your remote access, make sure your Office router/ASDL Box should come with Fixed Public IP address to avoid losing the BeanGateway® whenever it reboots for any reason.



How to get a fixed public IP:

- ***If you are using an ADSL Router at your office: you can ask to your ADSL Router provider to allocate you a fixed public IP.***
- ***You can purchase a Data SIM card with fixed public IP from your ISP (Example: Olivia Wireless) . If you are using a standard SIM card, some PORTS can be blocked by the ISP.***



It's not mandatory to use a SIM card with fixed public IP on the monitoring site.

2. Setup a Port Forwarding configuration on your Router (each router brand has its own configuration interface).

Example 1: GlobalNet ADSL Router Webserver configuration (North Africa)

The screenshot shows the GlobalNet router's web interface. On the left is a navigation menu with options like Quick Setup, WAN Setup, NAT, Virtual Servers, Port Triggering, DMZ Host, IP Address Map, ALG/Pass-Through, LAN, Wireless, Parental Control, and Home Networking. The main content area is titled "NAT -- Virtual Servers" and includes instructions: "Select the service name, and enter the server IP address and click 'Apply/Save' to forward IP packets for the same value as 'Internal Port Start'." Below this, there are radio buttons for "Choose All Interface" (selected) and "Choose One Interface". The "Use Interface" dropdown is set to "ppp_usb/ppp3". Under "Service Name", "Custom Service" is selected with "Berlin Remote Access" entered. The "Server IP Address" is "192.168.1.69". A checkbox for "Enable NAT Loopback" is checked. At the bottom, a table shows the configuration:

External Port Start	External Port End	Protocol	Internal Port Start	Internal Port End
5313	5313	TCP/UDP	5313	5313

Example 2 : Fritz Box (Germany)

The screenshot shows the Fritz!Box 7560 web interface. The left sidebar has a menu with "Internet" selected. The main content area is titled "Internet > Permit Access" and has a sub-tab for "Port Sharing". A message states: "All devices connected with the FRITZ!Box are safe from unauthorized access from the internet. However, certain applications (like online games) must be accessible for other users in the internet. By configuring port sharing you can allow such connections." Below this is a table with columns: Device / Name, IP Address, Sharing, Port Assigned Externally IPv4, Port Assigned Externally IPv6, and Independent Port Sharing. One device is listed: "DESKTOP-TNL8T5I" with IP "192.168.178.61" and "port" sharing, with "5313" assigned externally. The "Independent Port Sharing" checkbox is disabled. At the bottom, there are "Apply" and "Cancel" buttons.



Please be aware if the public IP Address of your ADSL Box is not fixed, you will lose the connection between the BeanGateway® and your Monitoring PC (at the office), whenever the router reboots. If you are not sure to have a fixed public IP, we suggest you use a 4G Router and a SIM Card with a fixed public IP.

2.2.2 Example of 4G Router (SIM CARD Provider Olivia wireless)



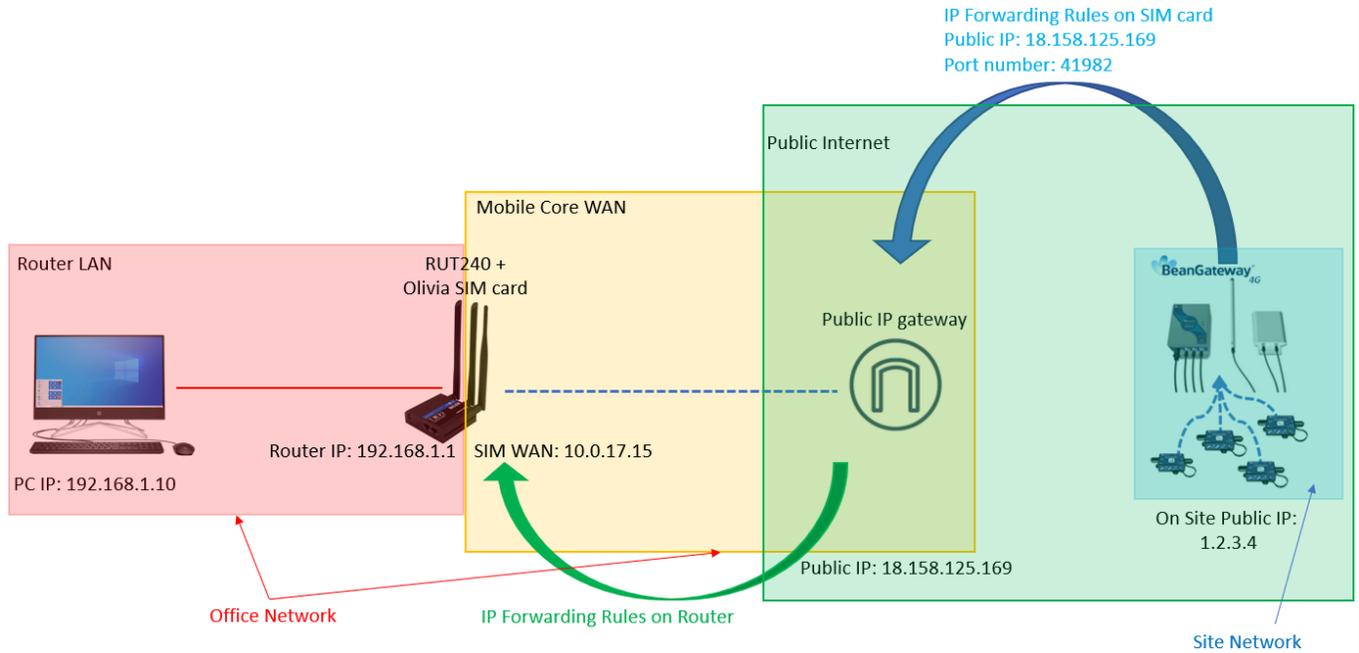
if you have a 4G router with a SIM card at your office, make sure that the SIM card comes with a Fixed Public IP address and your ISP provider doesn't restrict any port numbers.

In this example we will work with Olivia Wireless SIM card which comes with a Fixed public IP address.

2.2.2.1 System Architecture

Olivia is using a Public Gateway in its system architecture, in order to allow users on the internet to reach the SIM directly.

The Public Gateway is simply a port forward service that's why you have to create a port forwarding rules on both **SIM Card platform** and also on **your office router**.

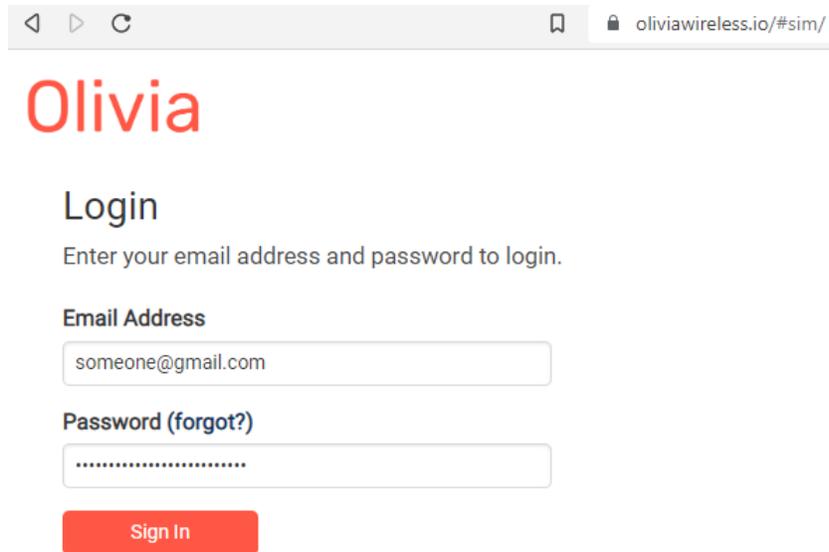


Please follow these steps to correctly configure the system.

- **Step 1: Verify that Public IP routes service is enabled on your SIM card**

We assume that you have already purchased the Fixed public IP service when you set up the payment method.

To verify that the Fixed Public IP address service is enabled, please login to your SIM Card platform



Then go to the tab SIM Cards.

Olivia

[Dashboard](#)
[SIM Cards](#)
[Support](#)
[Order SIM cards](#)
[My Company](#)
[Help](#)

Logged in as

[+ Register SIM card](#)

Registered SIM Cards

search by keyword search

[Export](#)

SIM Barcode	Device Name	SIM State	APN	Rate plan	Activation Date	Data Used
891030000001886354	Test_SIM-CARD	Active	rh	Selfservice SIM	03/06/2022	150MB

You should see “Public IP Route” noted under “Deployed Network Service” on the SIM cards details page.

Expiration Date

03/06/2023

Deployed Network Service

Public IP Route

If it's not the case you have to enable it before proceeding.

- **Step 2: Setup Port Forwarding on the Public IP Gateway (SIM Card)**

Navigate to “SIM card” and click on the SIM barcode

Olivia

[Dashboard](#)
[SIM Cards](#)
[Support](#)
[Order SIM cards](#)
[My Company](#)
[Help](#)

[+ Register SIM card](#)

Registered SIM Cards

search by keyword search

[Export](#)

SIM Barcode	Device Name	SIM State
891030000001886354	Test_SIM-CARD	Active

Then click on ADD Public IP Route

Top-ups

Order ID

No top-ups available

[Add Public IP Port Route](#)

Inbound access via fixed IP

- Give your route a recognizable name, Enter the port you would like to reach on the SIM/Router then select the protocol (usually TCP) and click 'Submit'.
- Create the PORT ID of your SIM card (**avoid ports 22, 80 and 443**)

Add Public IP Port Route

Add Route

Route Name *

Berlin Site

Port SIM Side *

5320

Transport layer *

TCP

Submit

A random port on the gateway will now be locked to be used with your SIM card

Routes Name	SIM IP	Port SIM Side	Public IP:Port	Delete
Berlin Site	10.0.17.15	5320	18.158.125.169:41988	

**IMPORTANT :**

- The PORT ID of your SIM card will be used to create the IP Forwarding rules on your LTE Router running at the office.
- *Note the Public IP and the PORT number, it will be used during your BeanGateway® configuration on your monitoring site.*
- **Install the SIM Card on the router and Configure the Mobile Network**

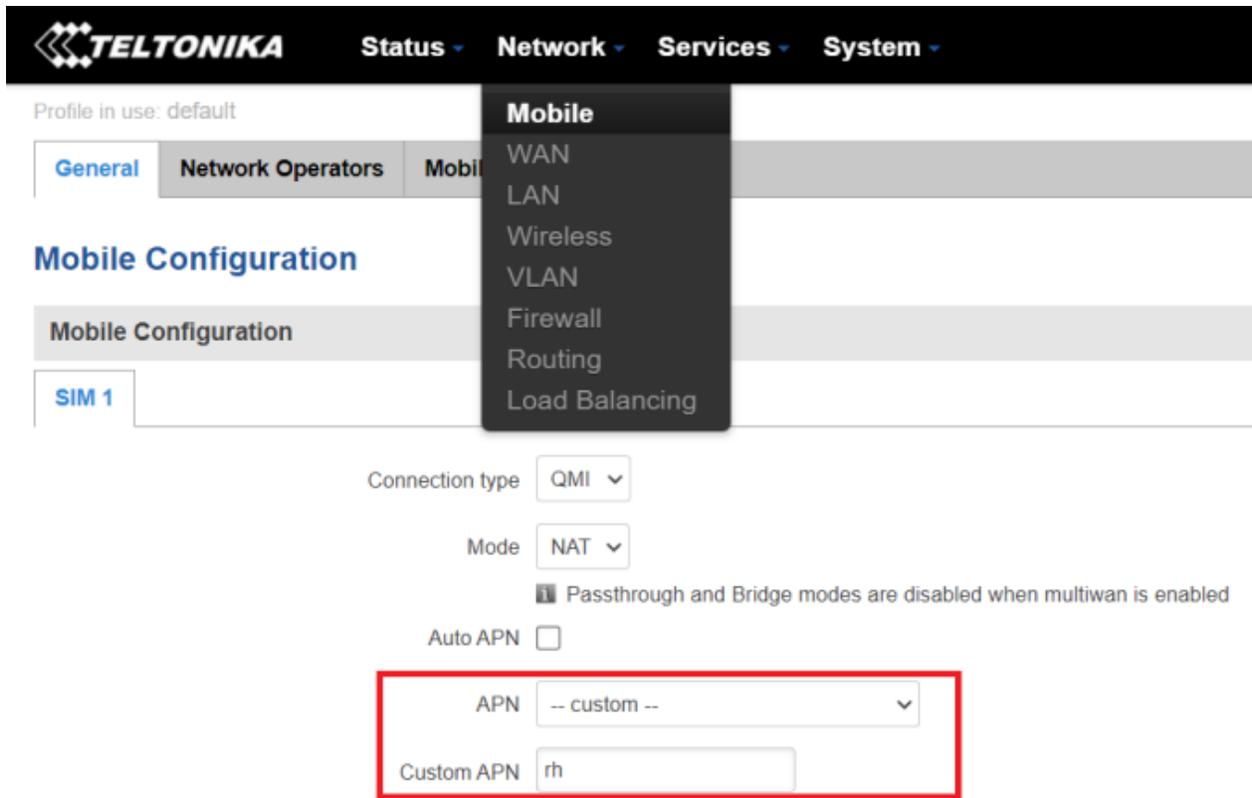
In this example we are using Teltonika Router RUT240, but the steps are similar for different types of routers.

