V1.4

TECHNICAL NOTE

BEANGATEWAY®
REMOTE ACCESS MANAGEMENT

BeanAir

Rethinking Sensing Technology

2.4 GHz

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.

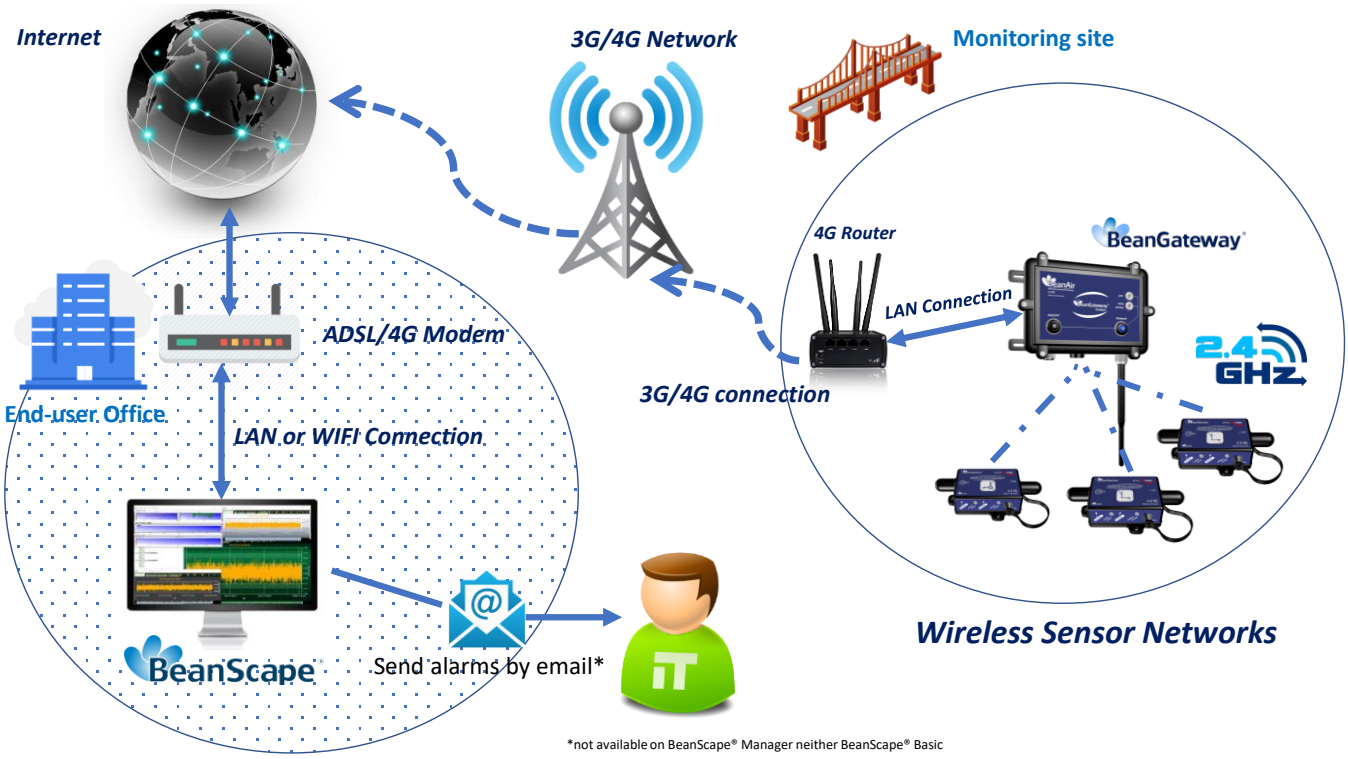
Beanair disclaims any and all responsibility for the application of the devices characterized in this document, and notes that the application of the device must comply with the safety standards of the applicable country, and where applicable, with the relevant wiring rules.

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.

Contents

1. CONNECTION TO A 3G/4G ROUTER



*not available on BeanScape® Manager neither BeanScape® Basic

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®:

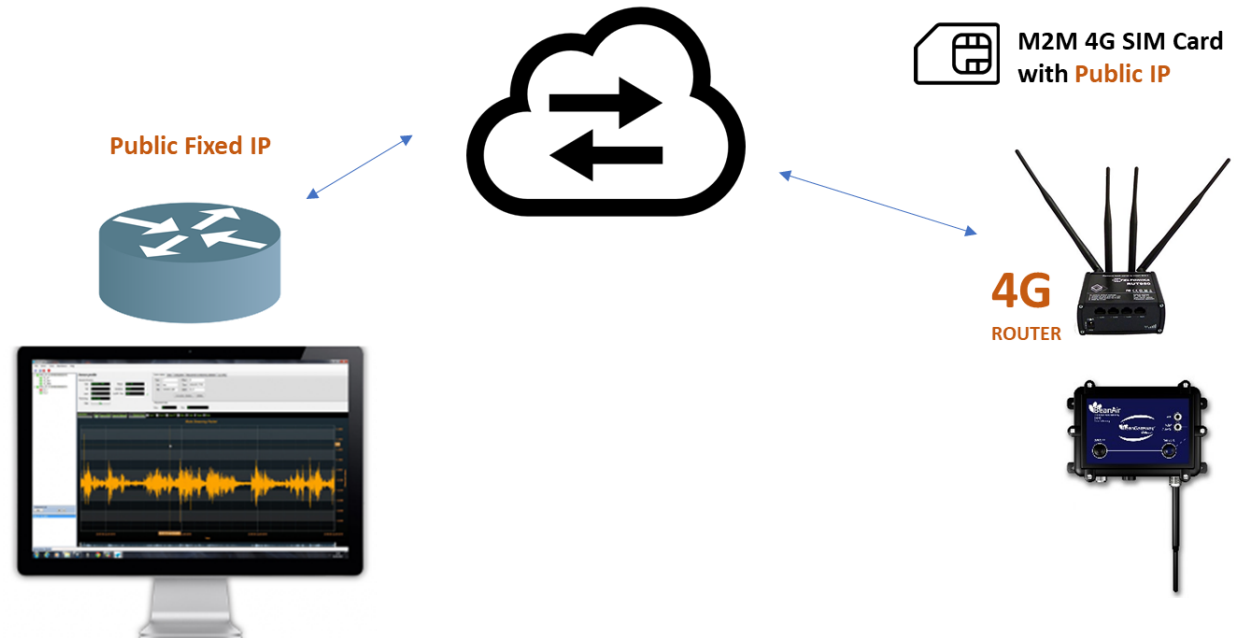
- Port Forwarding
- VPN/DDNS Access
- Direct VPN

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

1.2 MATERIAL REQUIREMENT

BeanGateway® version	*BeanGateway® Ethernet*
4G/3G Gateway	***TECHNOLOGY*** • HSUPA with fallback to: LTE, HSDPA, UMTS, EDGE ***Bands*** Tri-Band UMTS/HSDPA/HSUPA 850, 1900, 2100 MHz Or Quad-Band UMTS/HSDPA/HSUPA 850, 900, 1900, 2100 MHz ***HOST INTERFACES*** Ethernet: 10/100 BASE-T RJ-45 ***APPLICATION INTERFACES*** TCP/IP, UDP/IP, DHCP, HTTP, SNMP, SMTP, SMS, MSCI
ADSL Modem	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.

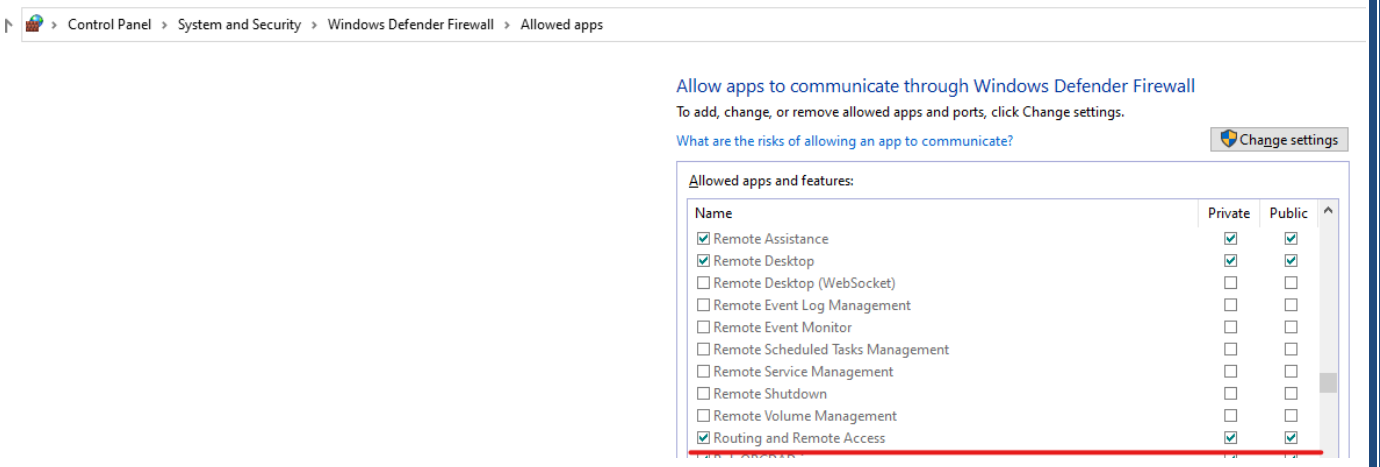
How to get a fixed public IP:

- ***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.

2.1 STEP 1: AT YOUR OFFICE, CONFIGURE YOUR FIREWALL FOR REMOTE ACCESS

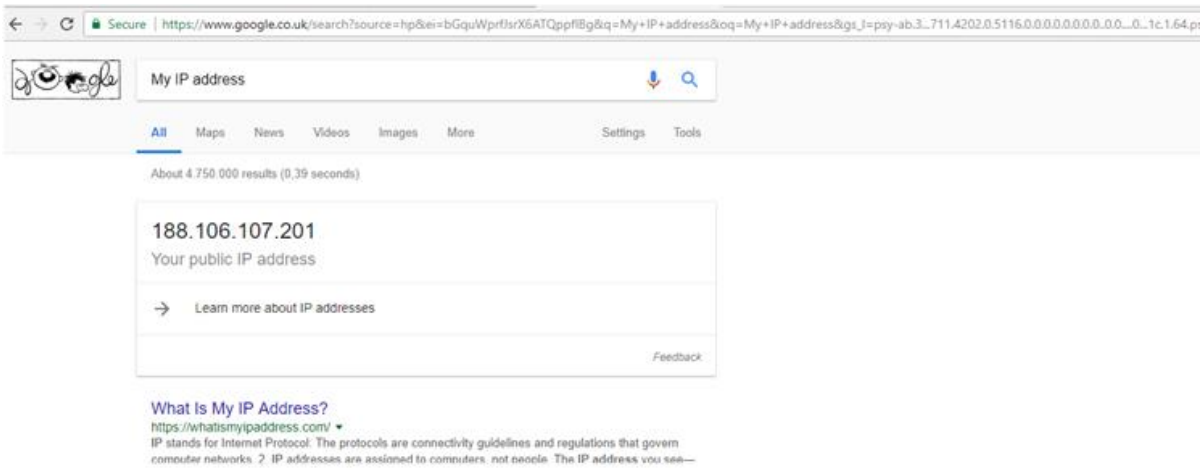
You have to enable Routing and Remote Access option for both Private and Public networks, communication through the firewall.



2.2 STEP 2: AT YOUR OFFICE, CONFIGURE IP FORWARDING RULES

2.2.1 Example with ADSL MODEM (NAT ROUTER Configuration)

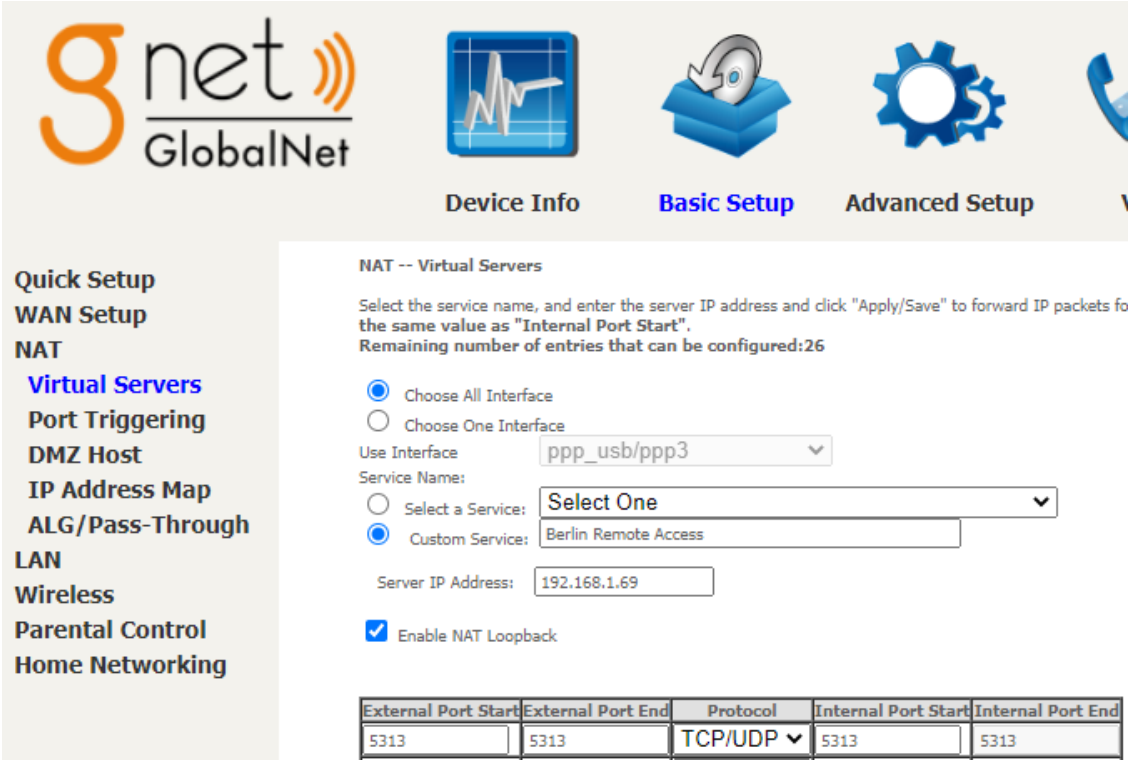
1. From your Office PC, search for your Public IP address (ex: search for MyIP on Google).



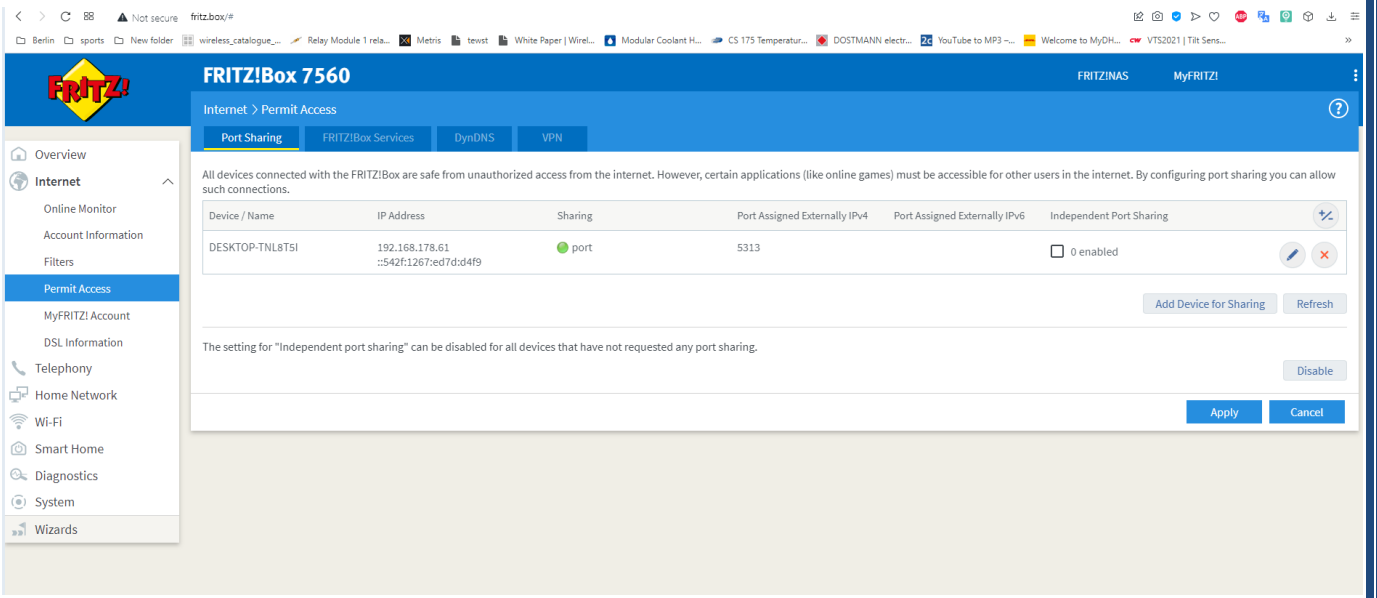
Make sure that no antivirus/firewall is blocking the Network activity between the BeanGateway® 2.4GHz and the BeanScape® 2.4GHz

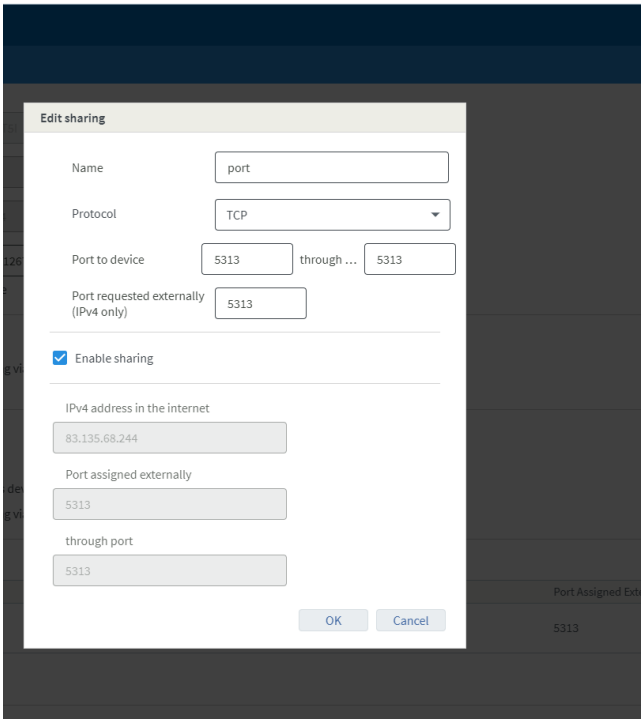
2. Setup a Port Forwarding configuration on your Router (each router brand has its own configuration interface).