Insert the SIM Card into your Router then use the corresponding User Name and Password to log in.

Then Navigate to Network → Mobile, then Enter the following configuration

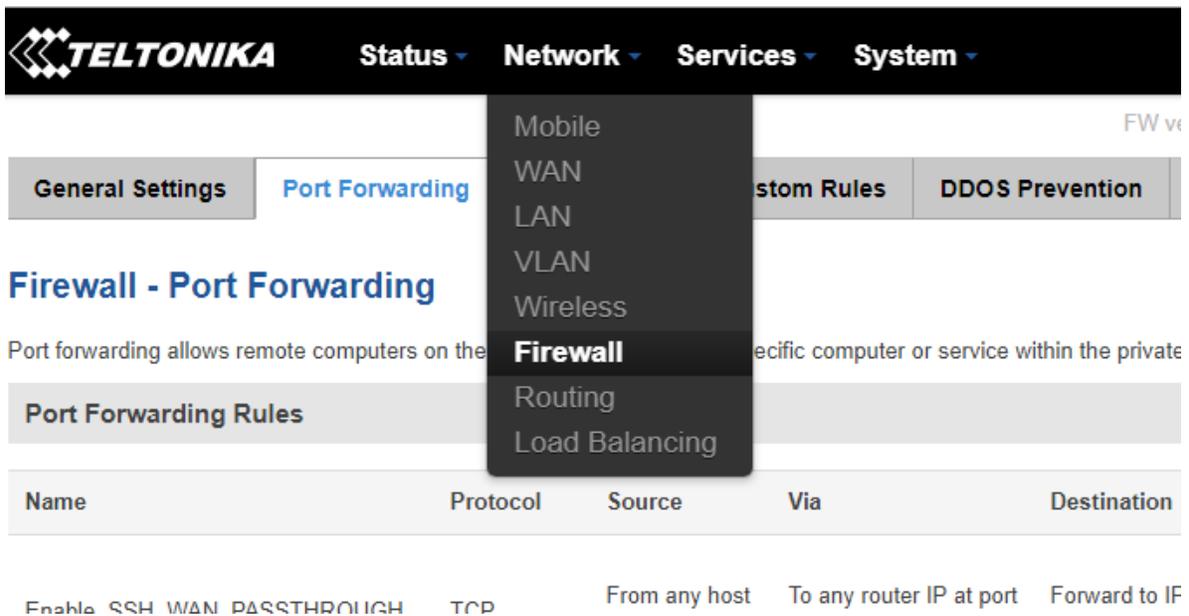
- APN: --custom--
- Custom APN: rh

And Keep all the other settings on default then click on save.



- **Step 4: Setup Port Forwarding on the router**

Login to your router, then navigate to Network → Firewall → Port Forward



Scroll down to New Port Forward Rule and set the following

- Name: Any recognizable name
- Protocol: **TCP+UDP**
- **External port (s): [SIM Card PORT ID](#) in our case **5320 (avoid ports 22, 80 and 443)****
- Internal IP: Select the IP of your PC
- **Internal port (s):** Any port on which you want to access (Port used on BeanScope software) **5313**

NAME Forward	EXTERNAL PORT 5320	INTERNAL IP ADDRESS 192.168.1.31 (00:23:24:73:87:67)	INTERNAL PORT 5313
-----------------	-----------------------	---	-----------------------

You can click on **edit** to see the configuration details.



Make sure that the port forwarding rule is configured from WAN: External Port (or Source Zone) to LAN: Internal Port.

Not secure | 192.168.1.1/cgi-bin/luci/stok=34c94d9c527a193eb4e90d1093ed09fc/admin/network/firewall/forwards/cfg383837

TELTONIKA Status Network Services System Logout

Profile in use: default FW ver.: RUT2XX_R_00.01.13.1

General Settings **Port Forwarding** Traffic Rules Custom Rules DDOS Prevention Port Scan Prevention Helpers

Firewall - Port Forwards - Forward

This page allows you to change advanced properties of the port forwarding entry. Although, in most cases there is no need to modify those settings.

Enable

Name

Protocol

Source zone

- gre: gre tunnel:
- hotspot:
- l2tp: l2tp:
- lan: lan:
- pptp: pptp:
- sstp:
- vpn: openvpn:
- wan: wan: ppp: tun: (empty) wan2:

Source MAC address

Source IP address

Source port

lztp: lztp:

 lan: lan:

 pptp: pptp:

 sstp:

 vpn: openvpn:

 wan: wan: ppp: tun: (empty) wan2:

Internal IP address

Internal port

Enable NAT loopback

Extra arguments

2.3 STEP 3: AT YOUR OFFICE, CONFIGURE THE PORT NUMBER ON YOUR BEANSCAPE®

On your office PC don't forget to put the BeanScope TCP port number the same as the internal Port TCP number chosen in the router port forwarding configuration rule.

NAME

BeanScope Configuration

Log

Keep Alive App

TCP/UDP

System

INTERNAL PORT

BeanGateway configuration via Udp :

 Udp port :

 Tcp port to listen :



If you change the default TCP port on BeanScope software to another port number different than 5313, you have to restart the server to establish the connection with the monitoring site.

2.1 STEP 4 : BEANGATEWAY® CONFIGURATION ON THE MONITORING SITE

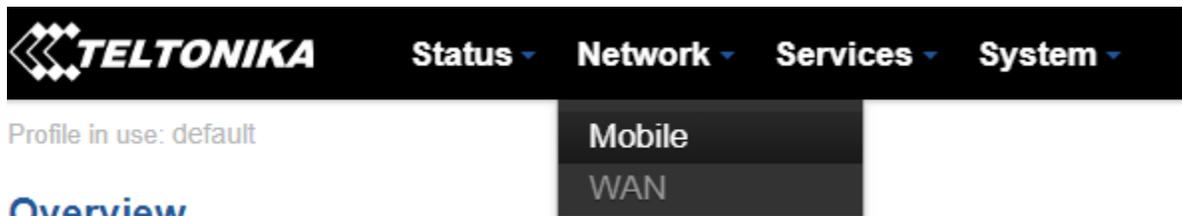
Now that you have your Public Fixed IP of your BeanScope® software running at your office. You can start to configure your BeanGateway® and LTE Router running on the monitoring site.

2.1.1 Sim card configuration

Use your browser on your PC and log in to the router using the following settings:

- IP address: **192.168.1.243** (tap it in google search bar)
- Username: **admin** | password: **Beanair2020!**

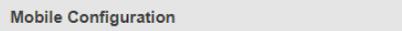
To configure your 4G/LTE Router go on **Network** then Click on **Mobile**



Now configure your mobile settings as follow



Mobile Configuration



Choose QMI connection type because PPP is slower than QMI. **QMI option is highly recommended.**

Check Auto APN and the connection will be established automatically. **Access Point Name (APN):** is a configurable network identifier used by a mobile device when connecting to a GSM carrier

Enter the right PIN number and PUK code of your SIM card

Used this field only if the SIM card's PIN number was used

Choose 1500

Choose Automatic as a service mode

Uncheck Deny data roaming option

Mobile Configuration

SIM 1

Connection type: QMI

Mode: NAT

ⓘ Passthrough and Bridge modes are disabled when multiwan is enabled

Auto APN: Connection will be established automatically

PIN number: 0000

PUK code:

Dialing number: *99#

MTU: 1500

Service mode: Automatic

Deny data roaming:

Mobile Data On Demand	
Enable	<input checked="" type="checkbox"/>
No data timeout (sec)	<input type="text" value="10"/>
Force LTE network	
Enable	<input checked="" type="checkbox"/>
Reregister	<input type="checkbox"/>
Interval (sec)	<input type="text" value="300"/>
<input type="button" value="Save"/>	



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.

2.1.2 Make sure the DHCP is enabled on your LTE router

LAN IP address should be 192.168.1.243 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

Local Network  	
IP / netmask	<input type="text" value="192.168.1.243 / 255.255.255.0"/>
Clients connected	3

TELTONIKA

[Status](#) [Network](#) [Services](#) [System](#) [Logout](#)

LAN

Configuration

General Setup

Advanced Settings

IP address

IP netmask

IP broadcast

DHCP Server

General Setup

Advanced Settings

DHCP

Start

Limit

Lease time

Start IP address: 192.168.1.100

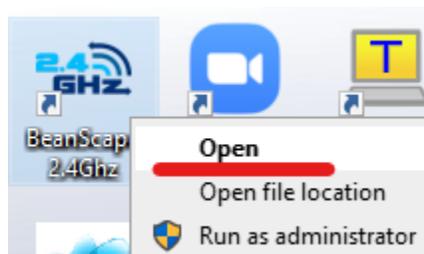
End IP address: 192.168.1.242

2.1.3 BeanGateway® 2.4GHz configuration with Public IP of your Office PC

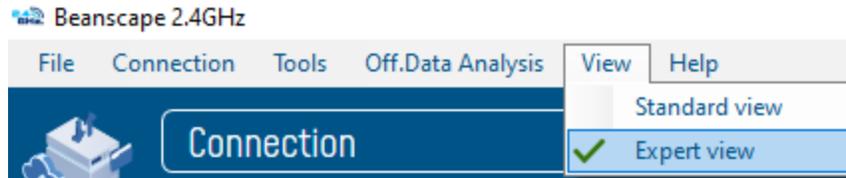
Now that your LTE Router is configured with your SIM card, it's time to configure correctly your BeanGateway® 2.4GHz.

Right after connecting your BeanGateway® 2.4GHz to your PC via the LAN cable,

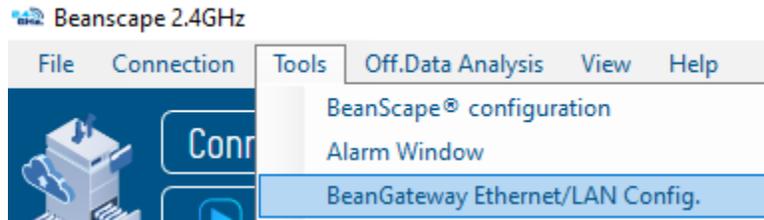
1. Right click on your BeanScape® software icon then click on [Open](#)



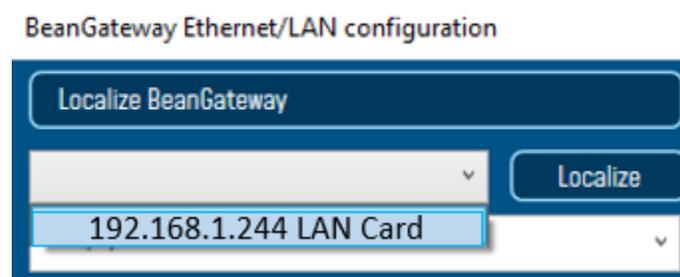
2. Switch to Expert view



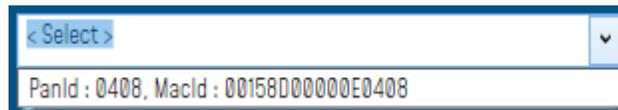
3. Navigate to Tools → BeanGateway Ethernet/LAN config



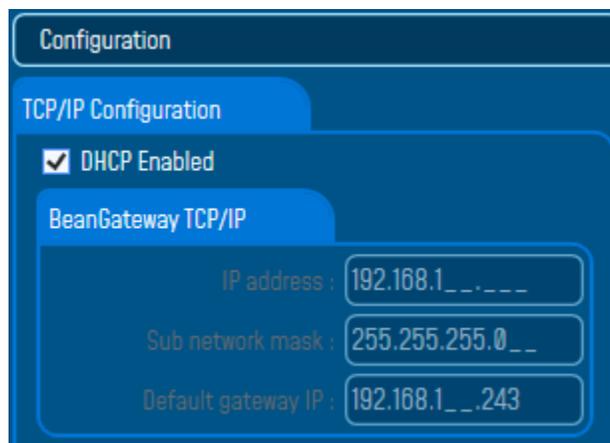
4. Select your LAN card IP Address (192.168.1.244), then click on Localize



5. After Localization process, select your 4G BeanGateway® MAC ID



6. Check DHCP option to assign an automatic IP address to your BeanGateway®, then click on validate



7. On BeanScape® frame:

- **Case 1 - If you are using a ADSL Router at your office**

Make sure to allocate the Public IP of the PC Hosting BeanScope software (you will get your Public IP from step 2) . In this case the Public IP is 188.106.107.201

Case 2 - If you are using a LTE Router with a Data SIM CARD (example of Olivia Wireless SIM CARD)

To forward data communication of your BeanGateway® to your Office PC, enter the **Fixed Public IP address which was created on the SIM Card before and its corresponding TCP Port number.**

Example of IP forwarding Rules created on the Router

Routes Name	SIM IP	Port SIM Side	Public IP:Port	Delete
Berlin Site	10.0.17.15	5320	<u>18.158.125.169:41988</u>	

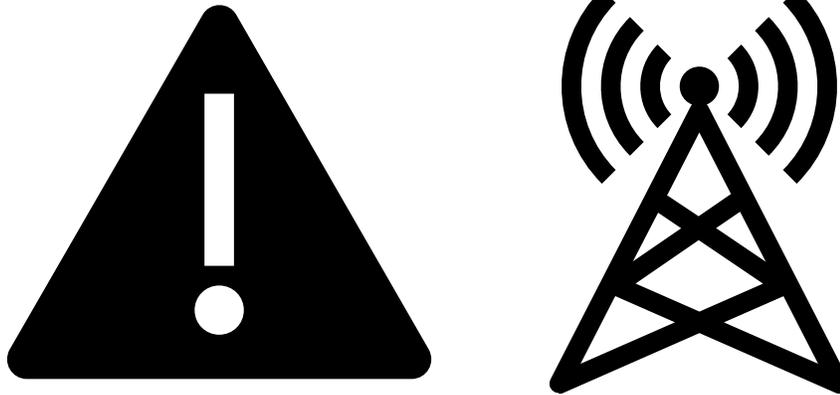


Make sure to use the Fixed Public IP address and the TCP Port number which are created on the SIM Card rule.