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



Example 2 : Fritze Box (Germany)





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)

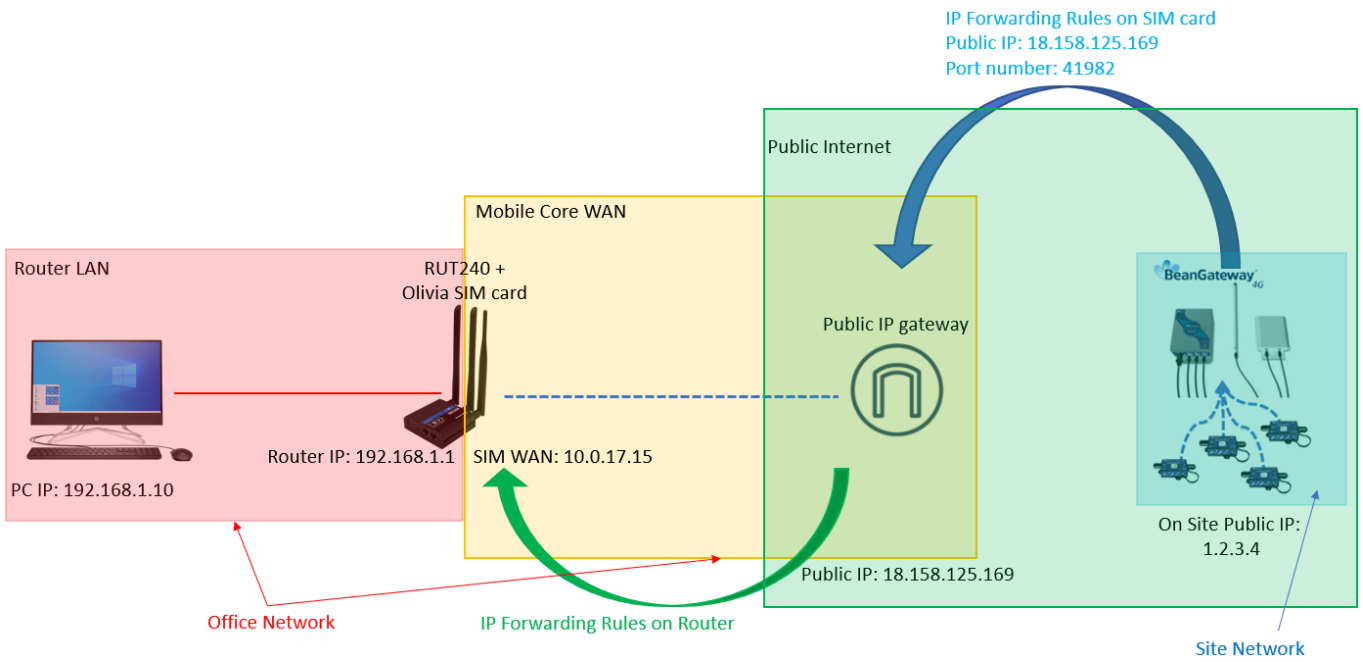
if you have a 4G router with a SIM card at your office, make sure that the SIM card comes with a Fixed Public IP address and your ISP provider doesn't restrict any port numbers.

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**.

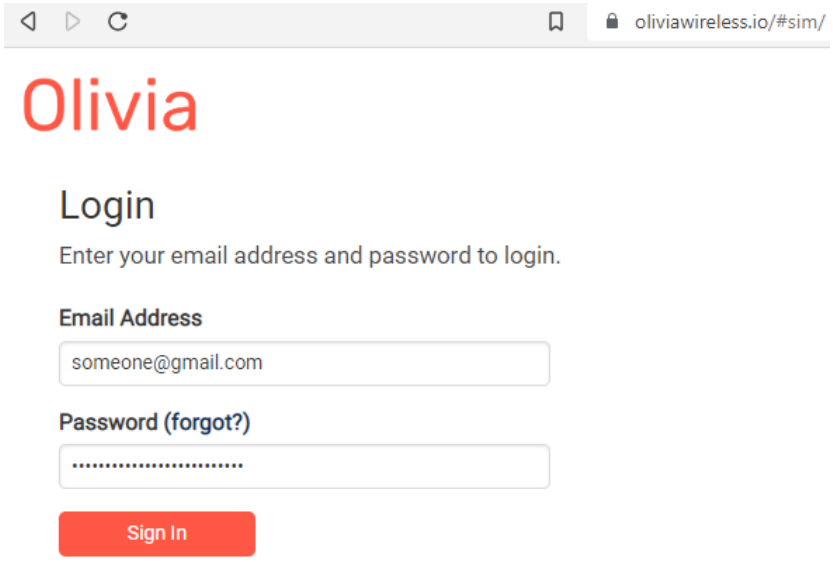


Please follow these steps to correctly configure the system.

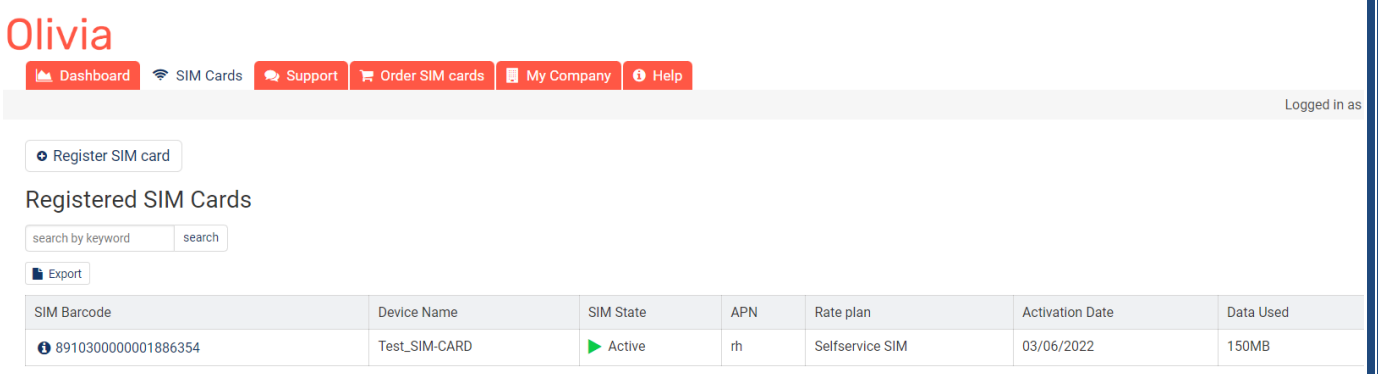
- **<u>Step 1: Verify that Public IP routes service is enabled on your SIM card</u>**

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

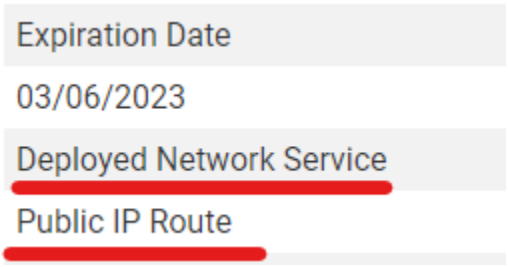
To verify that the Fixed Public IP address service is enabled, please login to your SIM Card platform



Then go to the tab SIM Cards.



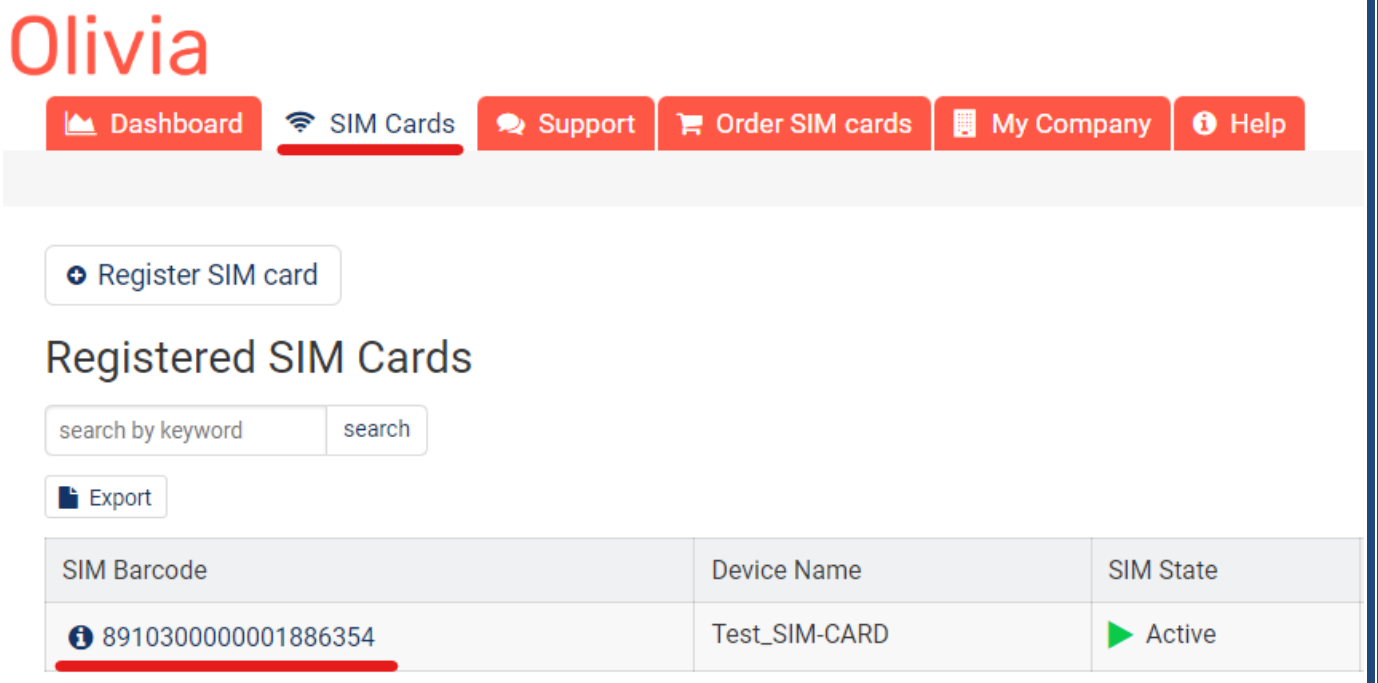
You should see “Public IP Route” noted under “Deployed Network Service” on the SIM cards details page.



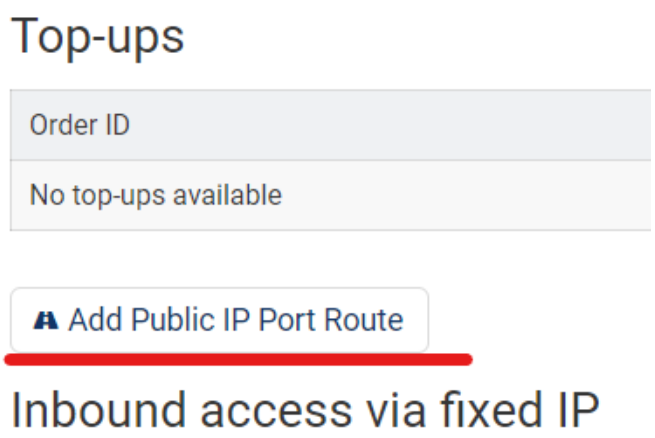
If it’s not the case you have to enable it before proceeding.

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

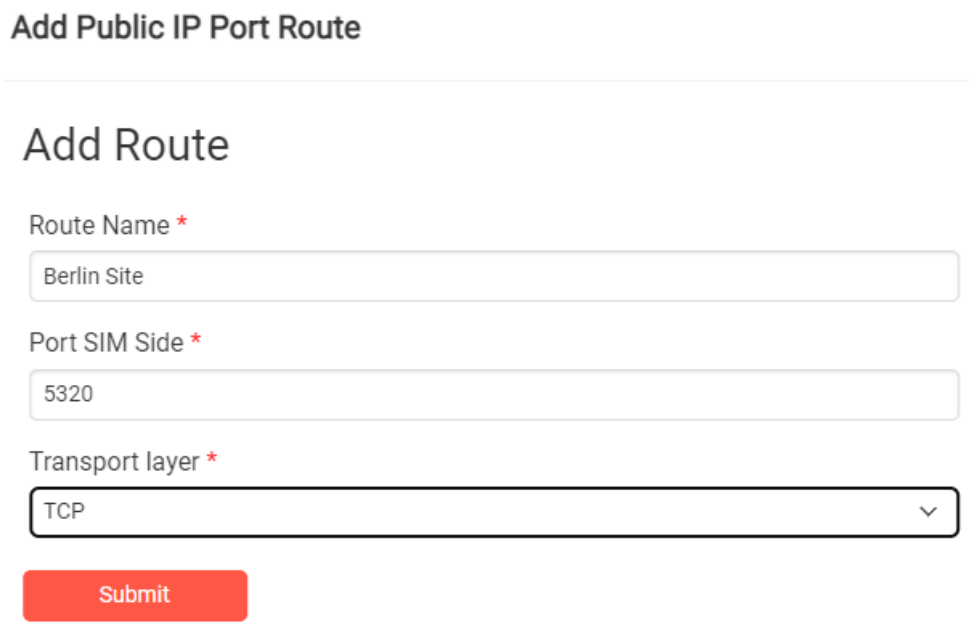
Navigate to “SIM card” and click on the SIM barcode



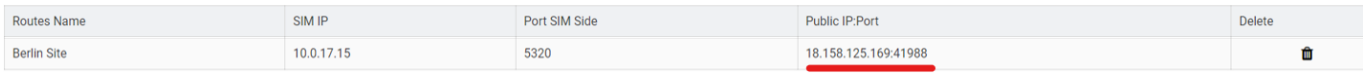
Then click on ADD Public IP Route



- 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)**



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**

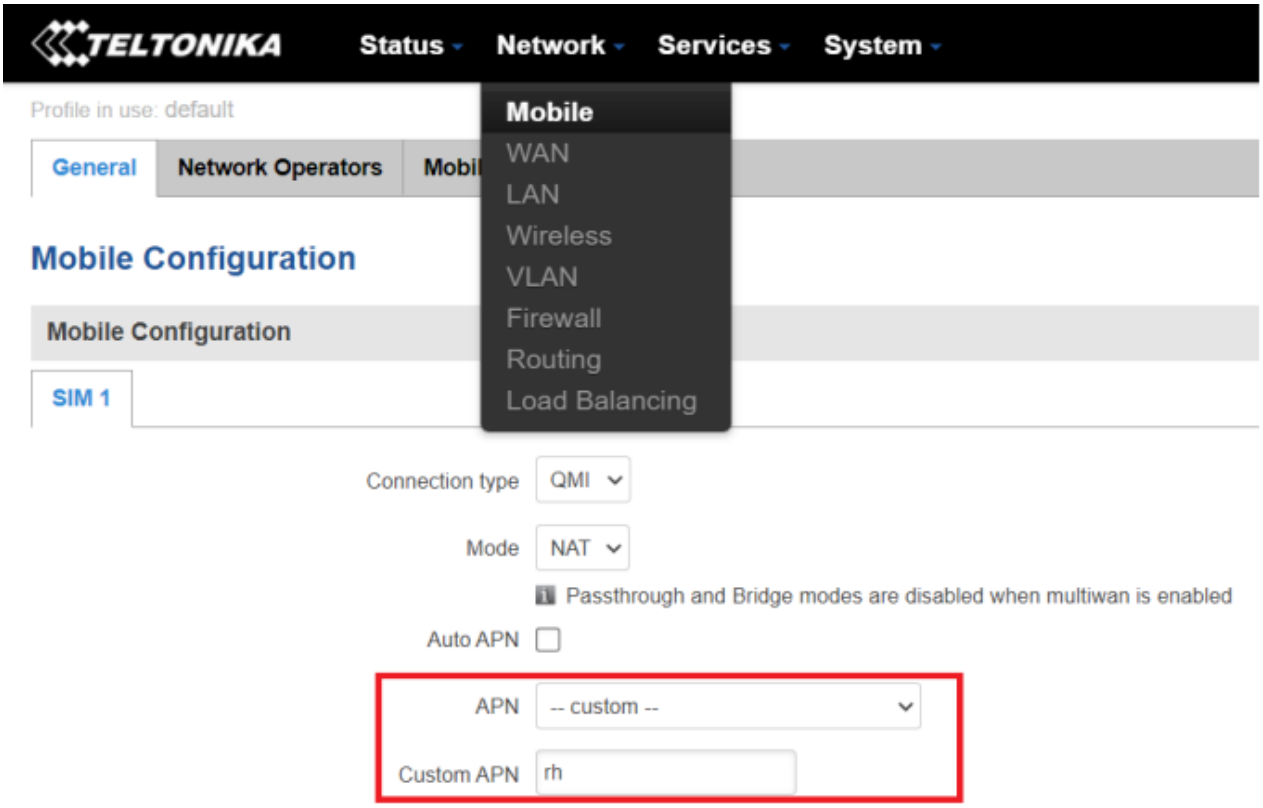
In this example we are using Teltonika Router RUT240, but the steps are similar for different types of routers.