Do Not use Google to search for your Public IP address, it will give you the IP address of the roaming ISP provider and the remote configuration will not work.

3. ALTERNATIVES OF PORT FORWARDING

In some customer cases, user do not have access to a Public Fixed IP address, or he is meeting a timeout issue due to his SIM provider network.



It is recommended to use a Dynamic DNS/PPTP VPN based solution or a direct VPN access via Fixed Public IP

Case of Dynamic IPs	Case of Time out issues
3.PPTP VPN based on DDNS	4.Direct PPTP or LT2P VPN access

For users who prefer to transfer BeanScape Log Files via FTP

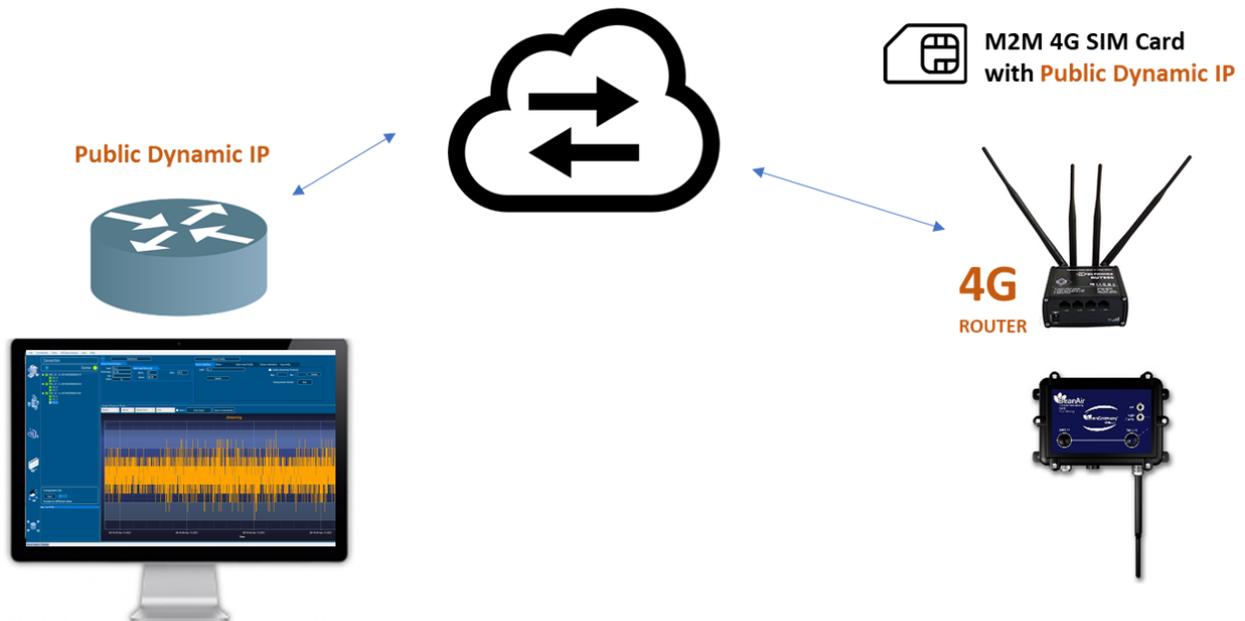
Please select

[5.FTP Synchronization](#)

4. VPN/DDNS ACCES FOR DYNAMIC IPS



This solution is recommended for users who are facing the issue of the Dynamic Public IP on the both side of the infrastructure.



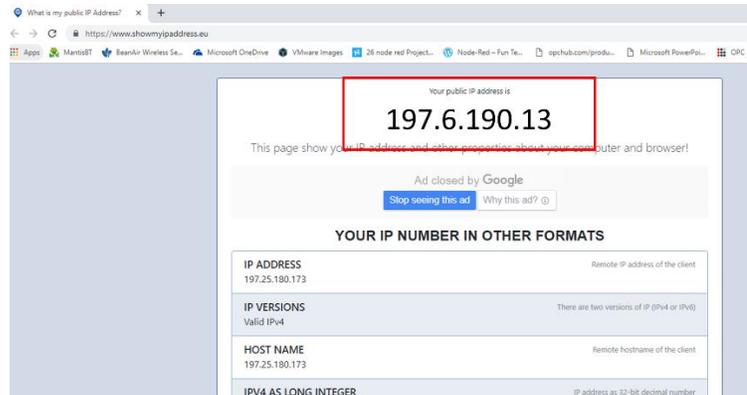
4.1 DYNAMIC DNS

Dynamic DNS (DDNS or DynDNS) is a method of automatically updating a name server in the Domain Name System (DNS). This is most often utilized when the end user has a **Public dynamic IP address** and wants to bind it to a static hostname.

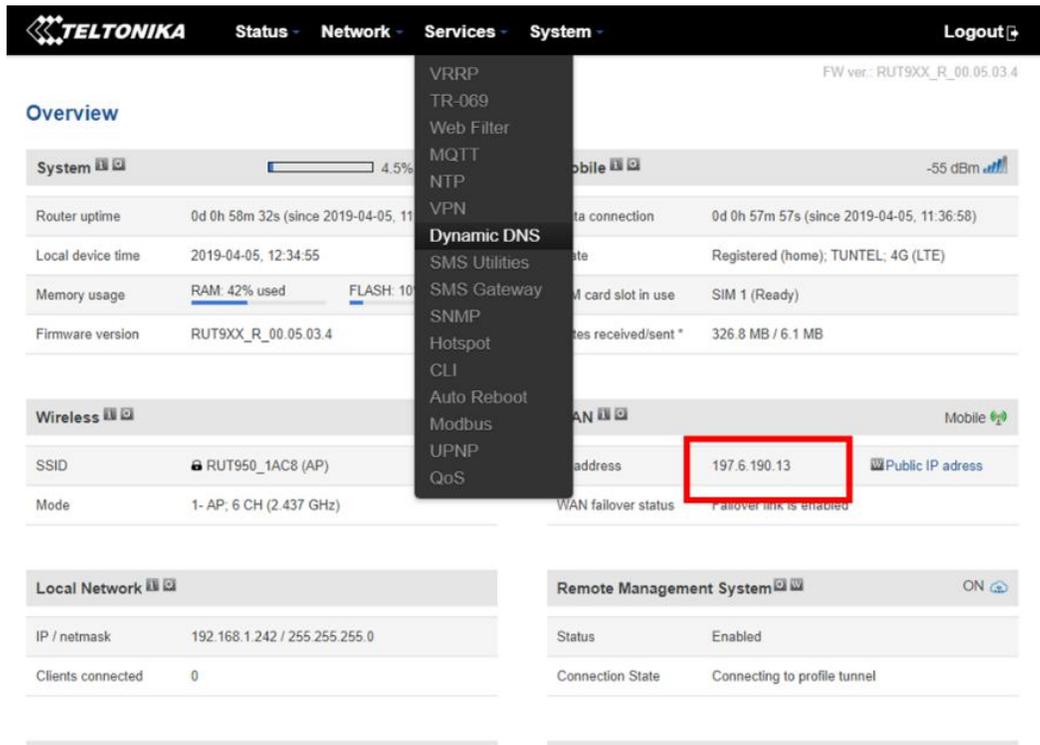
The DDNS configuration will be done on both 4G Router and the NoIP DDNS provider dashboard.

Make sure that you are using a SIM card connecting assigned to a public IP address otherwise the DDNS will not work

- Open your web browser and go to <https://www.showmyipaddress.eu/> to display your Public IP



- Connect to your 4 G Router Web User Interface and check if the Assigned IP to your Router is a Public IP and is the same as mentioned on <https://www.showmyipaddress.eu/>



- Go to the Dynamic DNS option, and create a new DDNS name

DDNS

DDNS Configuration

DDNS name	Hostname	Status	Enable
No DDNS records found.			

New configuration name:

- Click on Edit or enter to advanced configuration

TELTONIKA Status Network Services System Logout FW ver.: RUT9XX_R_00.06.00

New DDNS instance created successfully. Configure it now

DDNS

DDNS Configuration

DDNS name	Hostname	Status	Enable
DDNSname	mypersonaldomain.dyndns.org	N/A	<input type="checkbox"/>

New configuration name:

- Go to a No Ip DDNS provider and create an account then create a hostname. In our example we are using www.noip.com.
- It is recommended to use ddns.net as a Domain for the DDNS

Hostname

Domain

Record Type
 A

- The www.noip.com will detect automatically your Public IP. Make sure that you are connecting using your 4G Router during the configuration, otherwise you have to add the Public IP manually.

teltonikademo.ddns.net Expires in 28 days	Apr 5, 2019 03:37 PDT	197.6.190.13	A	Modify
--	--------------------------	--------------	---	--------

Mobile	
Address	197.6.190.13 Public IP address
failover status	Failover link is enabled
Remote Management System	
ON	

- On the 4g Router side, on the advanced setting of the DDNS
 - Enable the DynDNS
 - Select the service provider from the list (in our case no-ip.com)
 - Insert your Hostname which was create on the DDNS provider website, your login used to connect to the DDNS provider website and the password
 - The IP address source should be Public
 - Configure the IP renew interval to 5 minutes and the Force IP renew to 6 minutes

TELTONIKA

[Status](#)
[Network](#)
[Services](#)
[System](#)
[Logout](#)

DDNS

Enable

Use HTTP Secure

Status 2019-04-05, 11:37:45

Service

Lookup host

Hostname

User name

Password

IP address source

Public, Private, Custom or Script IP source setting, will disable DNS rebinding protection

URL to detect

IP renew interval

IP renew interval unit

Force IP renew

Force IP renew unit

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

- Click on save and wait until the router establish connection, once the Status displays the date and the time that's means that the configuration is accepted.

DDNS

DDNS Configuration

DDNS name	Hostname	Status	Enable	
DDNSname	teltonikademo.ddns.net	2019-04-05, 11:37:45	<input checked="" type="checkbox"/>	Edit Delete

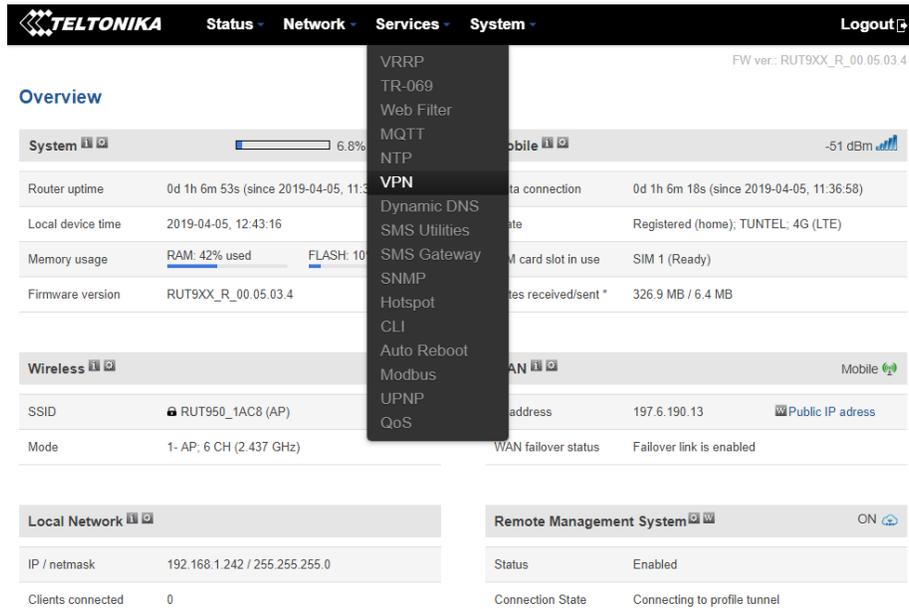
New configuration name: [Add New](#)

[Save](#)

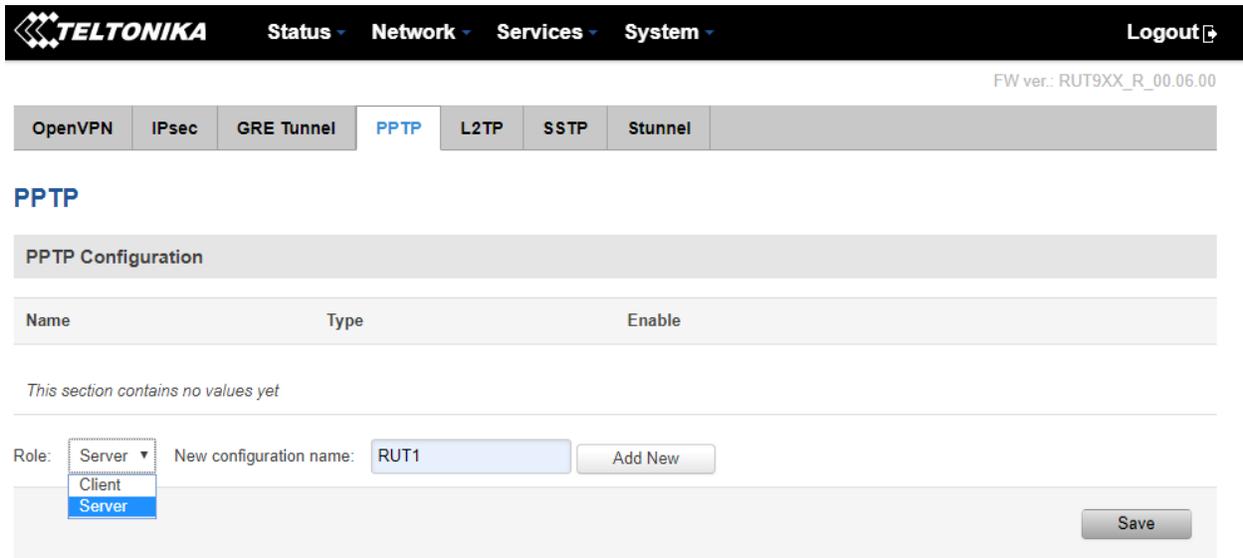
4.2 PPTP VPN

4.2.1 PPTP VPN Configuration

- On the same 4G Router hosting using the DDNS, Go to the VPN menu option



- Select to Go with a PPTP VPN and create a new Server.