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

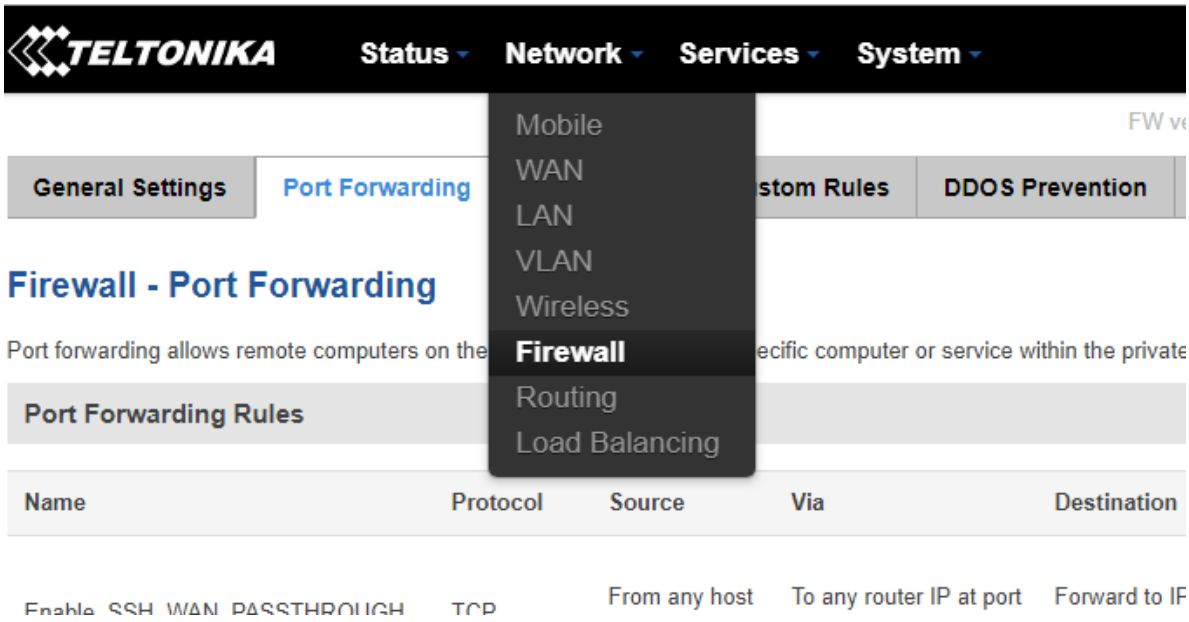
- APN: --custom–
- Custom APN: rh

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



- **<u>Step 4: Setup Port Forwarding on the router</u>**

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

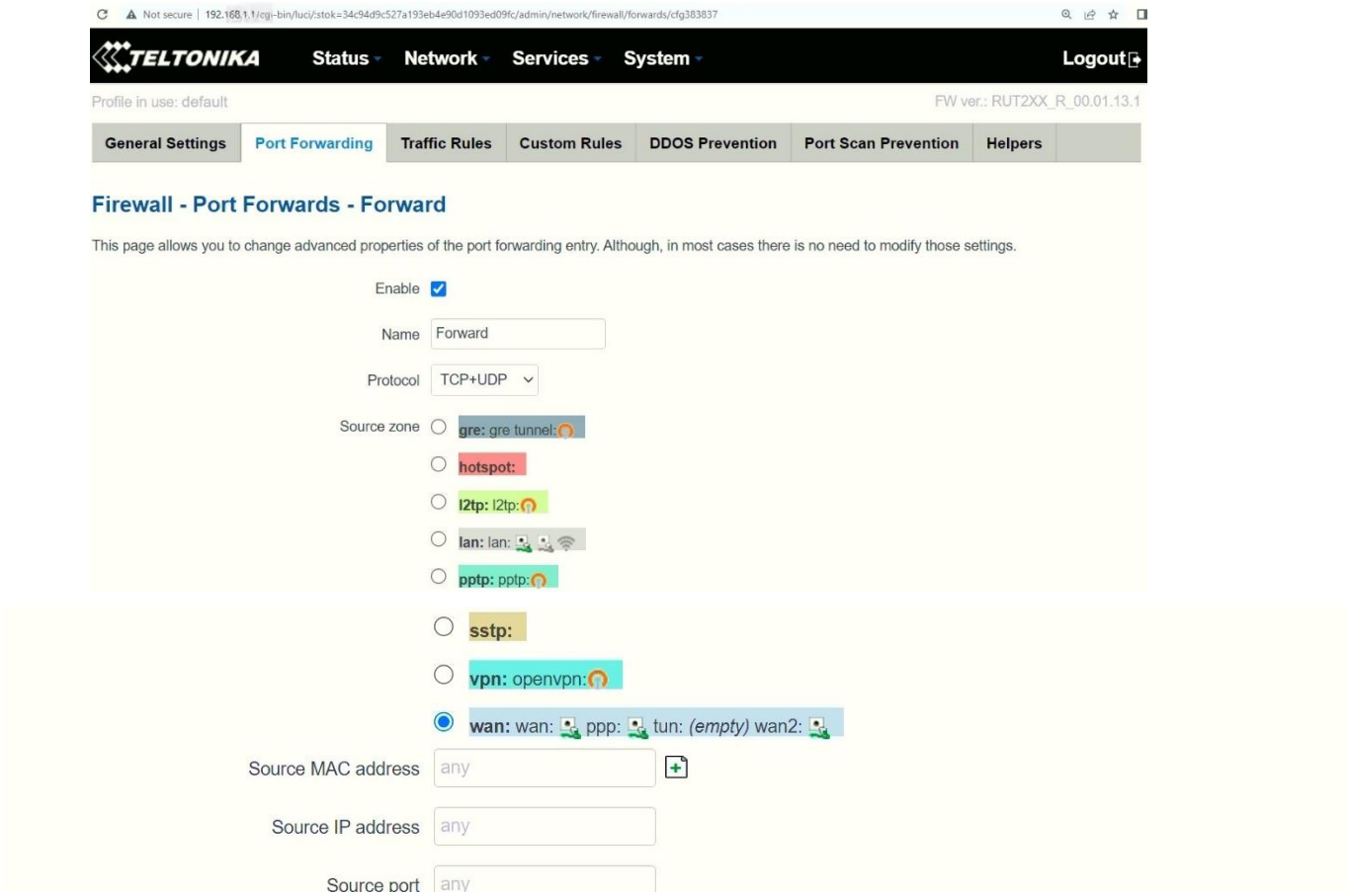


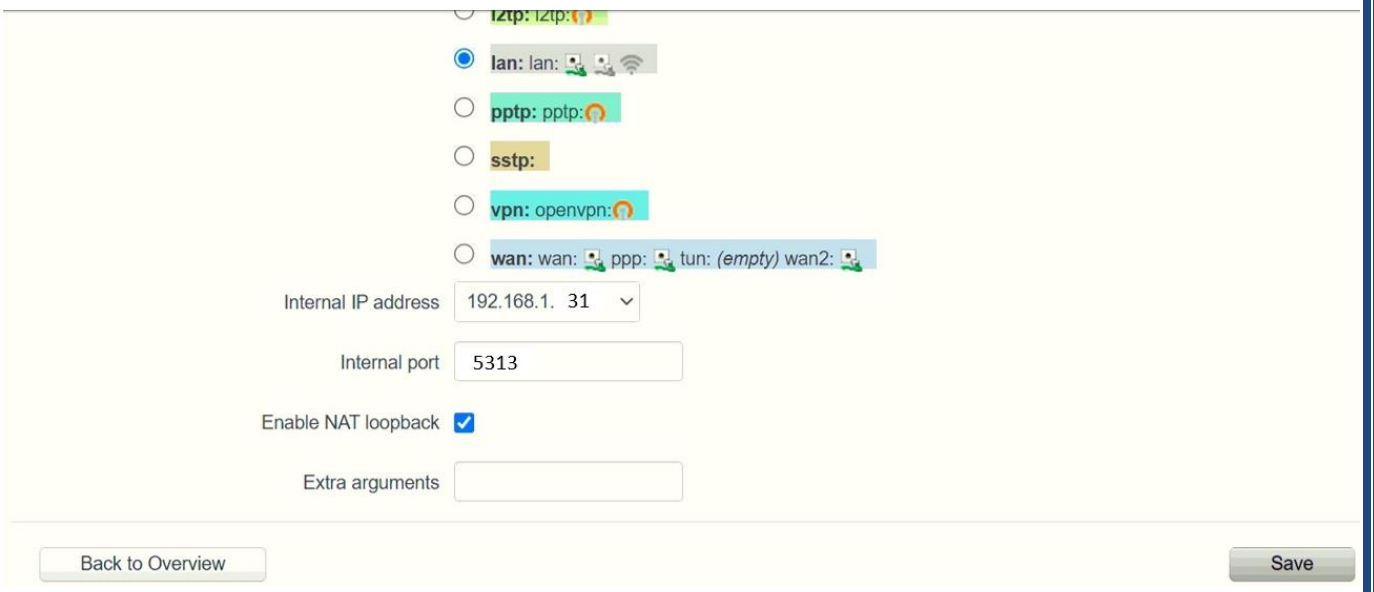
Scroll down to New Port Forward Rule and set the following

- 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 BeanScape software) **5313**

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

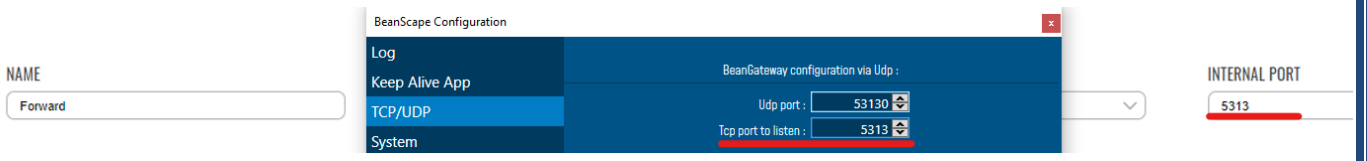
Make sure that the port forwarding rule is configured from WAN: External Port (or Sourec Zone) to LAN: Internal Port.





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

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



If you change the default TCP port on BeanScape 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

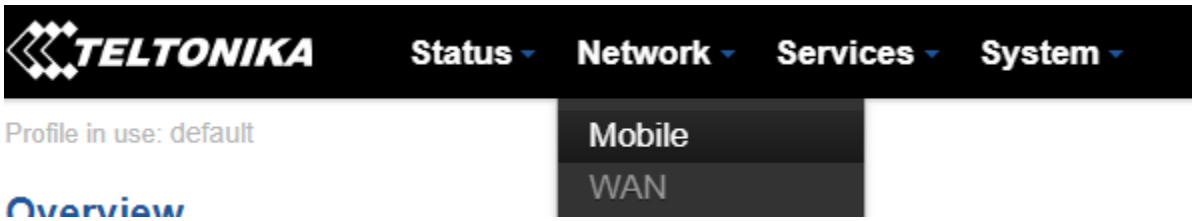
Now that you have your Public Fixed IP of your BeanScape® software running at your office. You can start to configure your BeanGateway® and LTE Router running on the monitoring site.

2.1.1 Sim card configuration

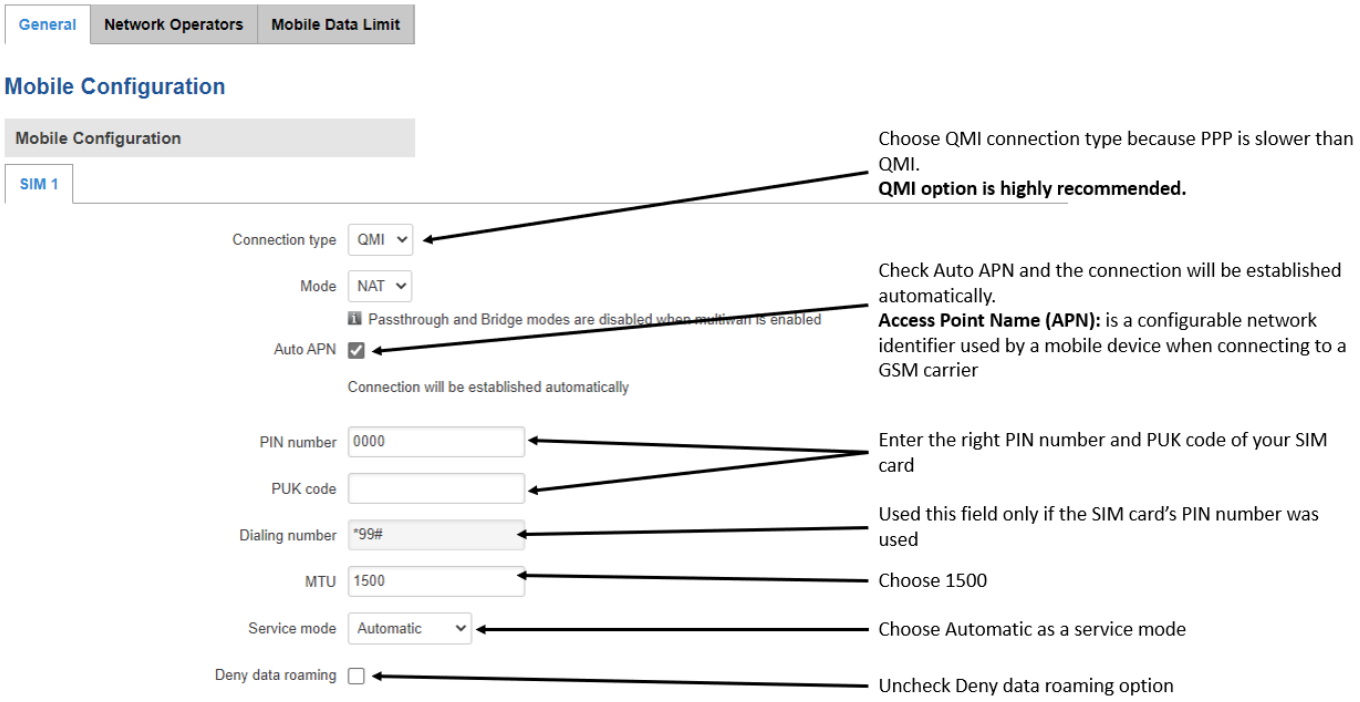
Use your browser on your PC and log in to the router using the following settings:

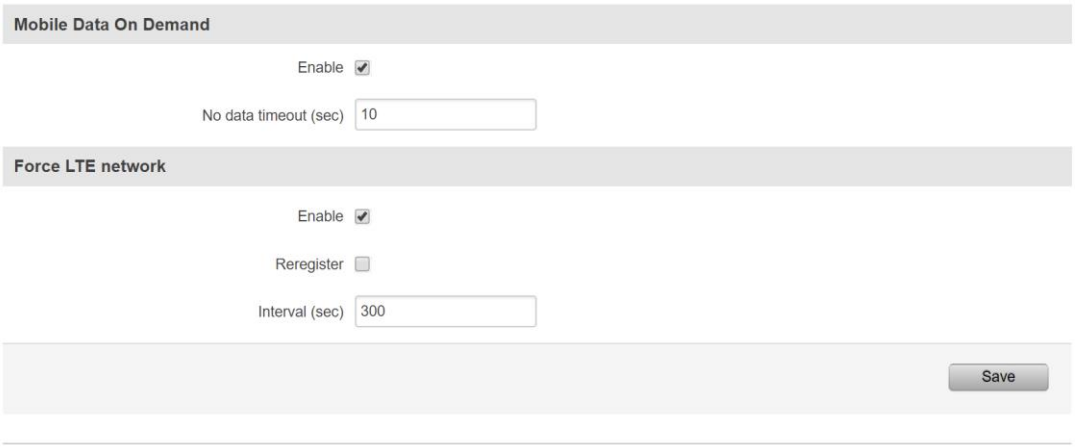
- IP address: 192.168.1.243 (tap it in google search bar)
- Username: admin | password: Beanair2020!

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



Now configure your mobile settings as follow



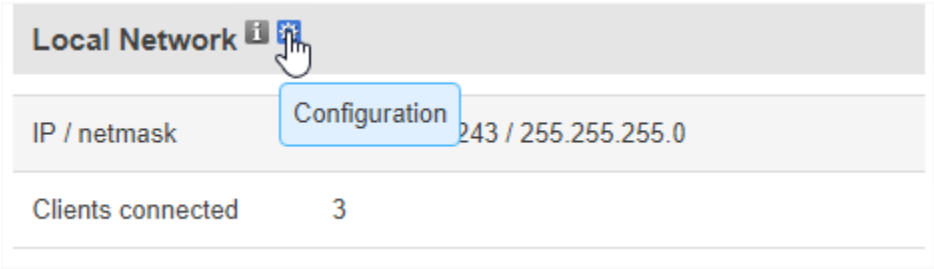


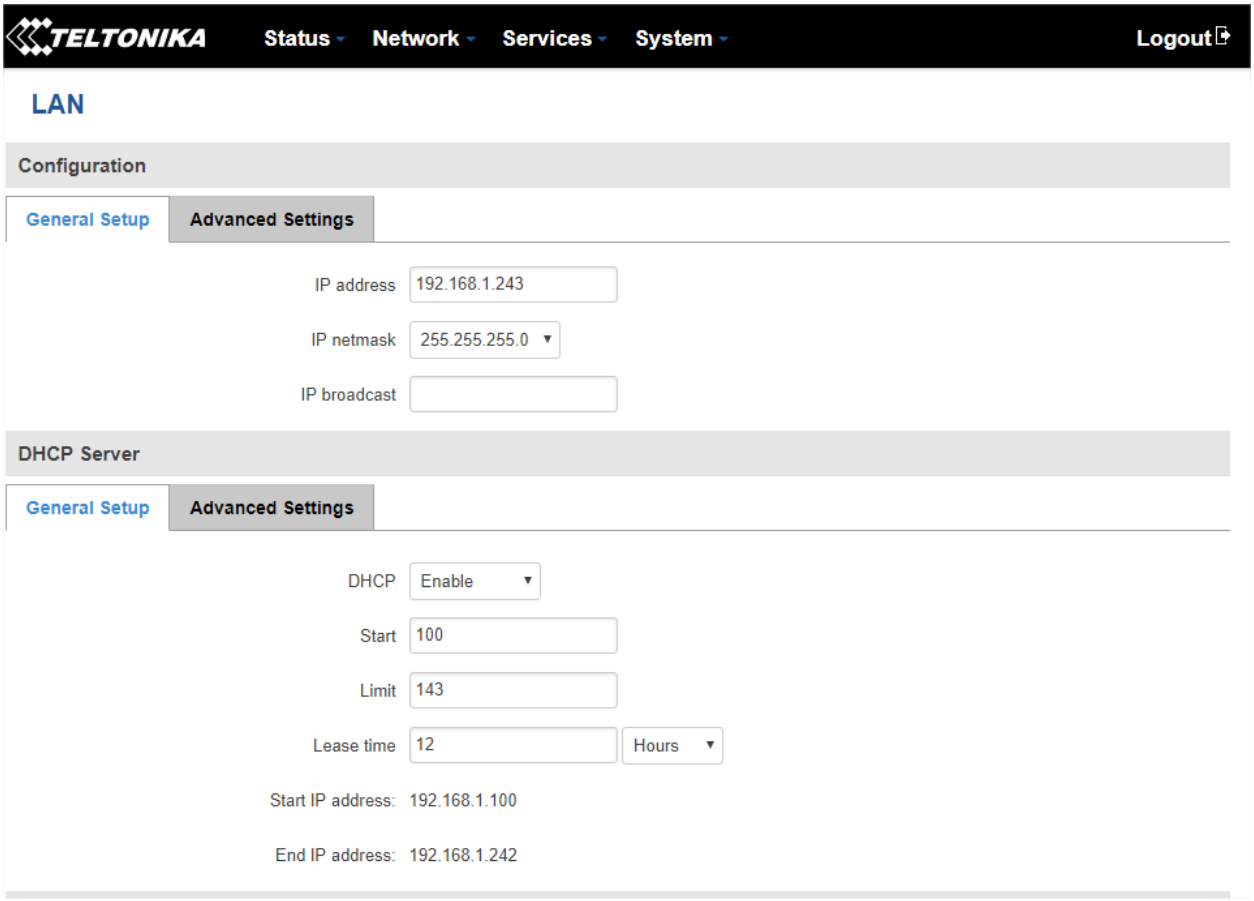
You can get the APN ID from your telecom operator provider

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



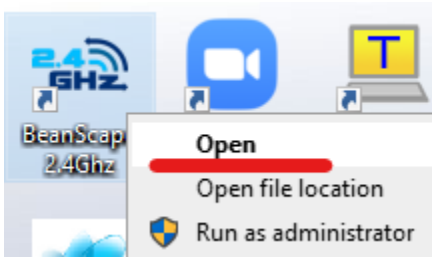


2.1.3 BeanGateway® 2.4GHz configuration with Public IP of your Office PC

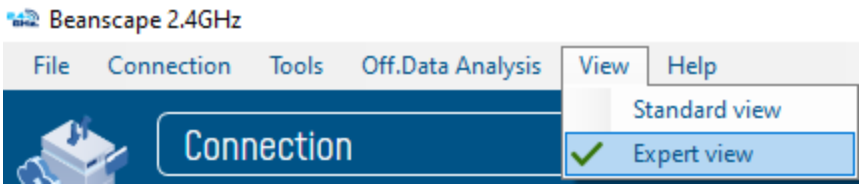
Now that your LTE Router is configured with your SIM card, it's time to configure correctly your BeanGateway® 2.4GHz.

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

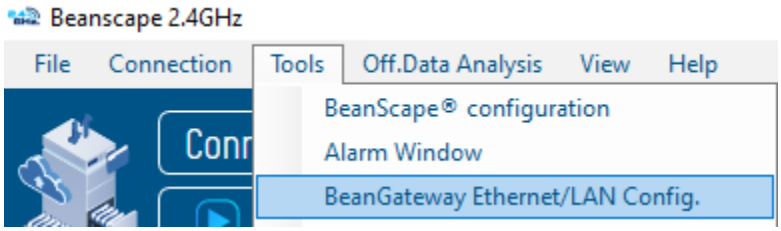
1. Right click on your BeanScape® software icon then click on Open



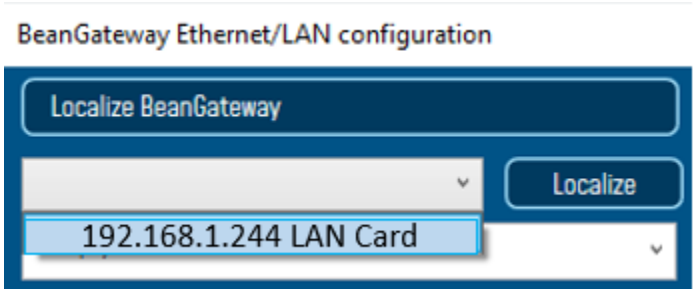
2. Switch to Expert view



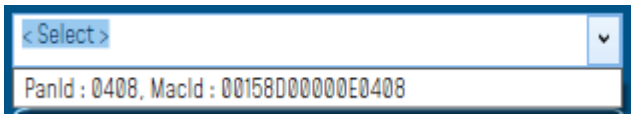
3. Navigate to Tools → BeanGateway Ethernet/LAN config



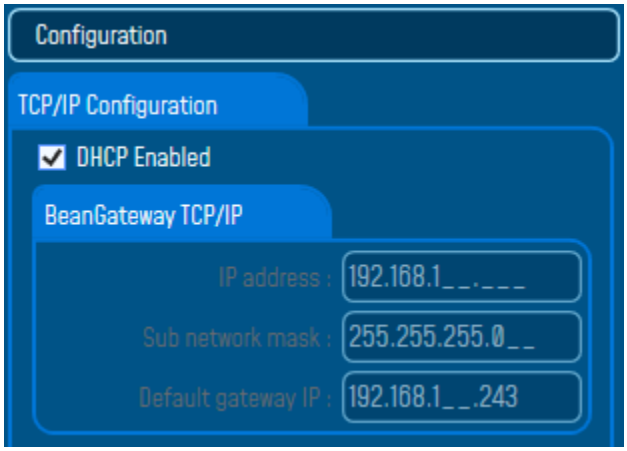
4. Select your LAN card IP Address (192.168.1.244), then click on Localize



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



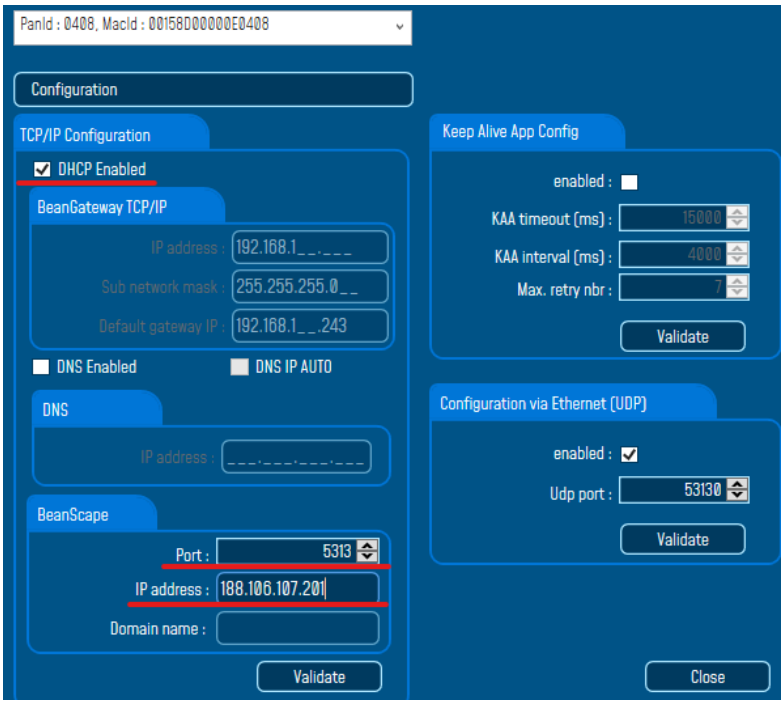
6. Check DHCP option to assign an automatic IP address to your BeanGateway®, then click on validate



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 BeanScape software (you will get your Public IP from step 2) . In this case the Public IP is 188.106.107.201

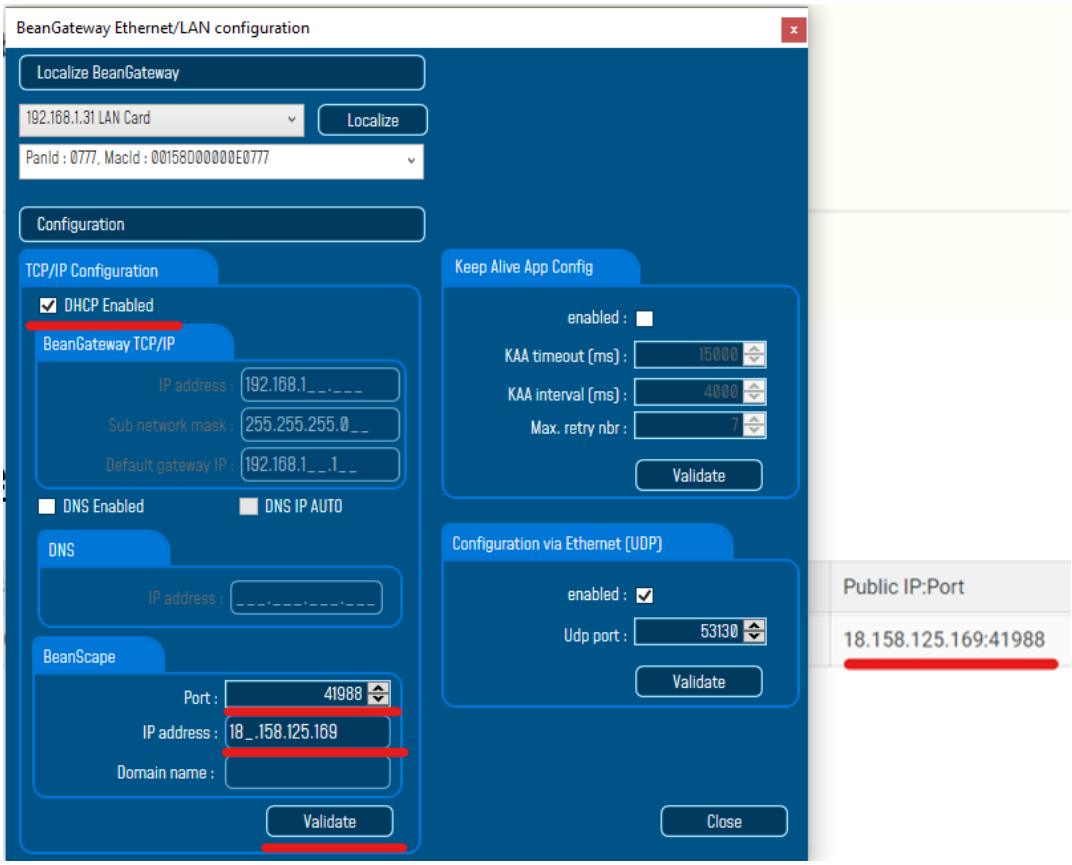


Case 2 - If you are using a LTE Router with a Data SIM CARD (example of Olivia Wireless SIM CARD)

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	18.158.125.169:41988	

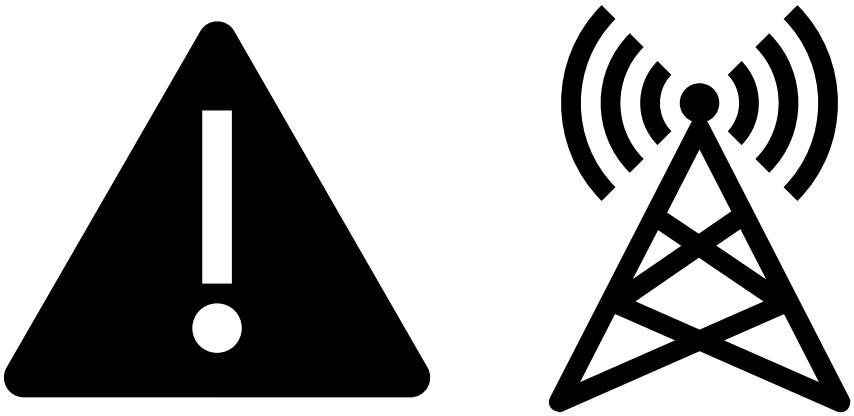


Make sure to use the Fixed Public IP address and the TCP Port number which are created on the SIM Card rule.

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 costumer 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.



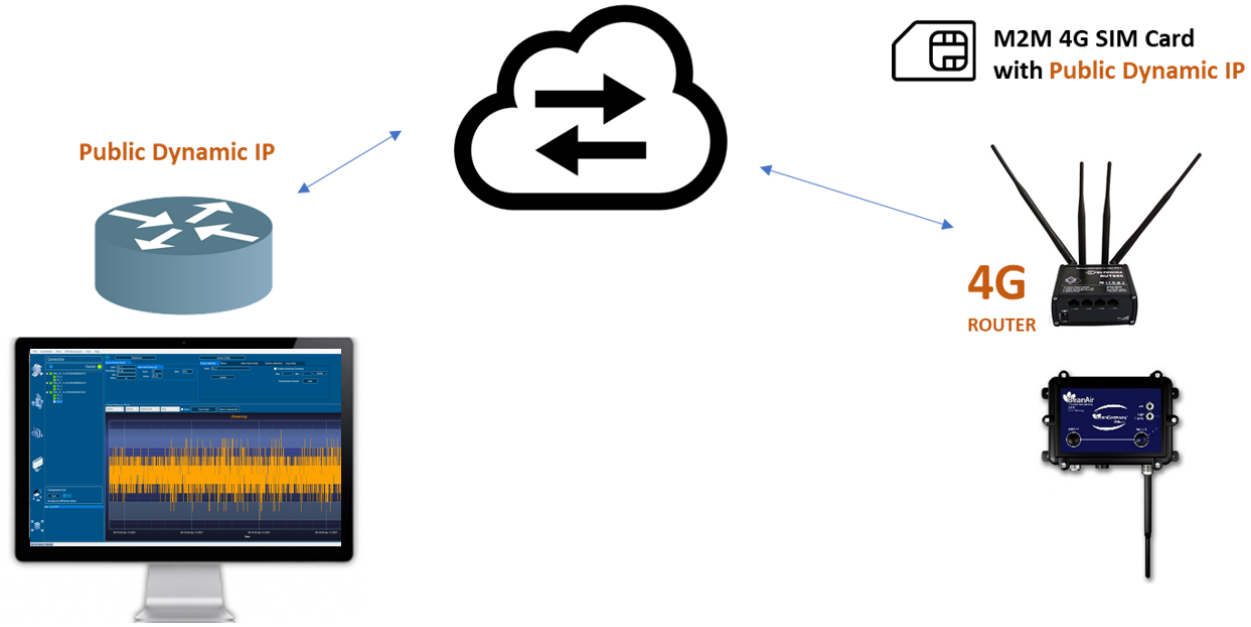
It is recommended to use a Dynamic DNS/PPTP VPN based solution or a direct VPN access via Fixed Public IP

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.