- On the advanced option:

- Enable the PPTP VPN Server
- Configure the VPN IP Pool: It is recommended that you serve maximum 2 addresses
- Create username and a password for the VPN Client
- Assign to the user the first IP address of the VPN IP Range

TELTONIKA Status Network Services System Logout

FW ver: RUT9XX_R_00.05.03.4 | [FW update available](#)

OpenVPN IPsec GRE Tunnel **PPTP** L2TP SSTP Stunnel

PPTP Server Instance: RUT1

Main Settings

Enable

Local IP

Remote IP range start

Remote IP range end

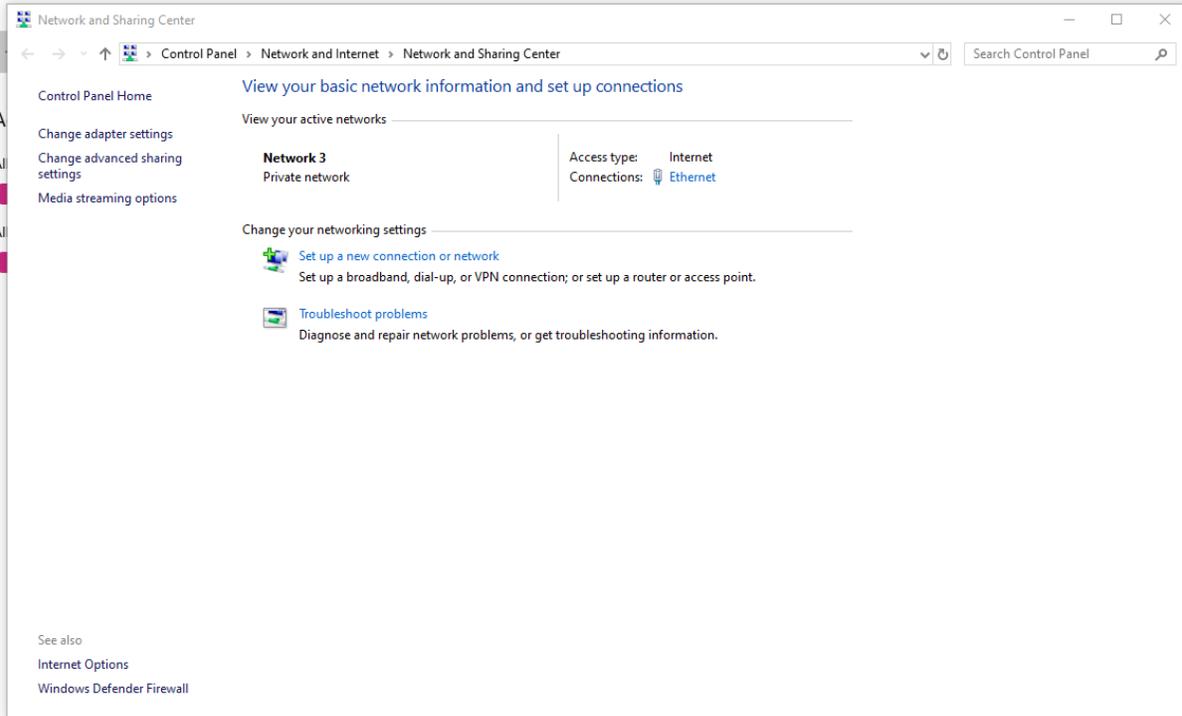
User name	Password	PPTP Client's IP	
<input type="text" value="user1"/>	<input type="password" value="....."/>	<input type="text" value="192.168.0.20"/>	<input type="button" value="Delete"/>

4.2.2 Distant VPN Client Configuration

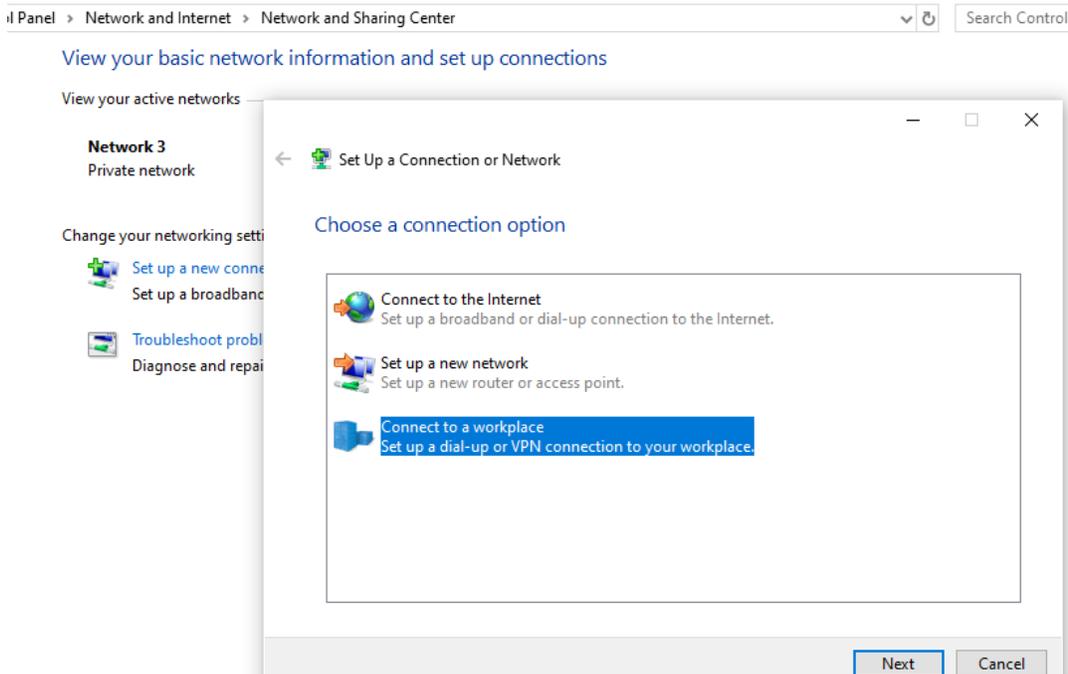
The VPN client is the distant computer situated on the office. User should configure a VPN connection to have access to the VPN server hosting his BeanGateway®.

- Go to Network and Sharing center (Network share center in Windows 7)
- Select Set up a new connection or network

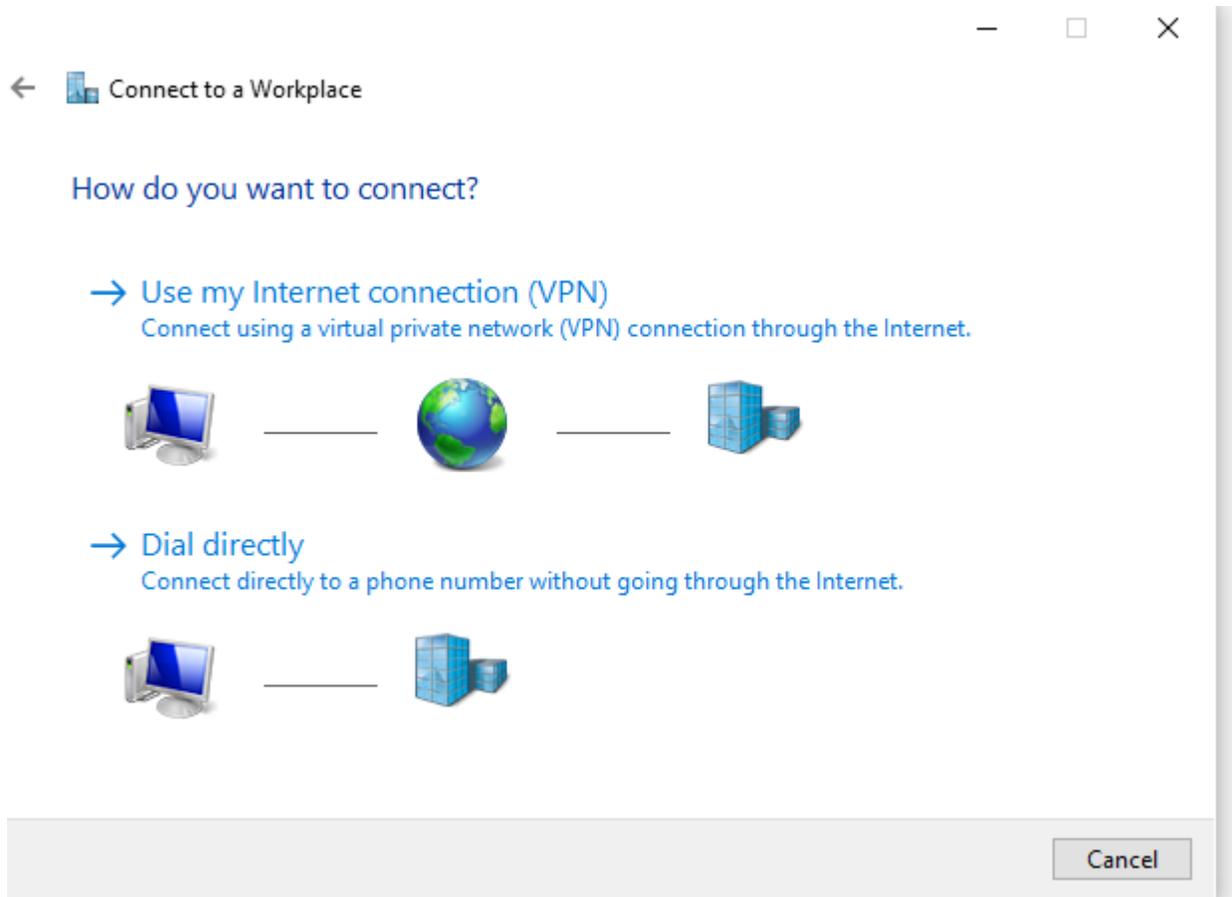
VPN



- Select Connect to a workplace



- Select Use my internet connection (VPN)



- Use the following inputs to configure the VPN connection
 - The name of the VPN server
 - The DDNS name assigned or your Public IP

←  Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

Destination name:

Use a smart card

Remember my credentials

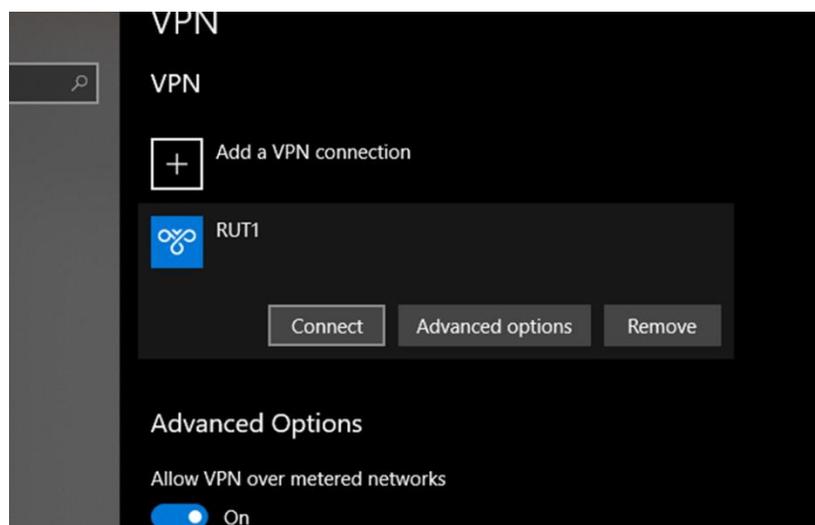
 Allow other people to use this connection

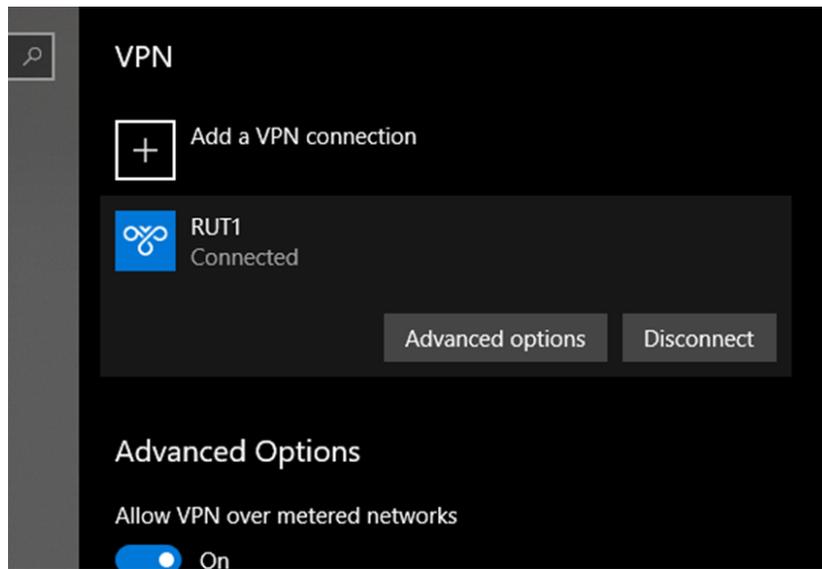
This option allows anyone with access to this computer to use this connection.