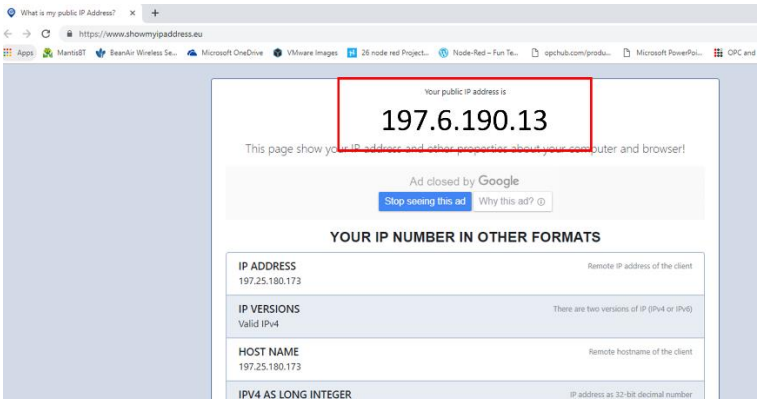
4.1 DYNAMIC DNS

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.

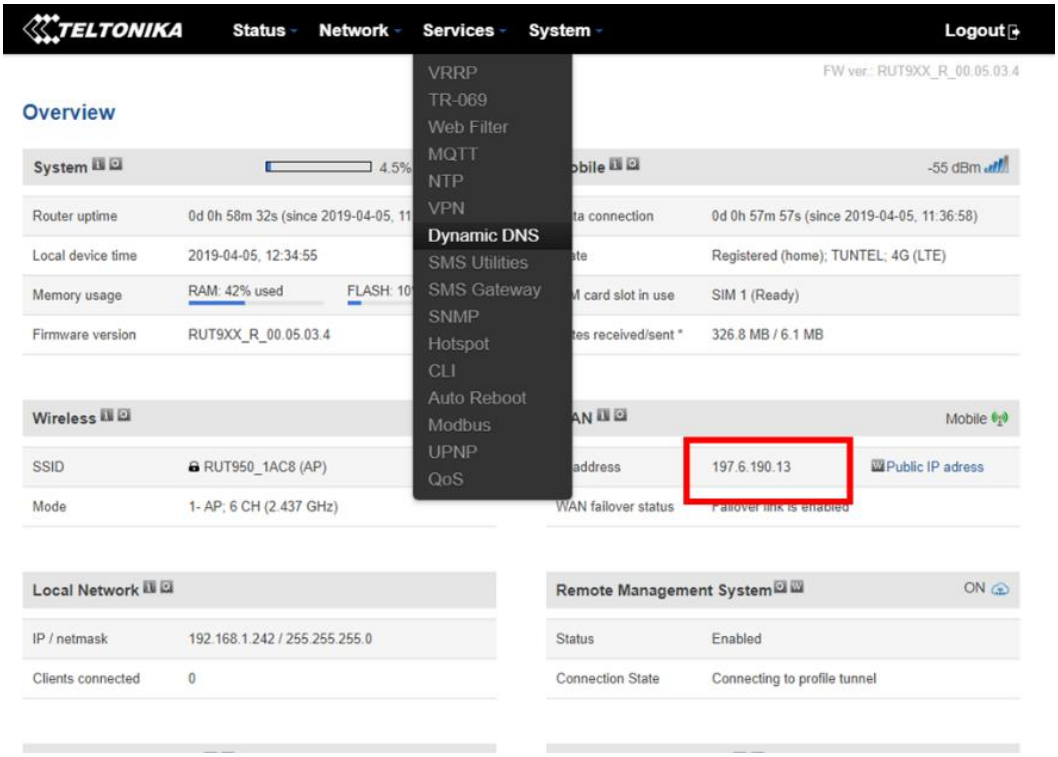
The DDNS configuration will be done on both 4G Router and the NoIP DDNS provider dashboard.

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

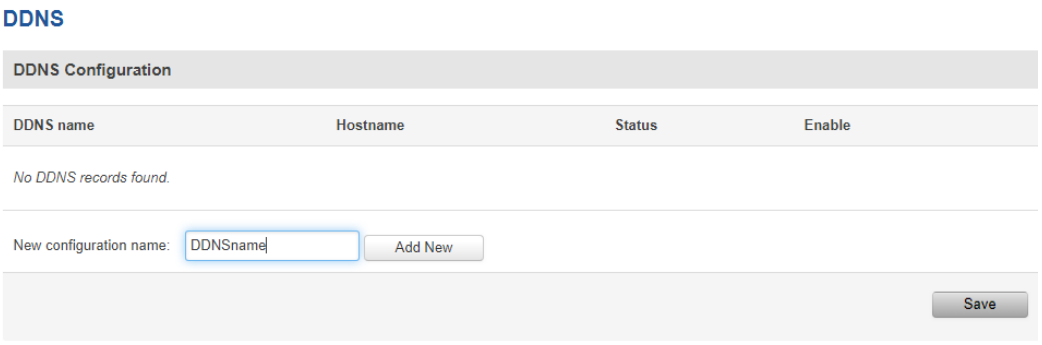
- Open your web browser and go to https://www.showmyipaddress.eu/ to display your Public IP



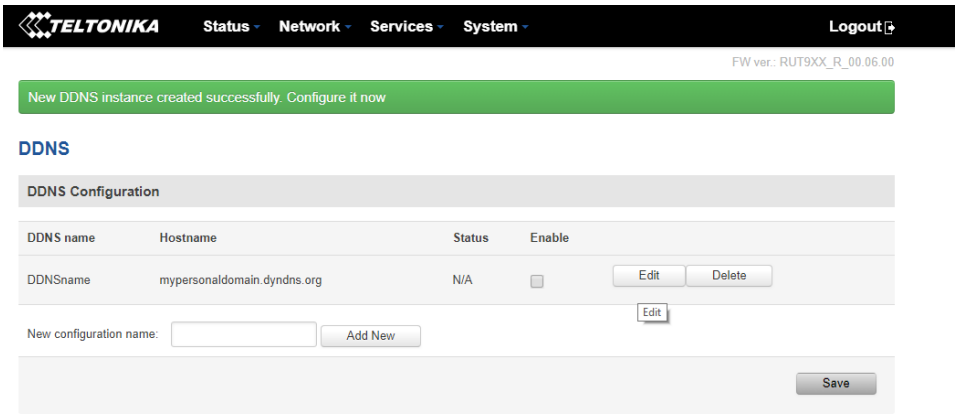
- Connect to your 4 G Router Web User Interface and check if the Assigned IP to your Router is a Public IP and is the same as mentioned on https://www.showmyipaddress.eu/



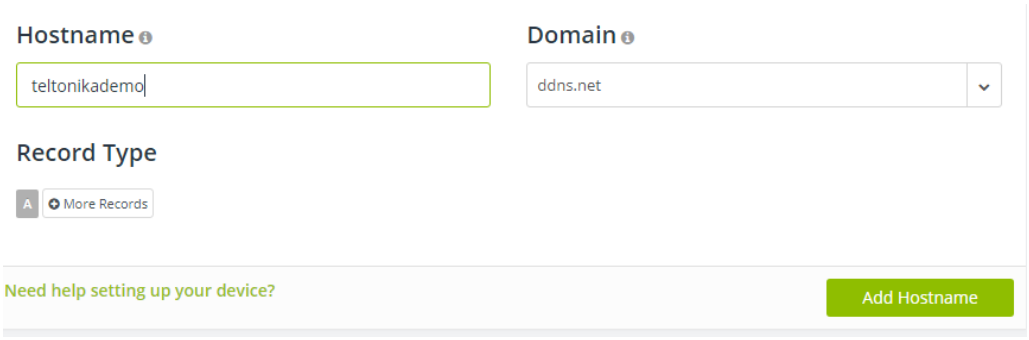
- Go to the Dynamic DNS option, and create a new DDNS name



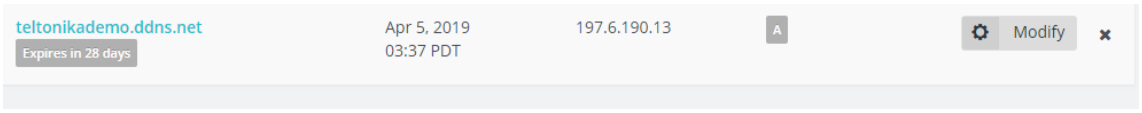
- Click on Edit or enter to advanced configuration



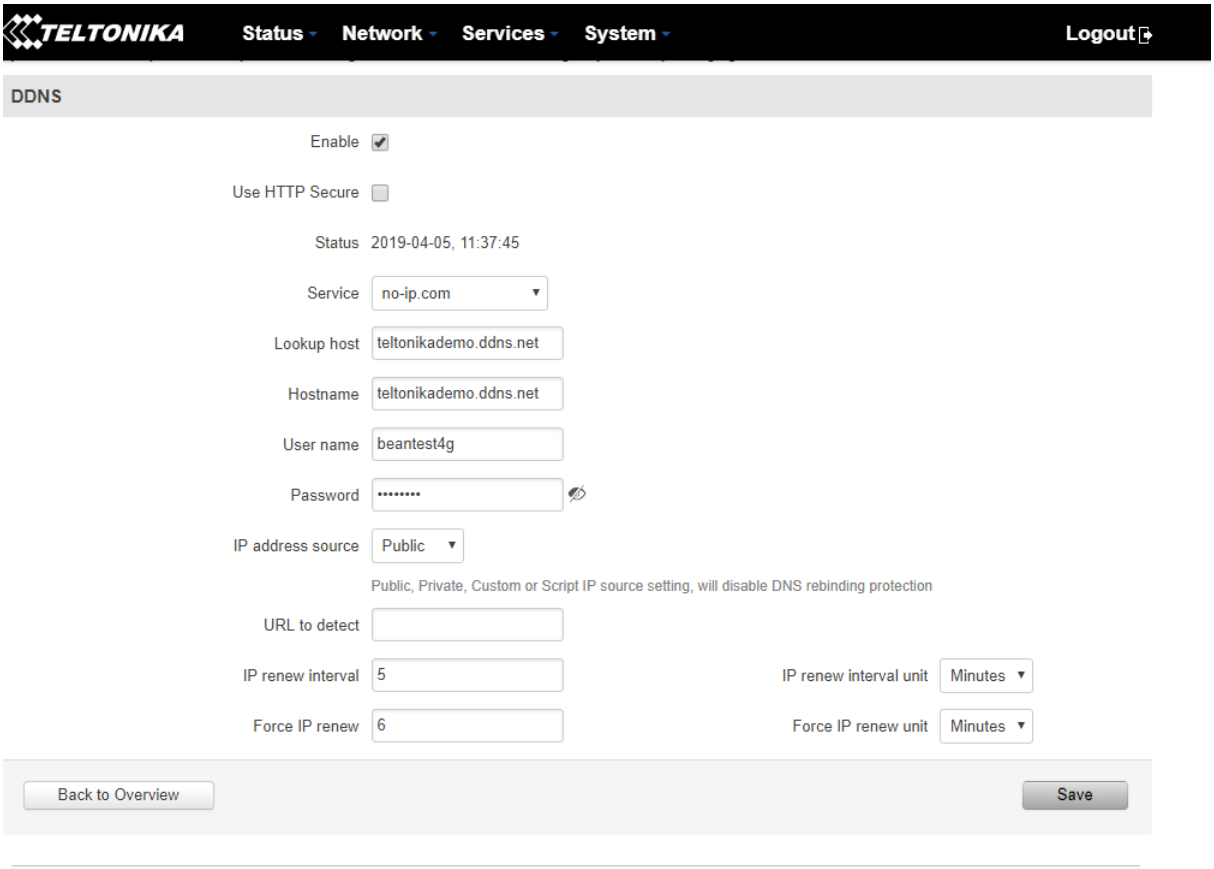
- Go to a No Ip DDNS provider and create an account then create a hostname. In our example we are using www.noip.com.
- It is recommended to use ddns.net as a Domain for the DDNS



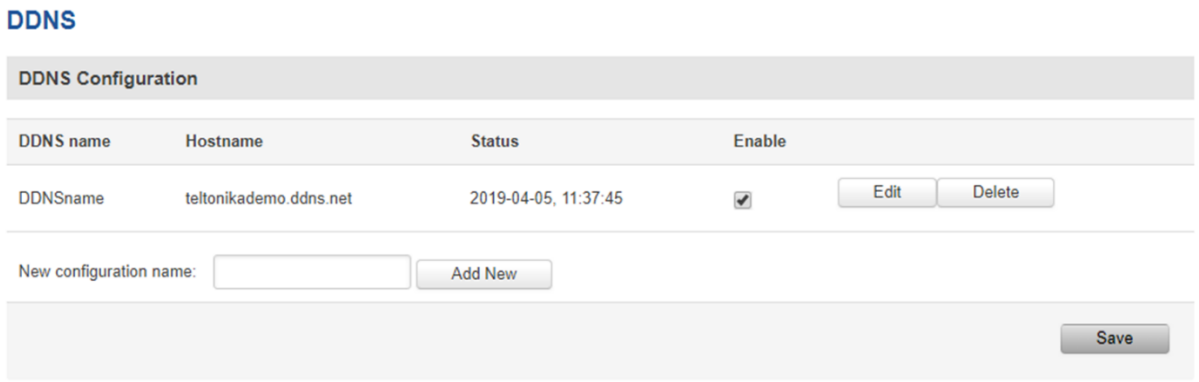
- The www.noip.com will detect automatically your Public IP. Make sure that you are connecting using your 4G Router during the configuration, otherwise you have to add the Public IP manually.



- 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



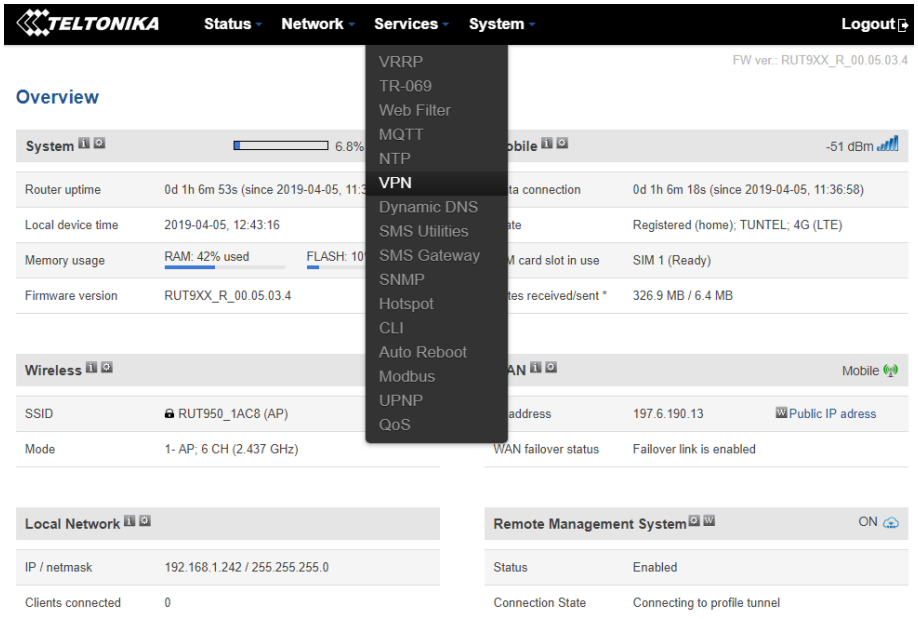
- Click on save and wait until the router establish connection, once the Status displays the date and the time that's means that the configuration is accepted.



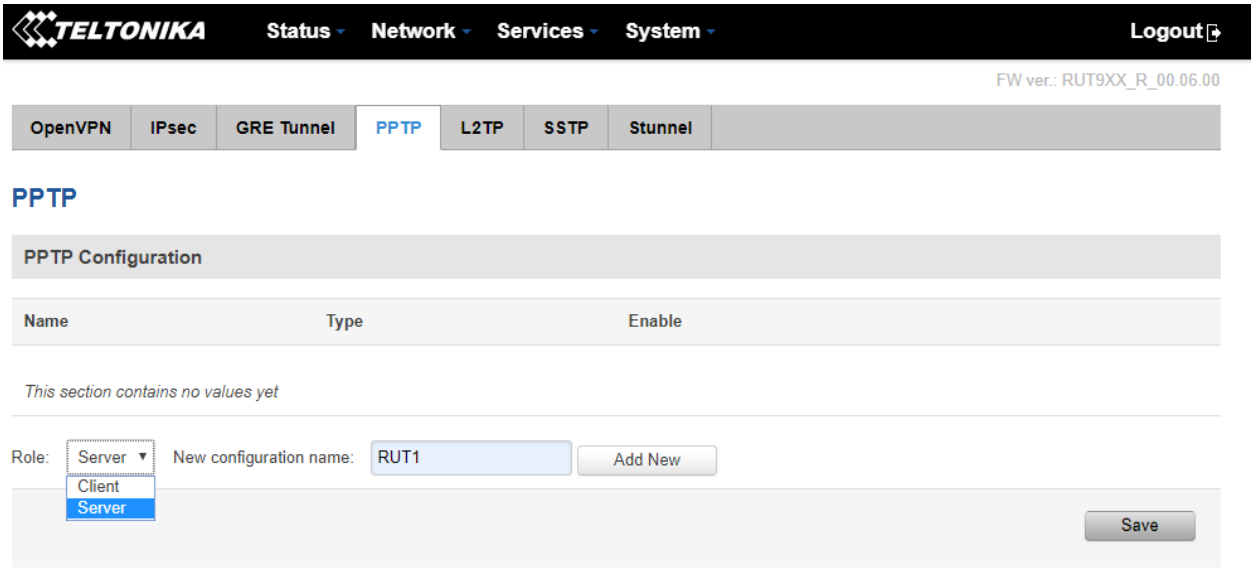
4.2 PPTP VPN

4.2.1 PPTP VPN Configuration

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

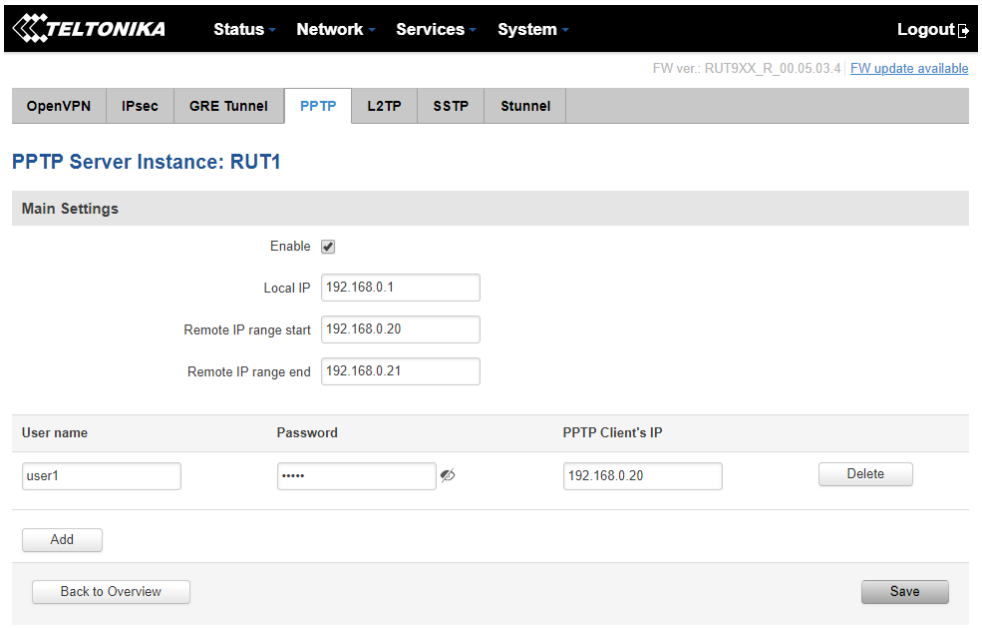


- Select to Go with a PPTP VPN and create a new Server.



- 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

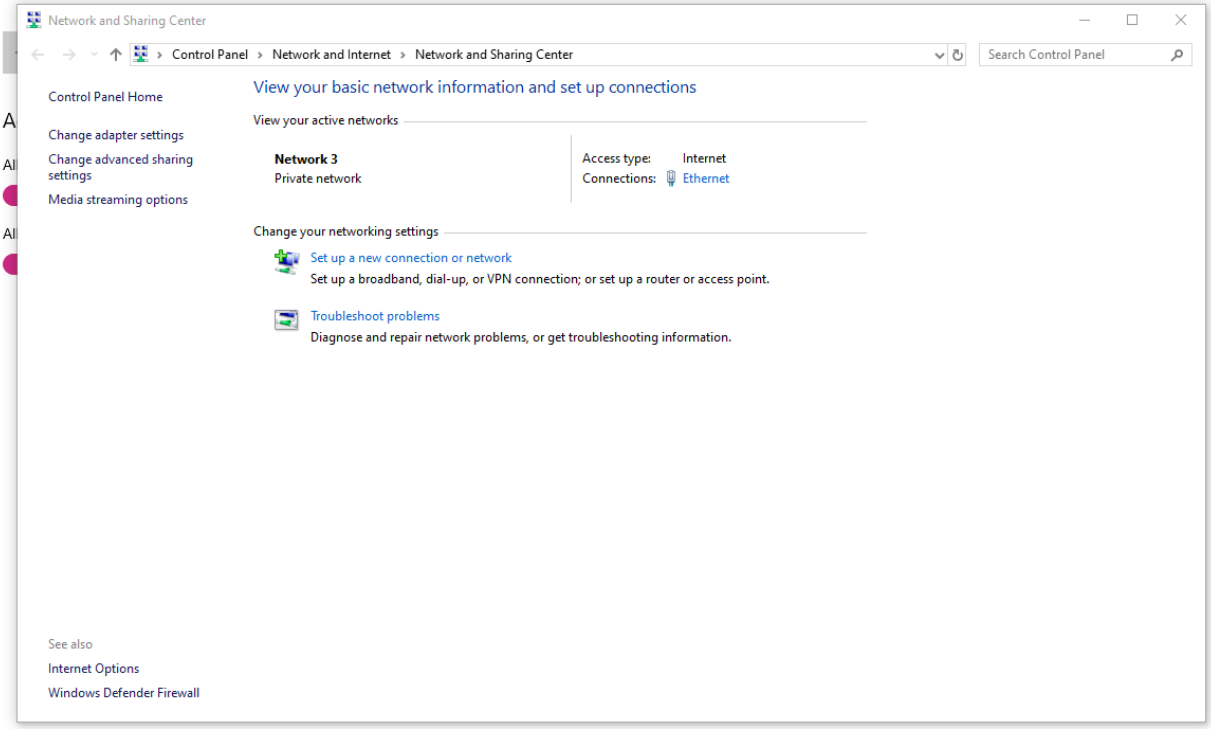


4.2.2 Distant VPN Client Configuration

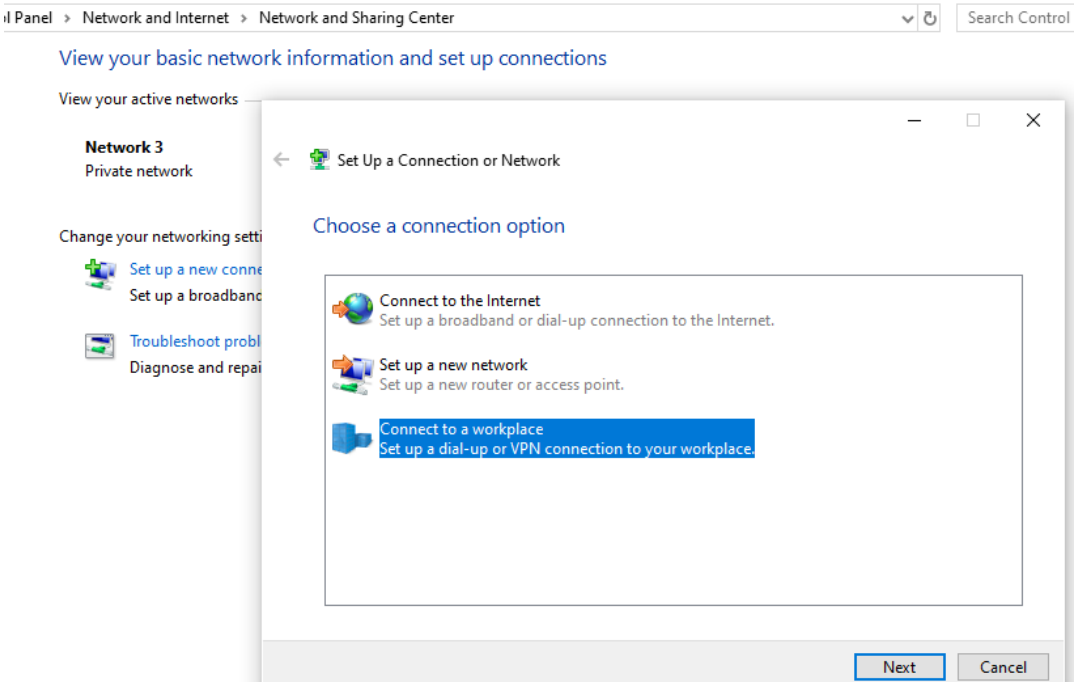
The VPN client is the distant computer situated on the office. User should configure a VPN connection to have access to the VPN server hosting his BeanGateway®.

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

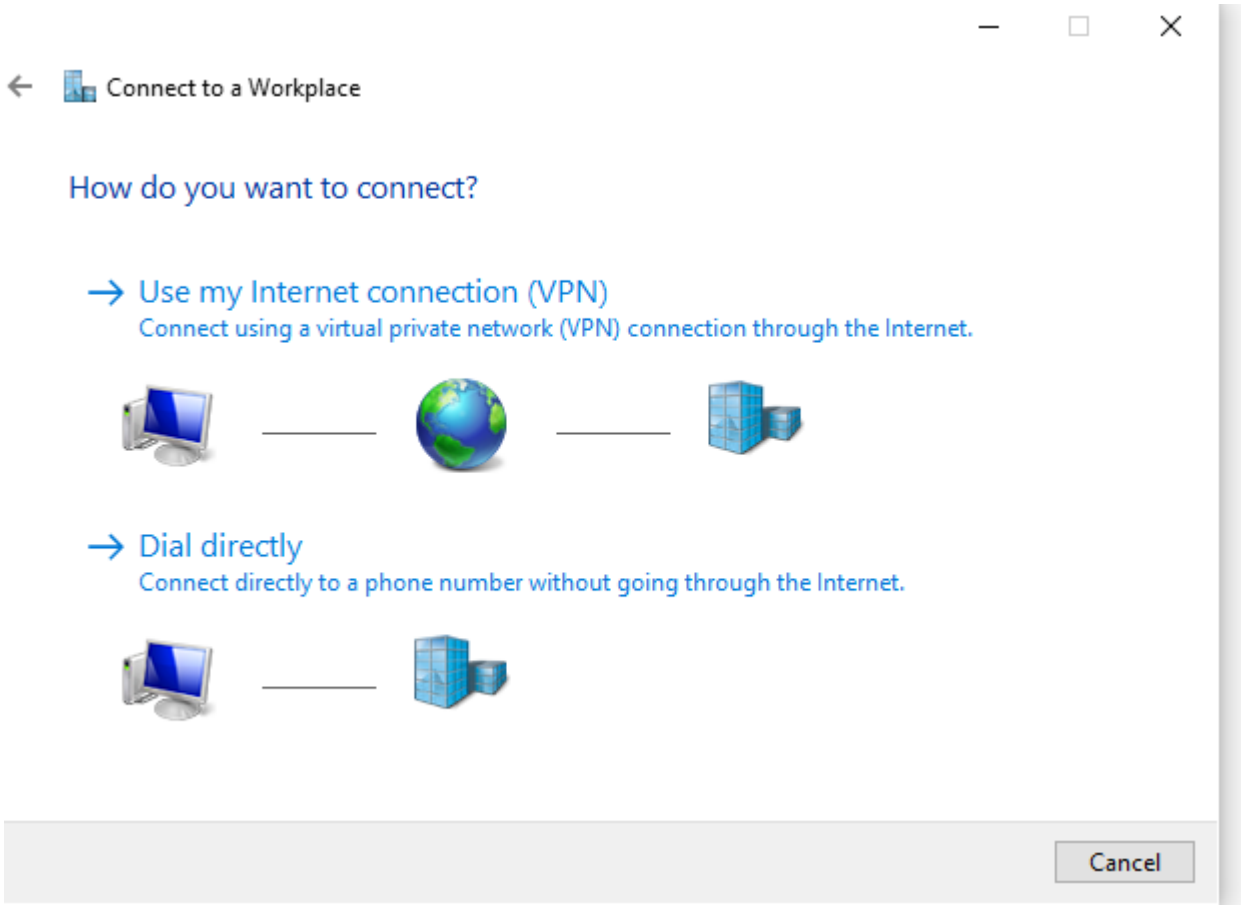
VPN



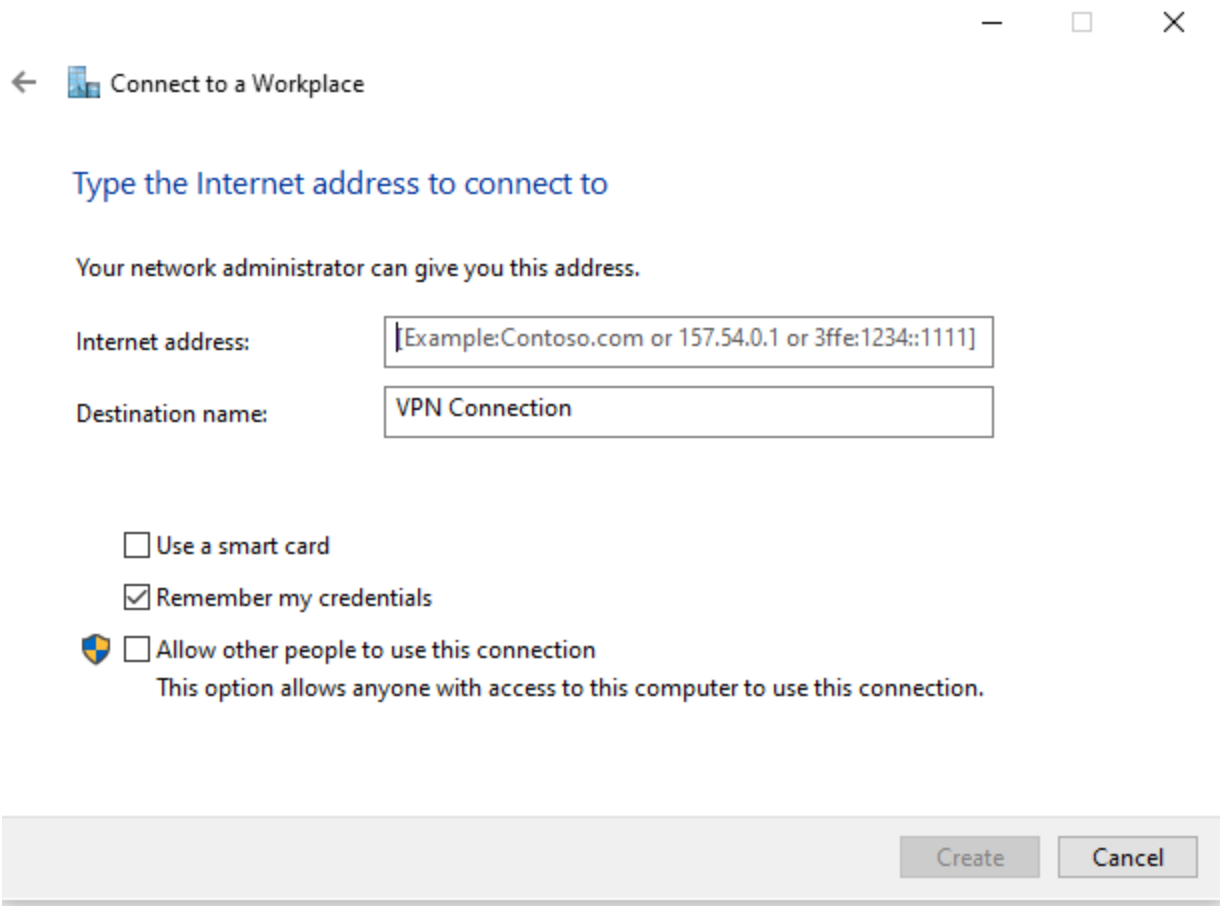
- Select Connect to a workplace



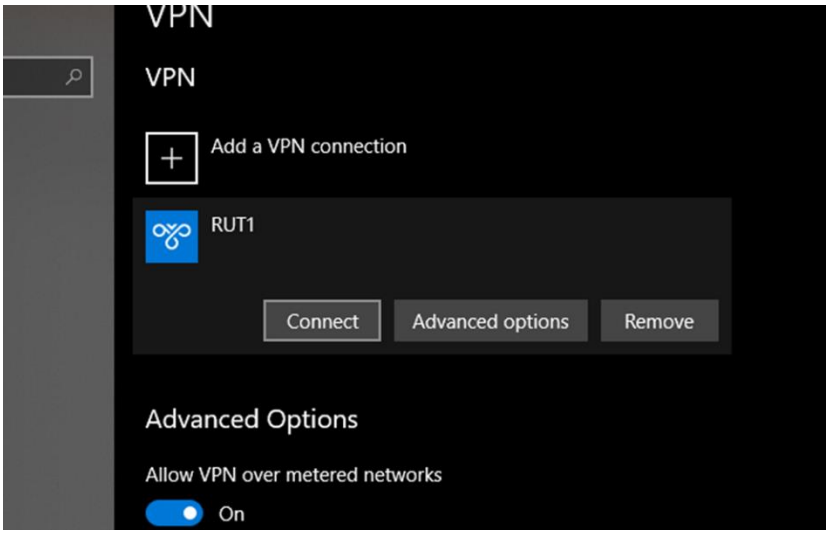
- Select Use my internet connection (VPN)