Create

Cancel

- The Computer is ready to join the VPN: Press connect





- Using IP config, user can figure out that he is connected to the VPN

```
Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

Connection-specific DNS Suffix  . :
Link-local IPv6 Address . . . . . : fe80::d58d:cc35:7284:709d%7
IPv4 Address. . . . . : 192.168.1.245
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

PPP adapter RUT1:

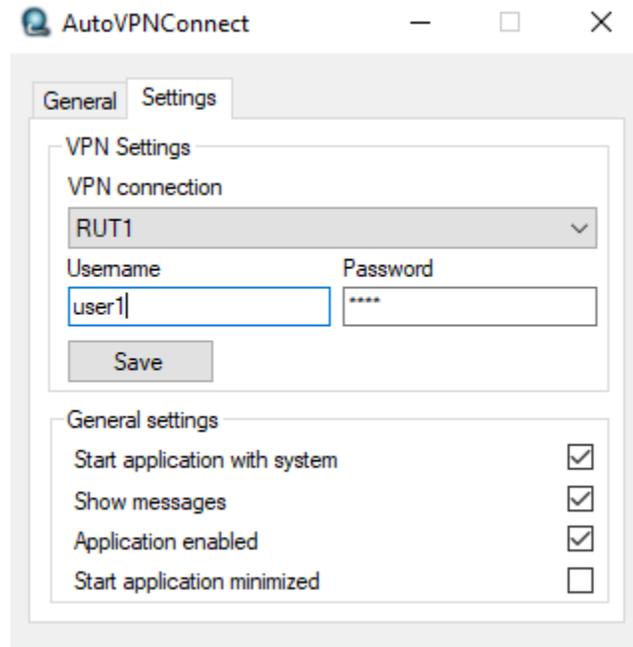
Connection-specific DNS Suffix  . :
IPv4 Address. . . . . : 192.168.0.20
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 0.0.0.0

Wireless LAN adapter Wi-Fi:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

C:\Users\TechSupport>
```

- Windows10 has removed the Auto Redial from the VPN connection, make sure that you Install AutoVPNconnect software after finishing the VPN configuration:
<https://sourceforge.net/projects/autovpnconnect/>



4.3 CONNECTING THE BEANGATEWAY TO THE VPN

- Connect your laptop to the 4G Router used to connect the BeanGateway
- Run BeanScape® 2.4 GHz
- Go to Tools > BeanGateway Ethernet/LAN configuration
- Localize your BeanGateway
- Assign to the BeanGateway a Local Static IP (example 192.168.1.xx)
- On the BeanScape Frame, put the VPN first IP address assigned to the VPN client which was in our example 192.168.0.20

BeanGateway Ethernet/LAN configuration

Localize BeanGateway

192.168.1.27 LAN Card Localize

MacId : 077D, MaclId : 00158D000000E077D

Configuration

TCP/IP Configuration

DHCP Enabled

BeanGateway TCP/IP

IP address : 192.168.1___.250

Sub network mask : 255.255.255.0__

Default gateway IP : 192.168.1___.1__

DNS Enabled DNS IP AUTO

DNS

IP address : _____

BeanScope

Port : 5313

IP address : 192.168._0_._.20

Domain name : _____

Keep Alive App Config

enabled :

KAA timeout (ms) : 15000

KAA interval (ms) : 4000

Max. retry nbr : 7

Validate

Configuration via Ethernet (UDP)

enabled :

Udp port : 53130

Validate

Validate Close

4.4 BEANSCAPE AT THE OFFICE

Once connected to the VPN, run the BeanScope® and click on Start the Server.

The BeanScope will display the BeanGateway profile.

Open the BeanScope Server Window, you can figure out that BeanGateway flow is coming from the VPN server 192.168.0.1

The screenshot displays the Beanscape 2.4GHz software interface. The main window is titled "Beanscape 2.4GHz" and includes a menu bar with "File", "Connection", "Tools", "Advanced func.", "Off.Data Analysis", "View", and "Help".

Connection: A "Started" indicator with a green light is shown. A tree view on the left lists MAC IDs and their corresponding O_n (X, Y, Z) coordinates.

BeanDevice system profile: This section contains several configuration fields:

- Identity:** Mac Id: 0015800000E1049, Site Id: MAC_ID - 0 x 0015800000E1049, Pan Id: 0770, Net Id: 0002, Platform: AX 30.
- Version:** Hard. vers.: V1R4, Soft. vers.: V7R6.
- Datalogger:** Status: Ready.
- BeanDevice Remote Config. Status:** Pending, Sent (highlighted), Deleted.
- Current data acq. mode:** DAQ Status: Stopped, Data Acq. mode: NA, Data Acq. cycle: NA, Sampling rate: NA, Data Acq. duration: NA.

BeanScope Server: A separate window displays a table with columns ID, PAN_ID, and IP. The table contains one entry: ID 7, PAN_ID 3A17, IP 192.168.0.1. Below the table is a log window showing repeated messages: "The site record found successfully in the UserCustomDB".

Data acquisition mode configuration: This section includes:

- Data Acq. mode: LowDutyCycle (dropdown), Start (green button), Stop (red button).
- Data Acq. cycle: ---:--:-- (dropdown), ddd.hh:mm:ss (input).
- Data acquisition mode options: Tx Only (selected), Log Only, Tx & Log.

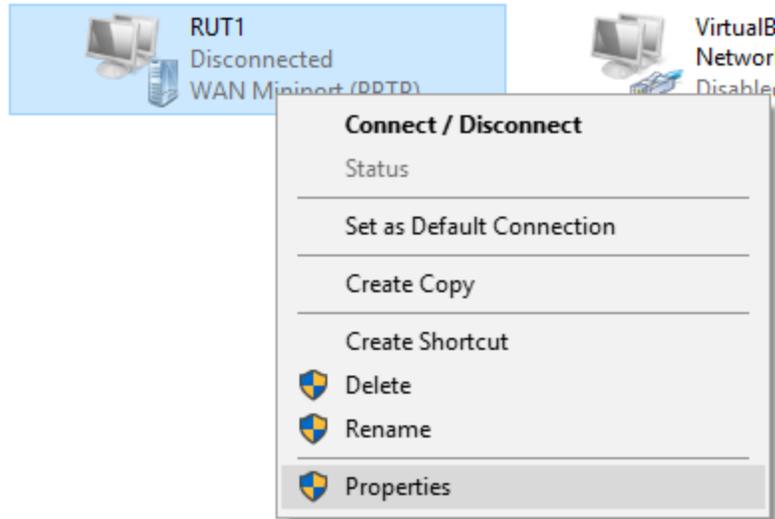
Component List: A section with "Sort", "+", and "-" buttons, and the text "Access to different sites". Below it, "Site: 0 x 0770" is listed.

At the bottom left, the status "Server status: Started" is displayed.

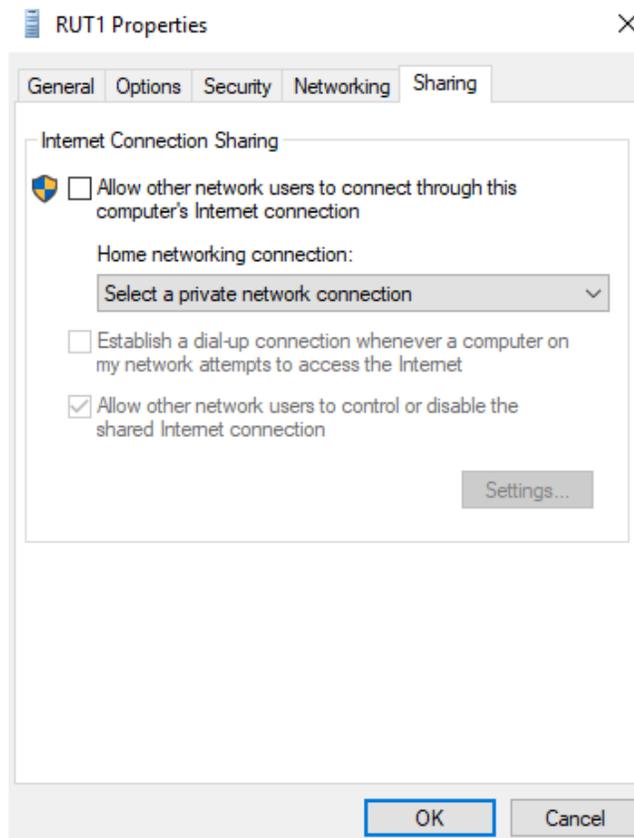
4.5 DATA CONSUMPTION

It is important to mention, That VPN can be used also to connect to internet, so it is important to make sure that this option is disabled on the VPN client proprieties.

Go to Control Panel > Network and sharing center > Change adapter settings and select the VPN Client proprieties



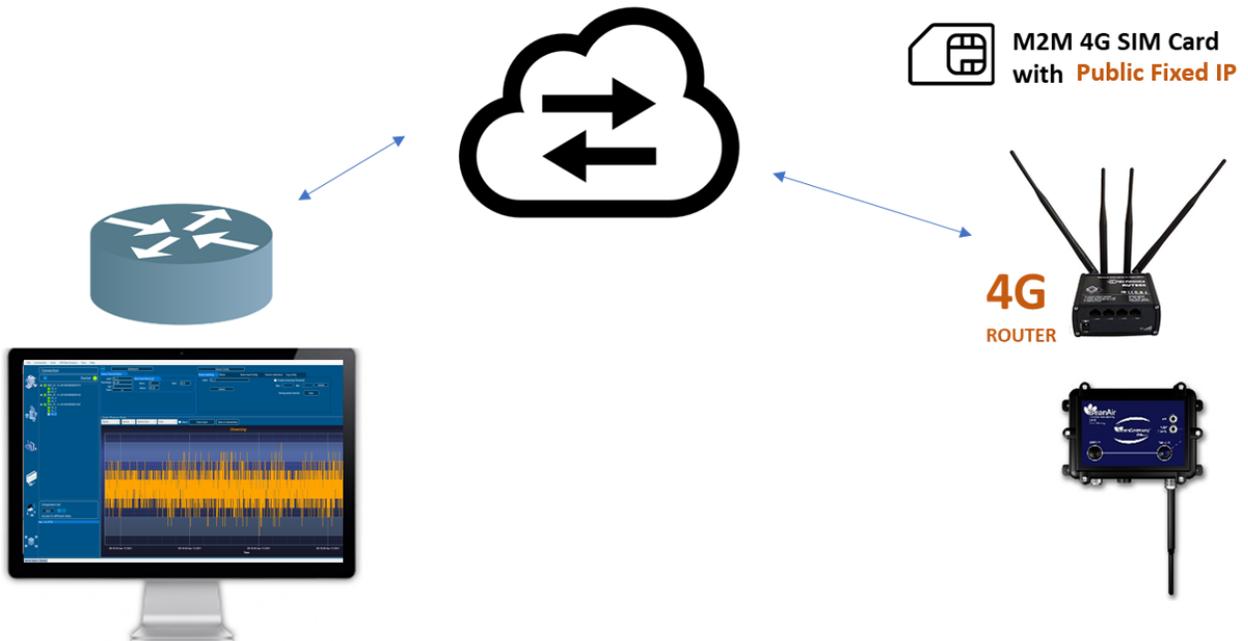
On the Sharing tab, make sure that the option is unchecked



5. DIRECT VPN ACCESS WITH DISTANT PUBLIC FIXED IP



This solution is recommended for users having fixed public IP used for the 4G router used to connect the BeanGateway.



5.1 PPTP VPN CONFIGURATION

- On the 4G, Go to the VPN menu option

The screenshot shows the Teltonika web interface. At the top, there are navigation tabs: Status, Network, Services, and System. The 'Services' menu is open, showing options like VRRP, TR-069, Web Filter, MQTT, NTP, VPN (highlighted), Dynamic DNS, SMS Utilities, SMS Gateway, SNMP, Hotspot, CLI, Auto Reboot, Modbus, UPNP, and QoS. The background displays system information such as Router uptime (0d 1h 6m 53s), Local device time (2019-04-05, 12:43:16), Memory usage (RAM: 42% used, FLASH: 10%), and Wireless settings (SSID: RUT950_1AC8 (AP), Mode: 1- AP, 6 CH (2.437 GHz)).