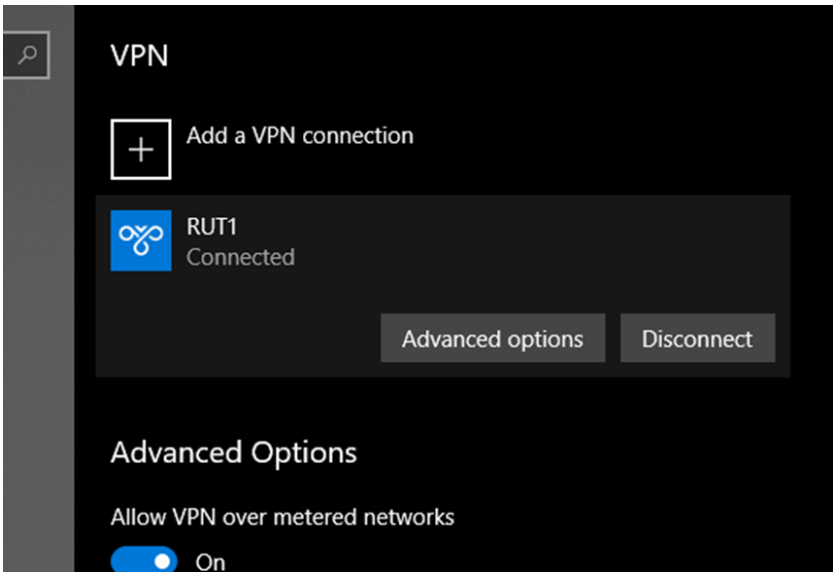


- Use the following inputs to configure the VPN connection
    - The name of the VPN server
    - The DDNS name assigned or your Public IP

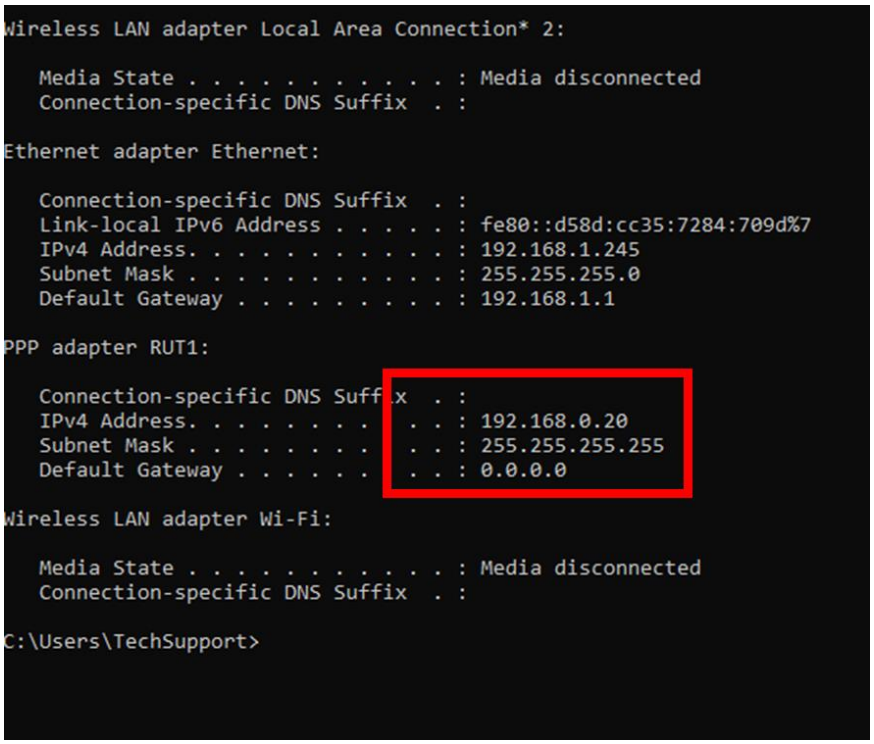


- The Computer is ready to join the VPN: Press connect

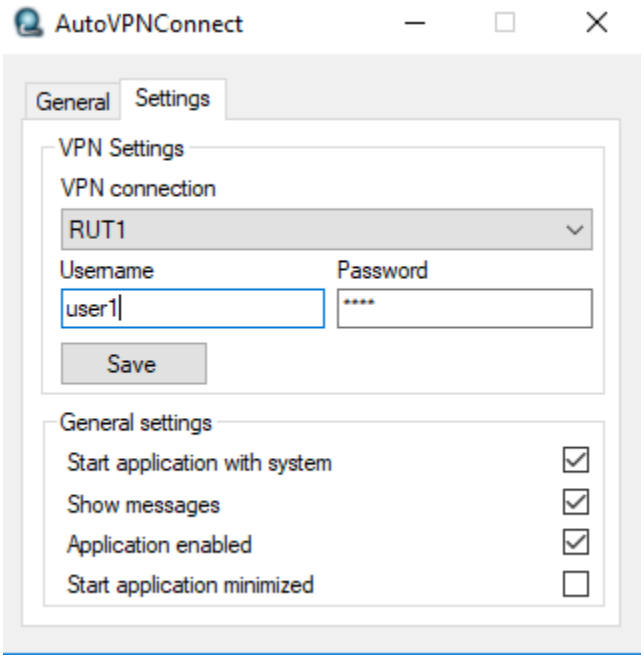




- Using IP config, user can figure out that he is connected to the VPN



- 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

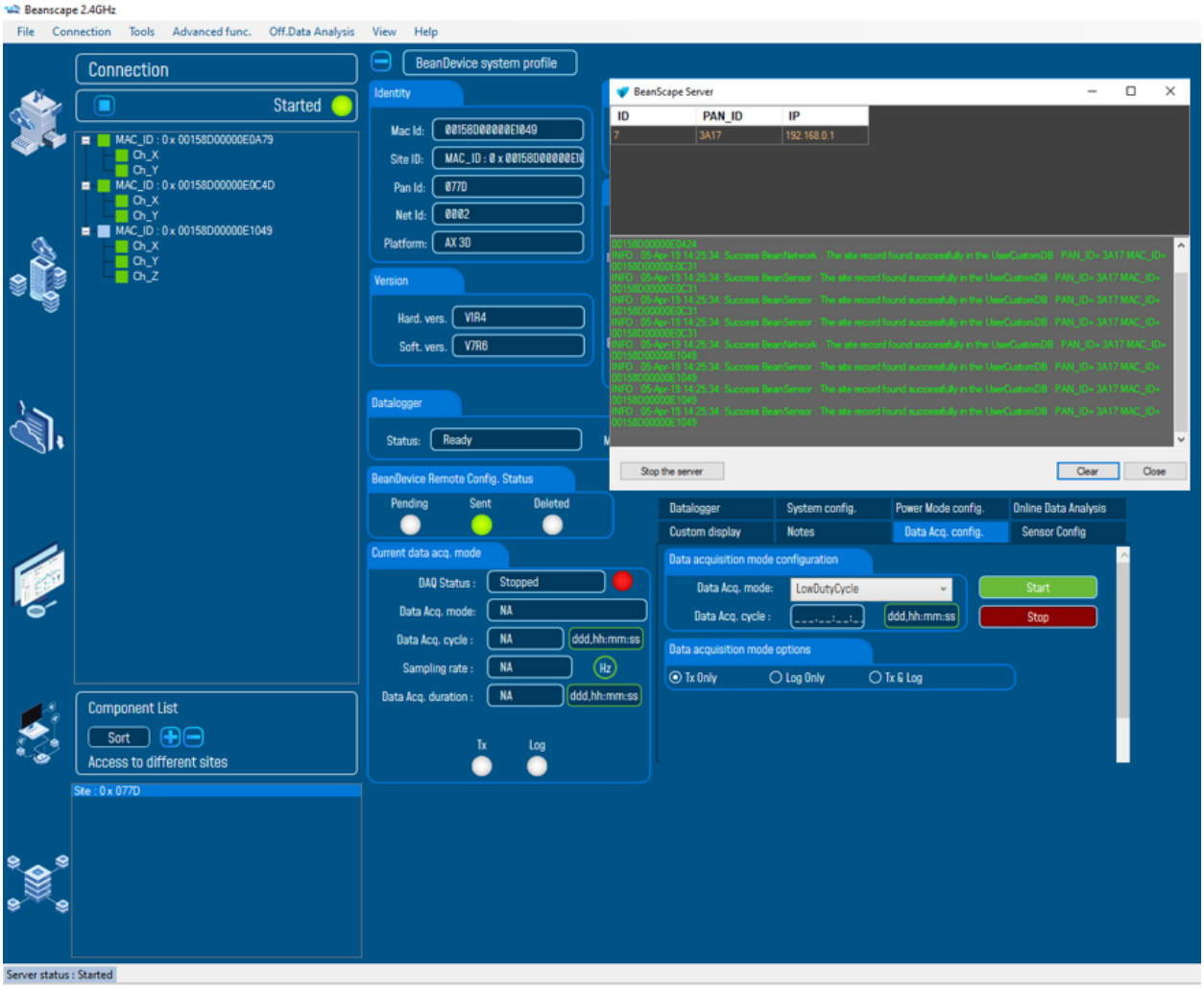
- Connect your laptop to the 4G Router used to connect the BeanGateway
- Run BeanScape® 2.4 GHz
- Go to Tools > BeanGateway Ethernet/LAN configuration
- Localize your BeanGateway
- Assign to the BeanGateway a Local Static IP (example 192.168.1.xx)
- On the BeanScape Frame, put the VPN first IP address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

4.4 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.

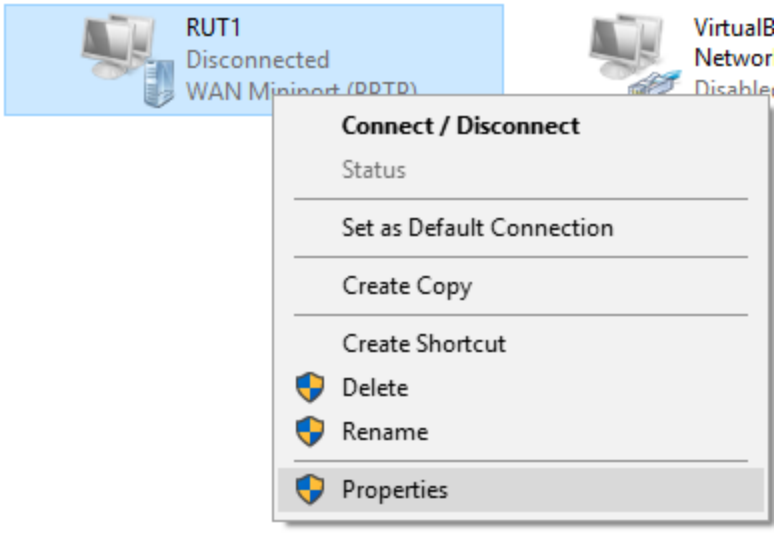
Open the BeanScape Server Window, you can figure out that BeanGateway flow is coming from the VPN server 192.168.0.1



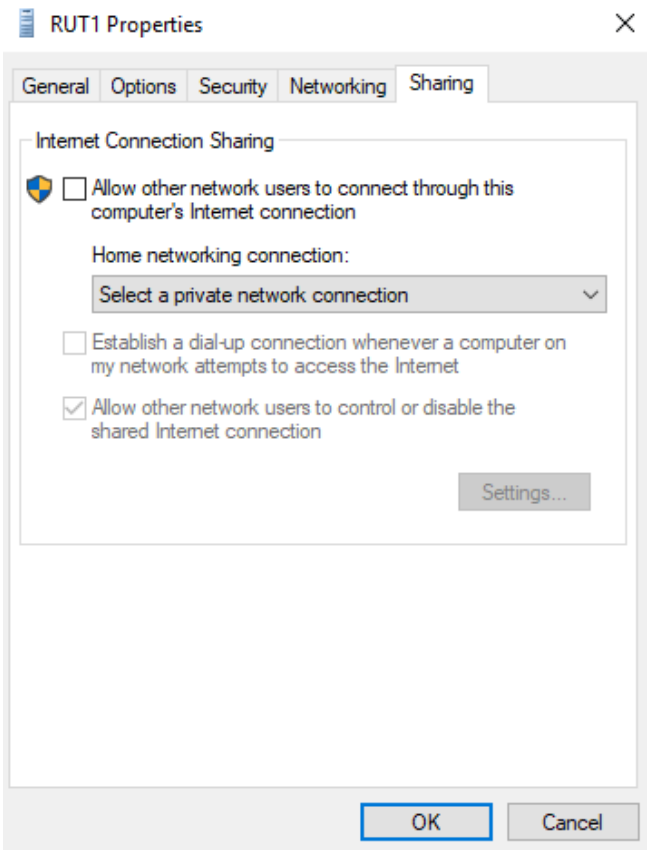
4.5 DATA CONSUMPTION

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

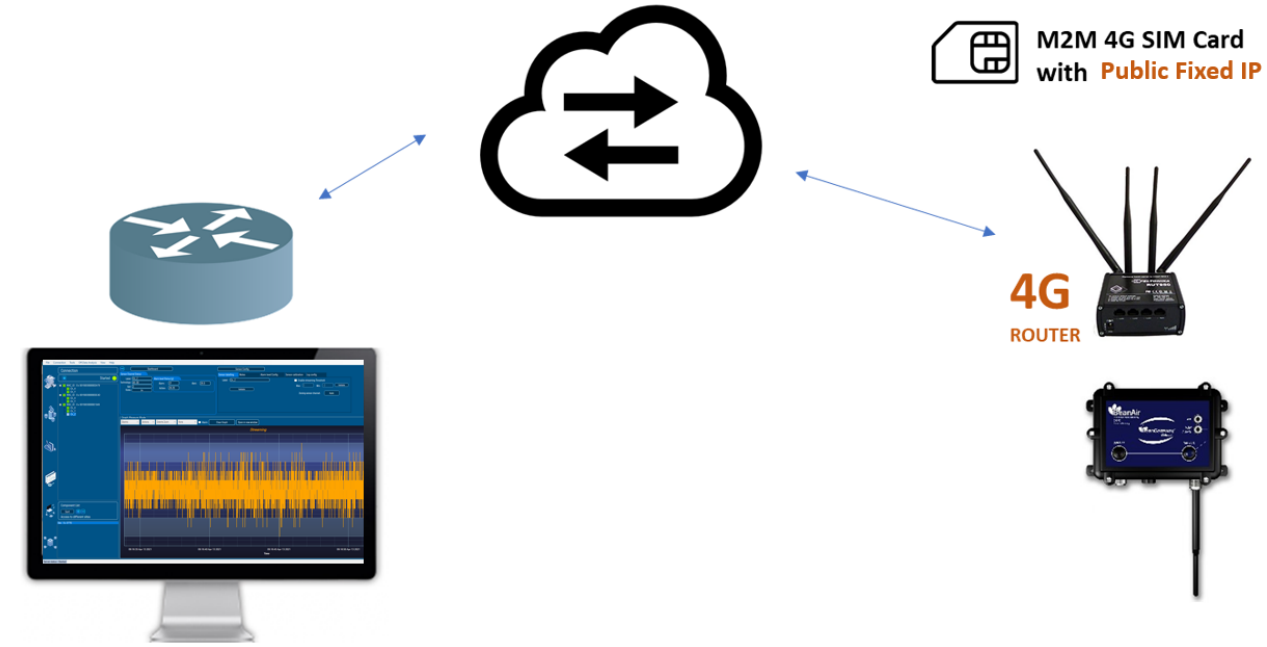


On the Sharing tab, make sure that the option is unchecked



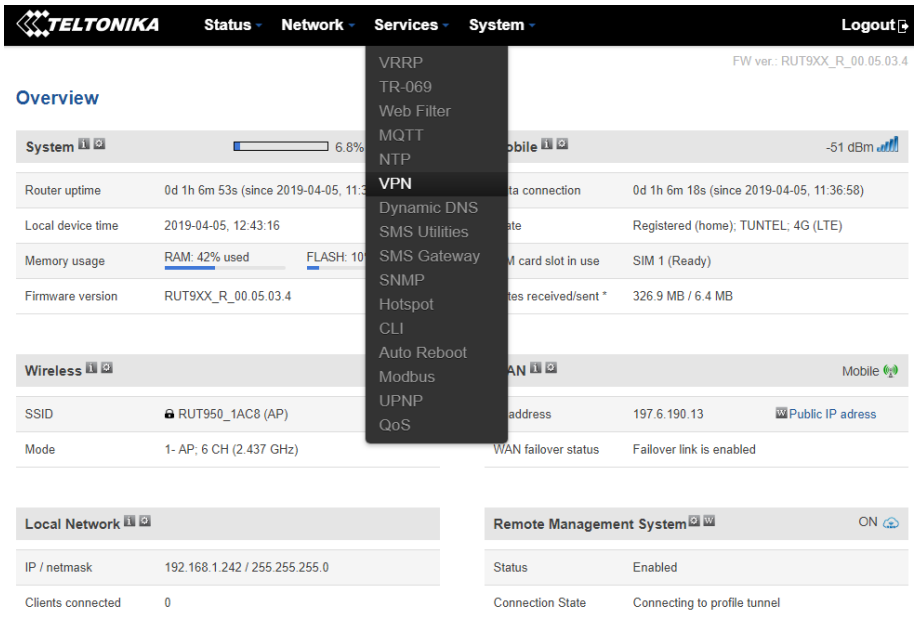
5. DIRECT VPN ACCESS WITH DISTANT PUBLIC FIXED IP