- Select to Go with a PPTP VPN and create a new Server.

The screenshot shows the PPTP configuration page in the Teltonika web interface. The navigation tabs are Status, Network, Services, and System. The 'Services' menu is open, and the 'PPTP' tab is selected. Below the navigation, there are tabs for OpenVPN, IPsec, GRE Tunnel, PPTP (selected), L2TP, SSTP, and Stunnel. The PPTP Configuration section is visible, with a table for configuration entries. Below the table, there is a form for creating a new configuration. The 'Role' dropdown is set to 'Server', and the 'New configuration name' field contains 'RUT1'. There is an 'Add New' button and a 'Save' button.

- On the advanced option:
 - Enable the PPTP VPN Server
 - Configure the VPN IP Pool: It is recommended that you serve maximum 2 addresses
 - Create username and a password for the VPN Client
 - Assign to the user the first IP address of the VPN IP Range

The screenshot shows the Teltonika web interface for configuring a PPTP Server Instance. The top navigation bar includes the Teltonika logo and menu items: Status, Network, Services, System, and Logout. The current page is titled "PPTP Server Instance: RUT1". Under the "Main Settings" section, there is an "Enable" checkbox which is checked. Below this are four input fields: "Local IP" (192.168.0.1), "Remote IP range start" (192.168.0.20), and "Remote IP range end" (192.168.0.21). A table below these fields lists user configurations. The table has columns for "User name", "Password", and "PPTP Client's IP". One user is listed with the name "user1", a masked password, and the IP "192.168.0.20". There is a "Delete" button next to this entry. Below the table is an "Add" button. At the bottom of the form are "Back to Overview" and "Save" buttons.

TELTONIKA Status Network Services System Logout

FW ver: RUT9XX_R_00.05.03.4 | [FW update available](#)

OpenVPN IPsec GRE Tunnel **PPTP** L2TP SSTP Stunnel

PPTP Server Instance: RUT1

Main Settings

Enable

Local IP

Remote IP range start

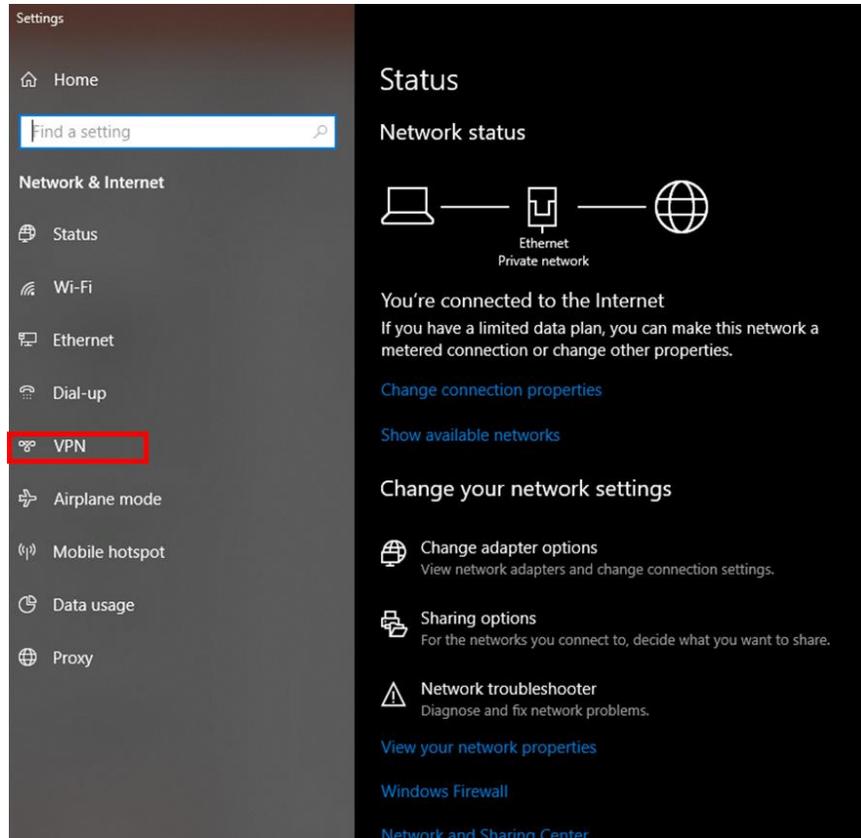
Remote IP range end

User name	Password	PPTP Client's IP	
<input type="text" value="user1"/>	<input type="password" value="....."/>	<input type="text" value="192.168.0.20"/>	<input type="button" value="Delete"/>

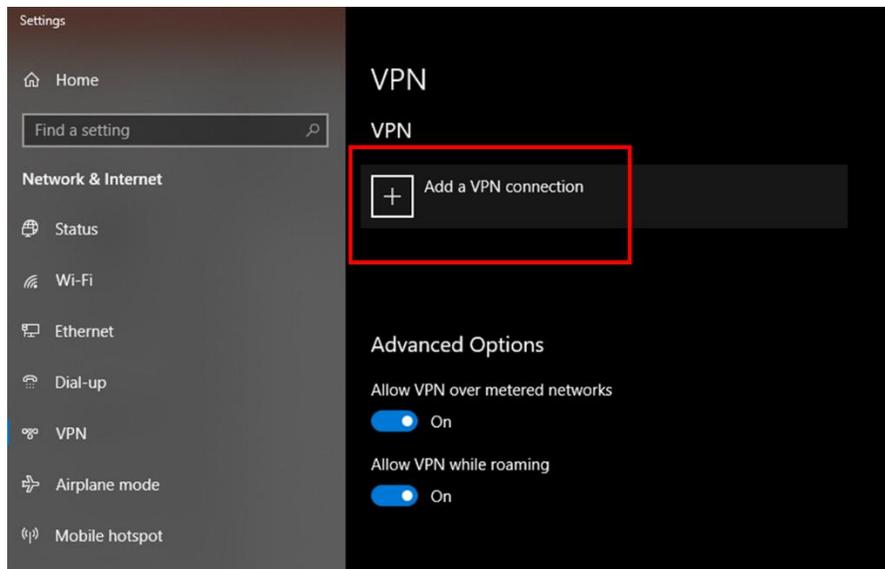
5.2 DISTANT VPN CLIENT CONFIGURATION

The VPN client is the distant computer situated on the office. User should configure a VPN connection to have access to the VPN server hosting his BeanGateway®.

- Go to Network and Internet Settings (Network share center in Windows 7)
- Select VPN to create a new VPN connection



- Add a new VPN connection



- Use the following inputs to configure the VPN connection
 - The name of the VPN server
 - The PUBLIC FIXED IP of the 4G Router
 - The VPN username created on the 4G Gateway and the Password

Add a VPN connection

VPN provider
Windows (built-in) ▾

Connection name
RUT1 ✕

Server name or address
197.6.190.13

VPN type
Automatic ▾

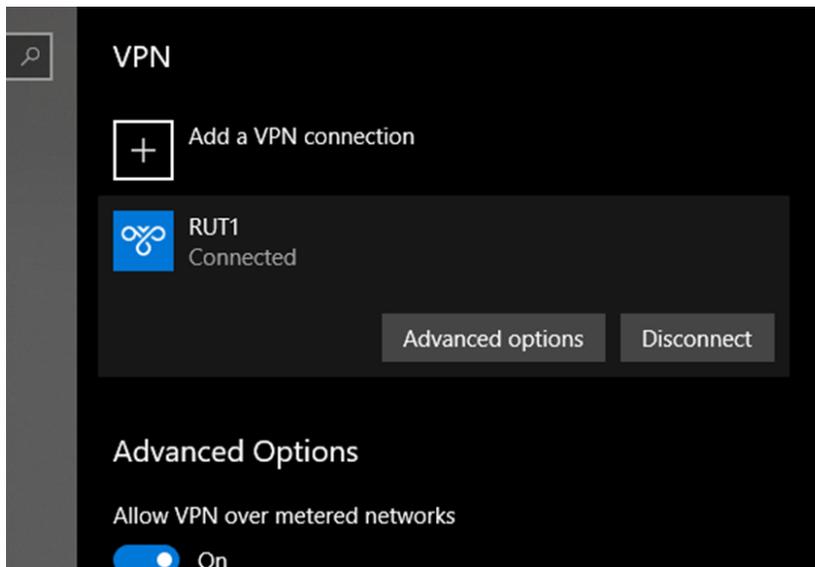
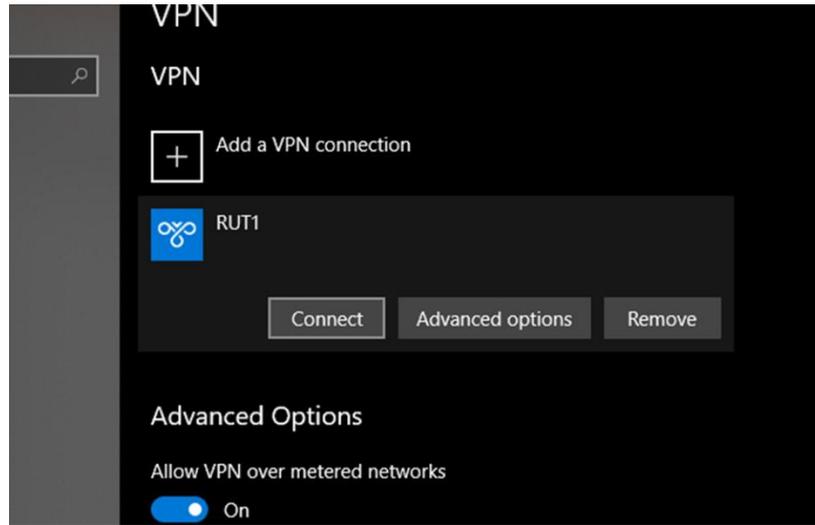
Type of sign-in info
User name and password ▾

User name (optional)
user1

Password (optional)
●●●●●●●●

Remember my sign-in info

- The Computer is ready to join the VPN: Press connect



- Using IP config, user can figure out that he is connected to the VPN

```
Wireless LAN adapter Local Area Connection* 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . . . . . :
Link-local IPv6 Address . . . . . : fe80::d58d:cc35:7284:709d%7
IPv4 Address. . . . . : 192.168.1.245
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1

PPP adapter RUT1:

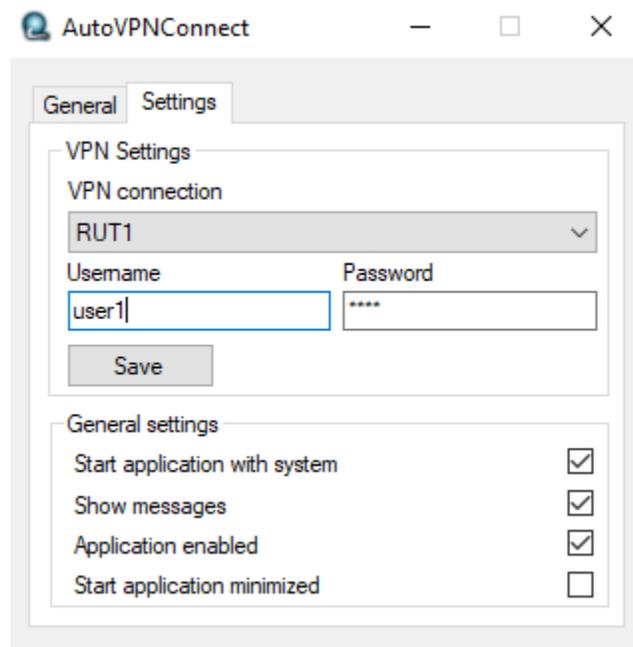
Connection-specific DNS Suffix . . . . . :
IPv4 Address. . . . . : 192.168.0.20
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . : 0.0.0.0

Wireless LAN adapter Wi-Fi:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . . . . :

C:\Users\TechSupport>
```

- Windows10 has removed the Auto Redial from the VPN connection, make sure that you Install AutoVPNconnect software after finishing the VPN configuration:
<https://sourceforge.net/projects/autovpnconnect/>



5.3 CONNECTING THE BEANGATEWAY TO THE VPN

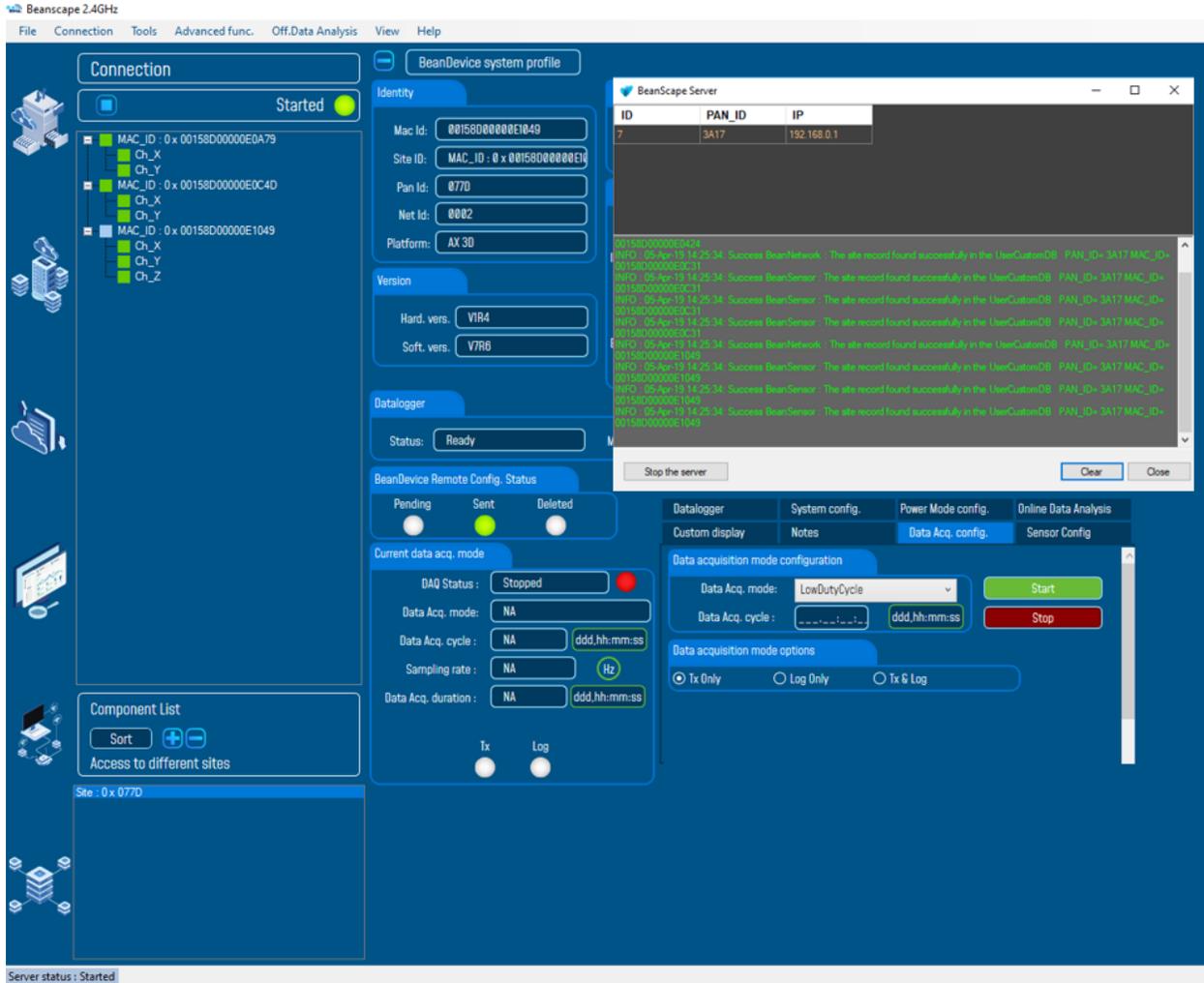
- Connect your laptop to the 4G Router used to connect the BeanGateway
- Run BeanScape® 2.4 GHz
- Go to Tools > BeanGateway Ethernet/LAN configuration
- Localize your BeanGateway
- Assign to the BeanGateway a Local Static IP (example 192.168.1.xx)
- On the BeanScape Frame, put the VPN first IP address assigned to the VPN client which was in our example 192.168.0.20

5.4 BEANSCAPE AT THE OFFICE

Once connected to the VPN, run the BeanScape® and click on Start the Server.

The BeanScape will display the BeanGateway profile.

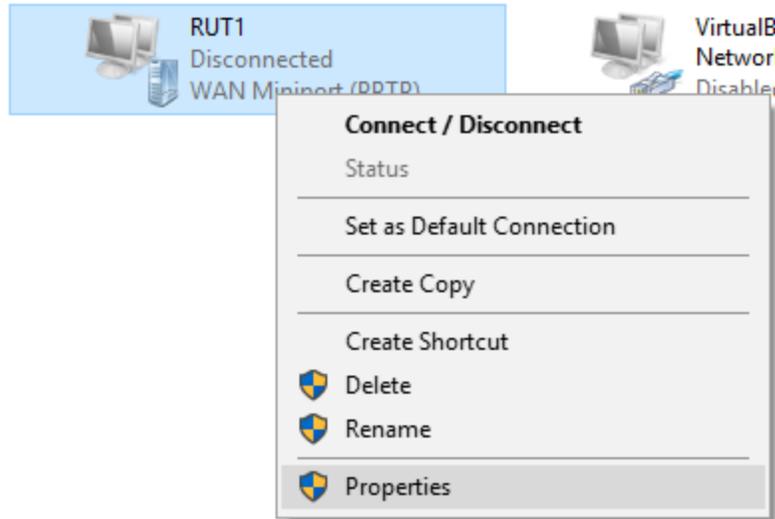
Open the BeanScape Server Window, you can figure out that BeanGateway flow is coming from the VPN server 192.168.0.1



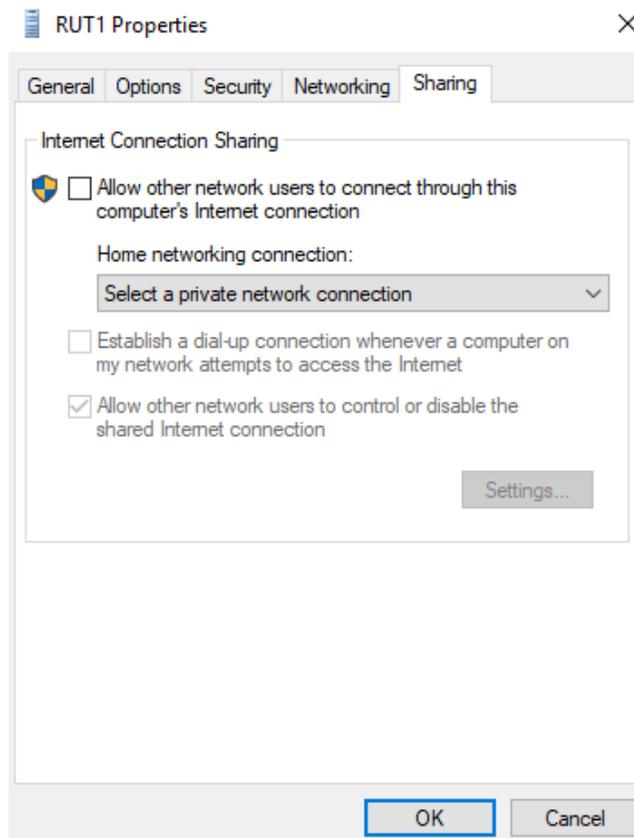
5.5 DATA CONSUMPTION

It is important to mention, That VPN can be used also to connect to internet, so it is important to make sure that this option is disabled on the VPN client proprieties.

Go to Control Panel > Network and sharing center > Change adapter settings and select the VPN Client proprieties



On the Sharing tab, make sure that the option is unchecked

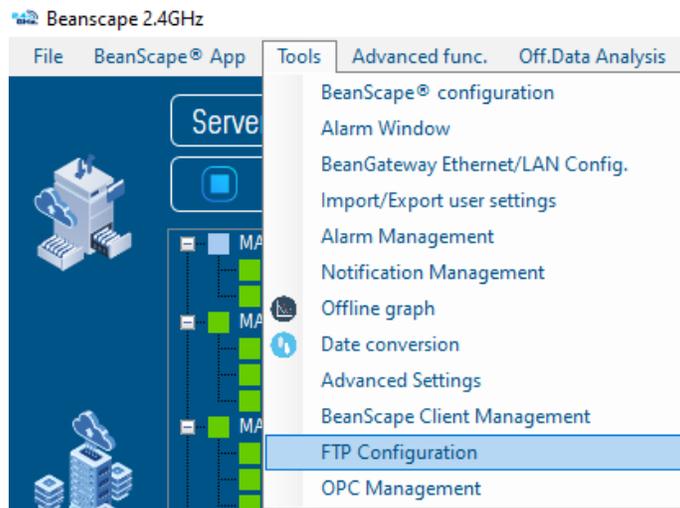


6. FTP SYNCHRONIZATION

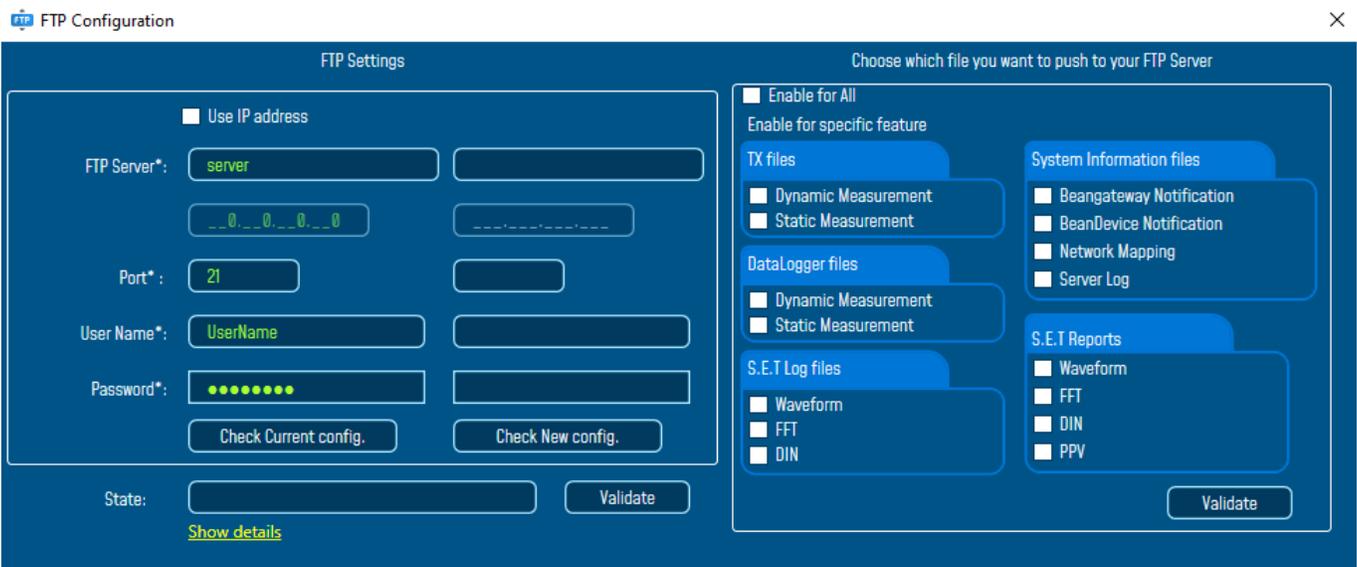
In some customer cases, users prefer transferring Log files stored on their computers to a distant FTP Directory.

6.1 USING BEANSCAPE FTP FEATURE

The user has the ability to send all his measurement data log files to the FTP Server through the FTP feature.



Check FTP enable check box then enter the right FTP Server setting using the following window



You should connect to your FTP server before setting up the FTP configuration on the BeanScape software.

FTP Settings

Use IP address

FTP Server*: server

Port*: 21

User Name*: UserName

Password*: ●●●●●●●

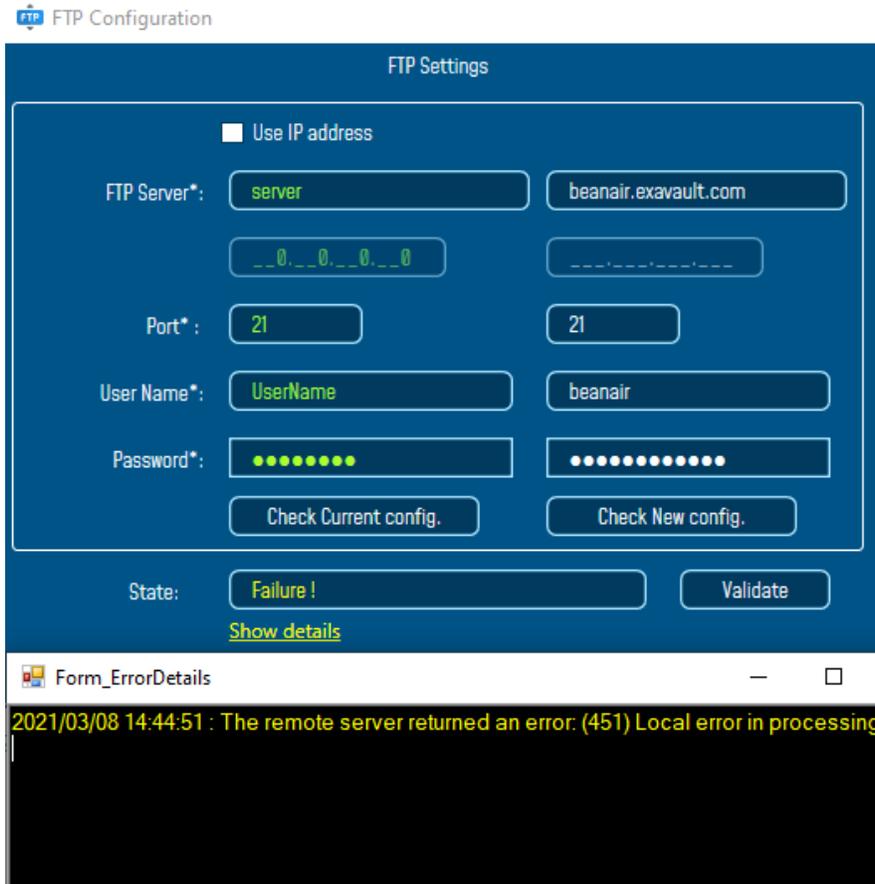
Check Current config. Check New config.

State: Validate

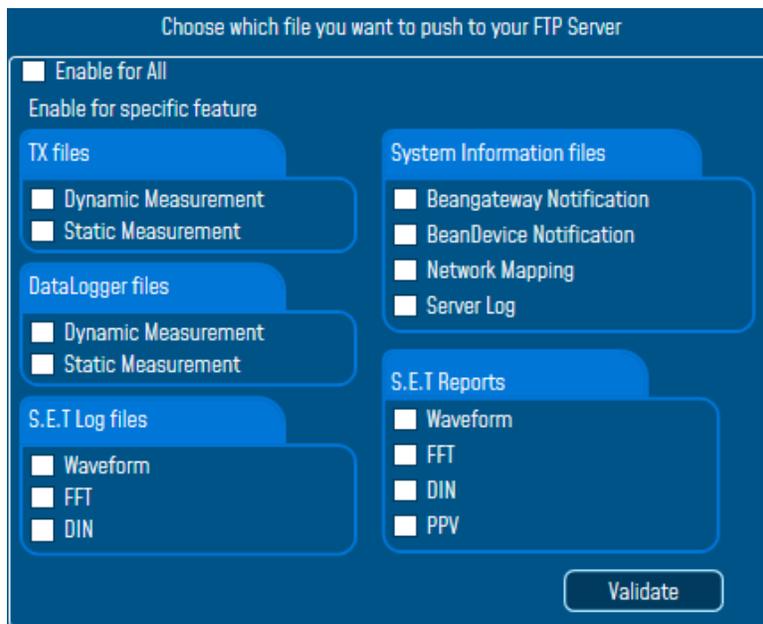
[Show details](#)

- **FTP Server:** Enter your FTP Server DNS or IP address by checking use IP address checkbox
- **User Name:** Enter your FTP user name
- **Password:** Enter your right FTP password
- **Port:** By default, the FTP port is 21, you can change it also
- **Check New Configuration:** click on check new configuration to make sure the settings are correct.
- **Validate:** click on validate to save the setting and proceed
- **State:** display if the connection status successfully established or failed.

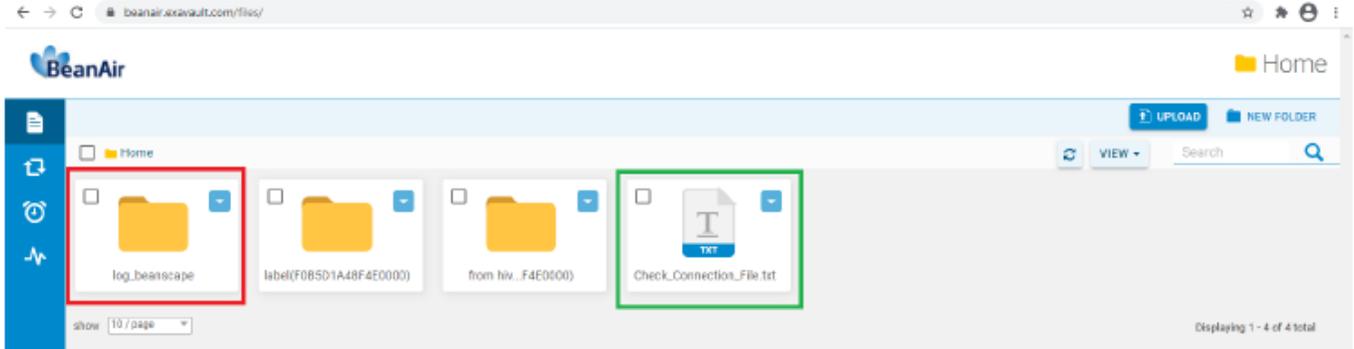
If the connection was failed, please click the Show details link to see the cause of the issue.



Then check the type of files which you want to send to you FTP server, and click on Validate



The files will be stored on your FTP server every 1 min.

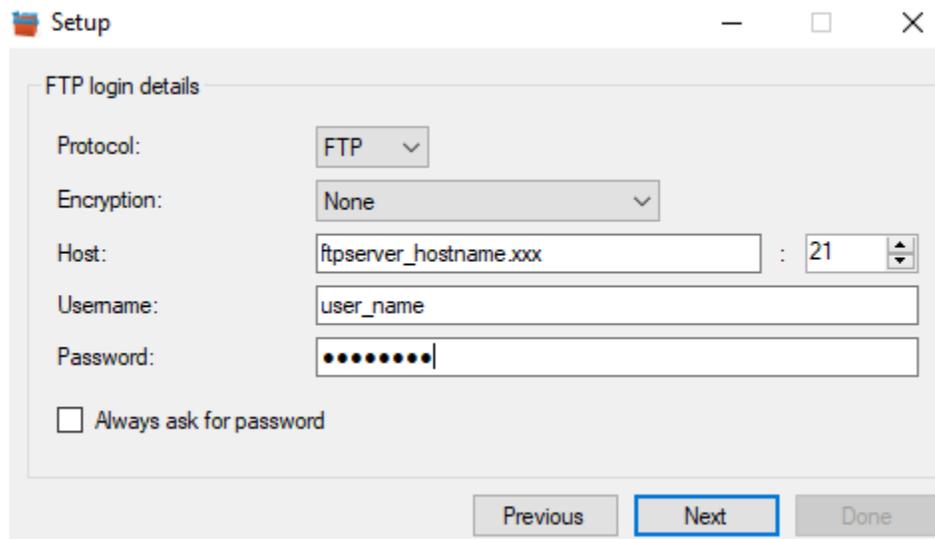


[Watch the FTP Configuration video](#)

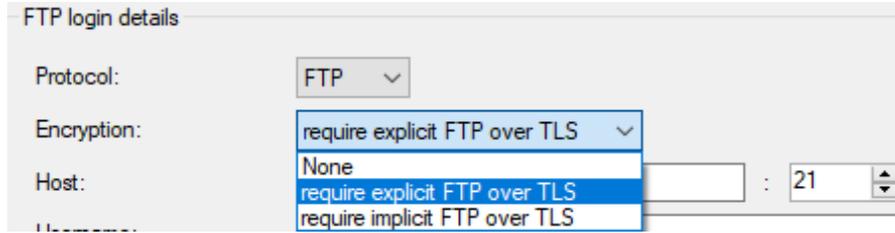
6.2 USING THIRD PARTY FTP SOFTWARE

To configure the transfer of Log_BeanScape directory to an FTP directory, you can use an FTP software, like the FTP Box : <http://ftpbox.org/>

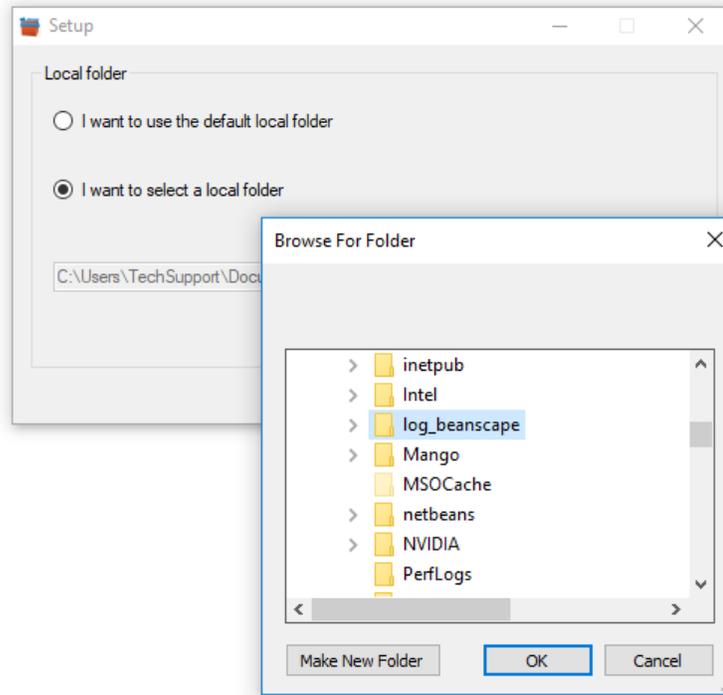
- After the installation, use the suitable language and setup the FTP parameters:



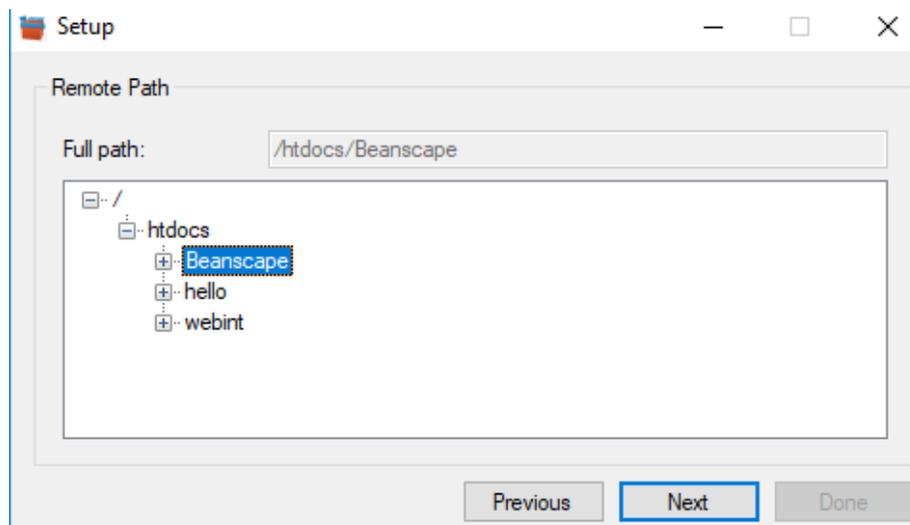
- If you prefer using TLS encryption, select the suitable option from the List below:



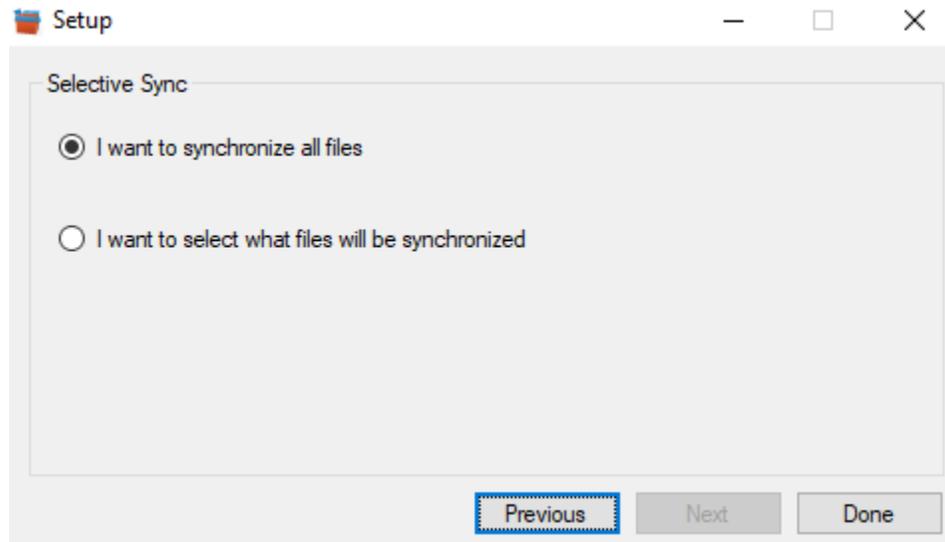
- Select the local directory used for the BeanScope Log files to be synchronized via FTP



- Select from the Tree the distant FTP folder located in your FTP server/distant folder



- Before finishing the setup, you have to configure the software to synchronize all files and directories in your Local Folder or precise which data should be synchronized.



7. TROUBLESHOOTING

7.1 HOW CAN I GET THE IP CONFIGURATION ON MY PC?

Open up your windows start menu and Type **cmd** in the “Search programs and files box” and press **Enter** on your keyboard. This will call the Windows command prompt window.



The IP Address can be found by launching DOS command Window and entering the console application IPconfig. This application displays all current TCP/IP network configuration values and can modify Dynamic Host Configuration Protocol DHCP and Domain Name System DNS settings.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.
C:\Users\BeanairDamon>ipconfig
Configuration IP de Windows

Carte Ethernet Connexion au réseau local :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . . . :

Carte réseau sans fil Connexion réseau sans fil :
    Suffixe DNS propre à la connexion. . . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::10fd:51e8:7c3c:6403%11
    Adresse IPv4. . . . . : 192.168.1.22
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.1.1

Carte Tunnel isatap.{F8DCBBD9-AAB4-485D-8F43-469125E1D43F} :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . . . :

Carte Tunnel isatap.{C6A390C2-D720-45CB-B612-F7A53D4F0777} :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . . . :

Carte Tunnel Teredo Tunneling Pseudo-Interface :
    Suffixe DNS propre à la connexion. . . . . :
    Adresse IPv6. . . . . : 2001:0:5ef5:79fb:2cef:234a:b18e:4b
    Adresse IPv6 de liaison locale. . . . . : fe80::2cef:234a:b18e:4b30%15
    Passerelle par défaut. . . . . : ::

C:\Users\BeanairDamon>
  
```

IP config command

IP Address of your PC

7.2 HOW CAN I MODIFY MY PC NETWORK INTERFACE CONFIGURATION?

Please visit Microsoft support pages that will show how you can access and modify your PC interface configuration.

https://support.microsoft.com/en-us/windows/change-tcp-ip-settings-bd0a07af-15f5-cd6a-363f-ca2b6f391ace#WindowsVersion=Windows_10