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

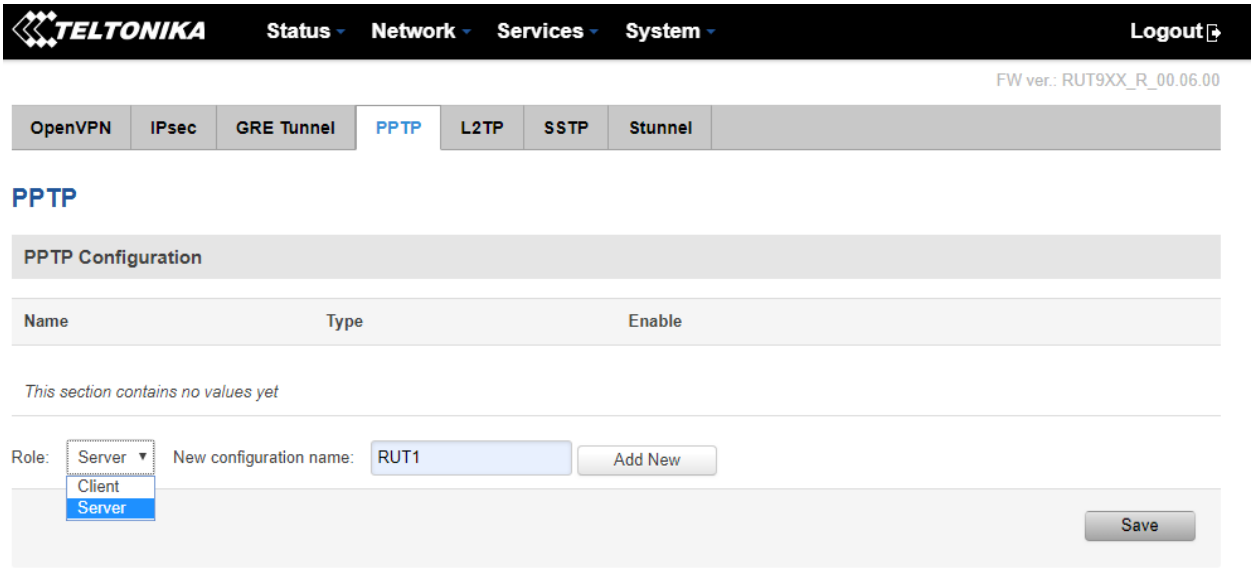


5.1 PPTP VPN CONFIGURATION

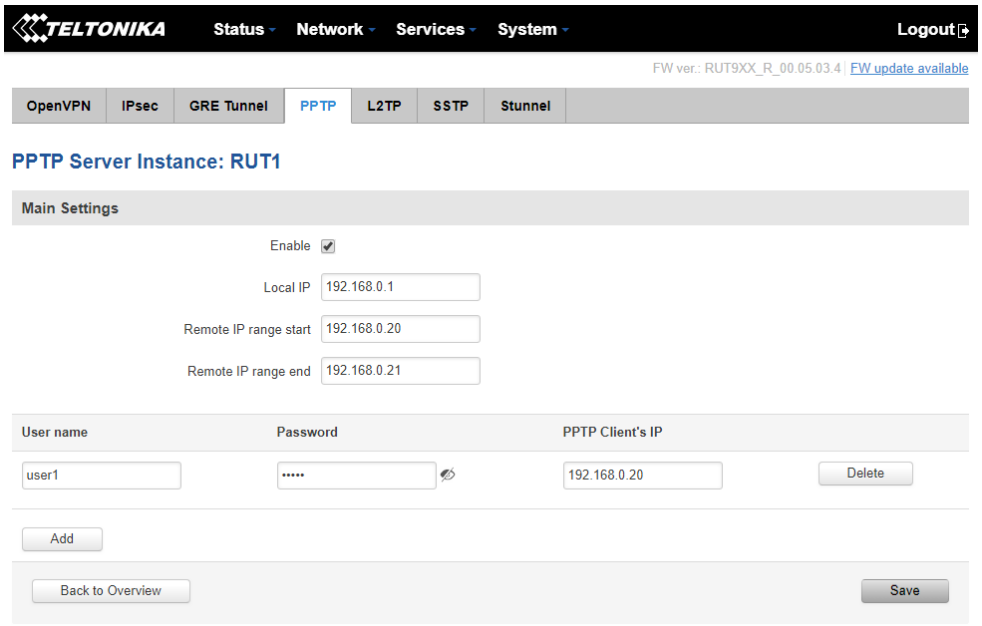
- On the 4G, Go to the VPN menu option



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



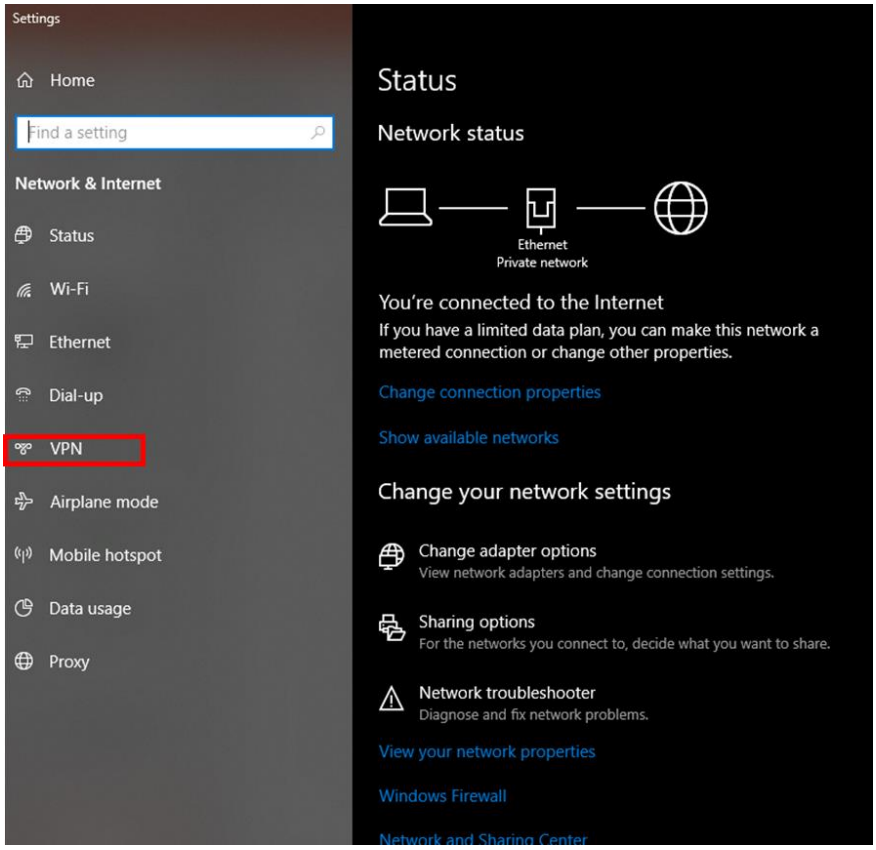
- On the advanced option:
  - Enable the PPTP VPN Server
  - Configure the VPN IP Pool: It is recommended that you serve maximum 2 addresses
  - Create username and a password for the VPN Client
  - Assign to the user the first IP address of the VPN IP Range



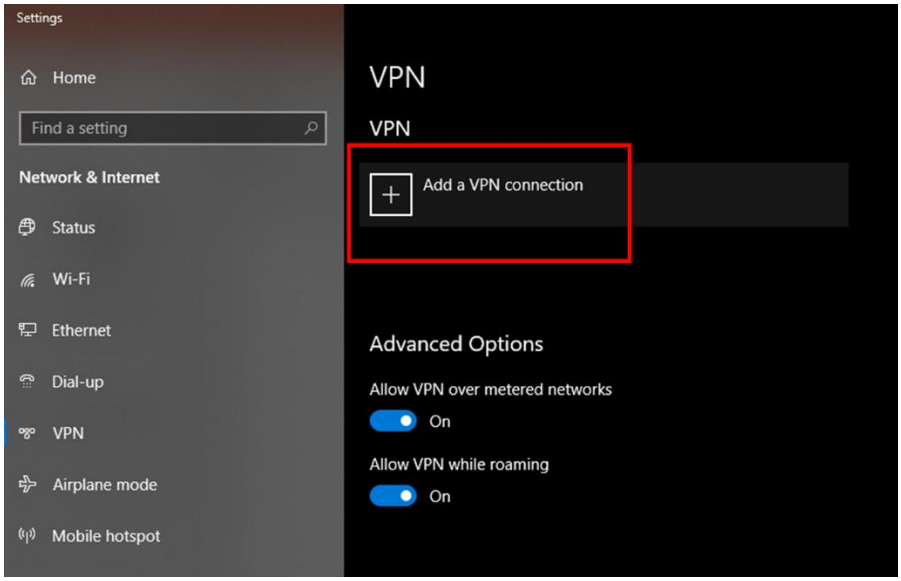
5.2 DISTANT VPN CLIENT CONFIGURATION

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®.

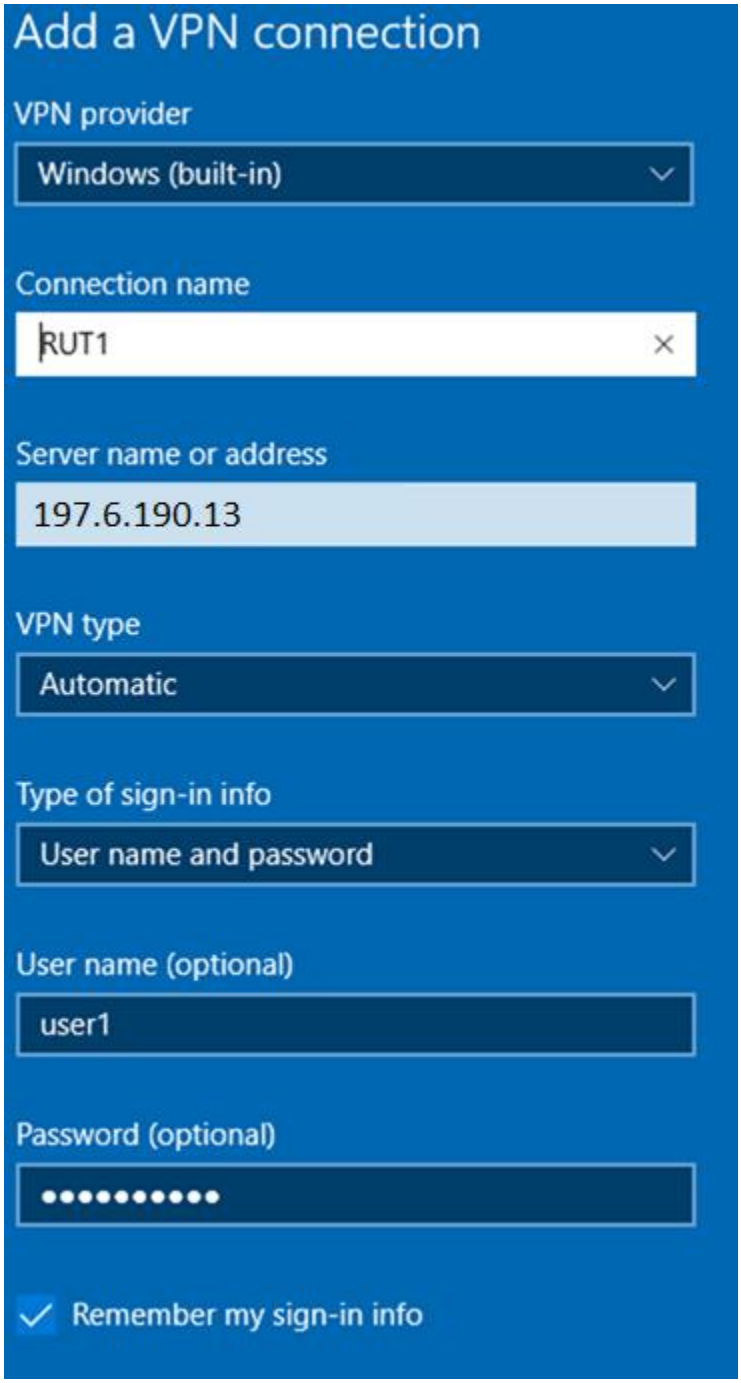
- Go to Network and Internet Settings (Network share center in Windows 7)
- Select VPN to create a new VPN connection



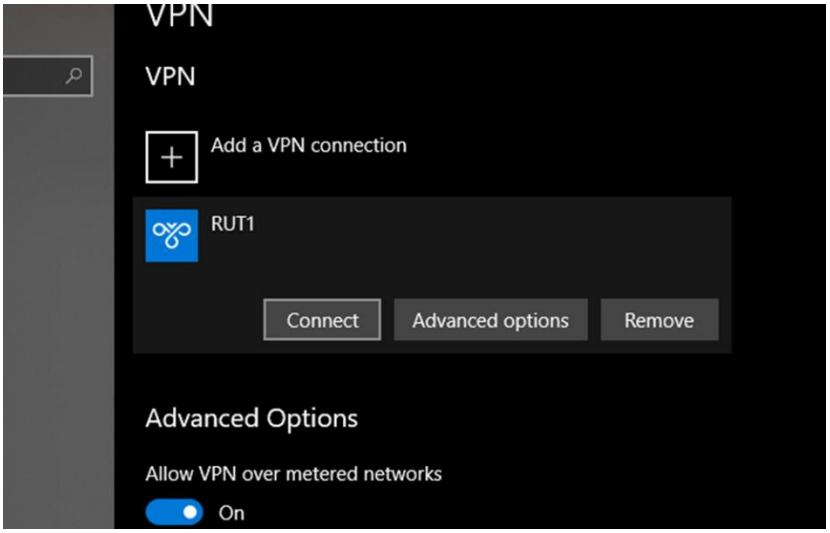
- Add a new VPN connection

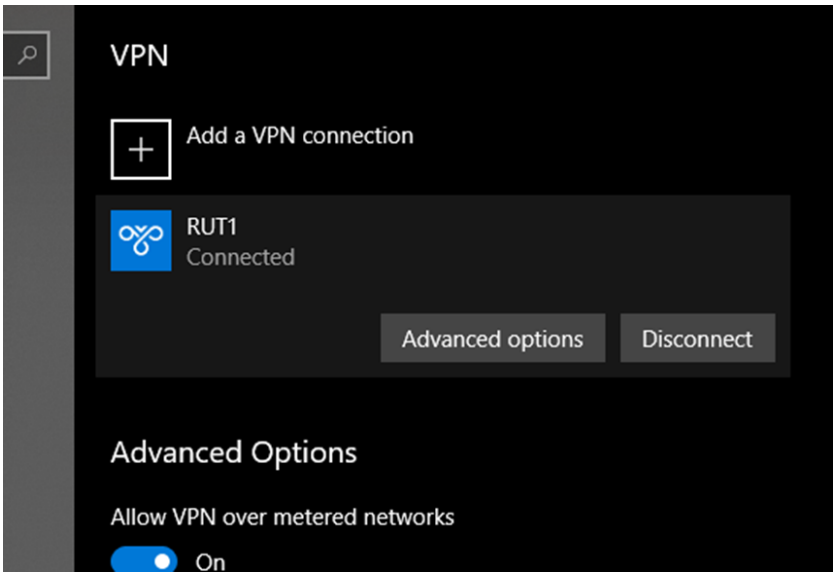


- Use the following inputs to configure the VPN connection
    - The name of the VPN server
    - The PUBLIC FIXED IP of the 4G Router
    - The VPN username created on the 4G Gateway and the Password

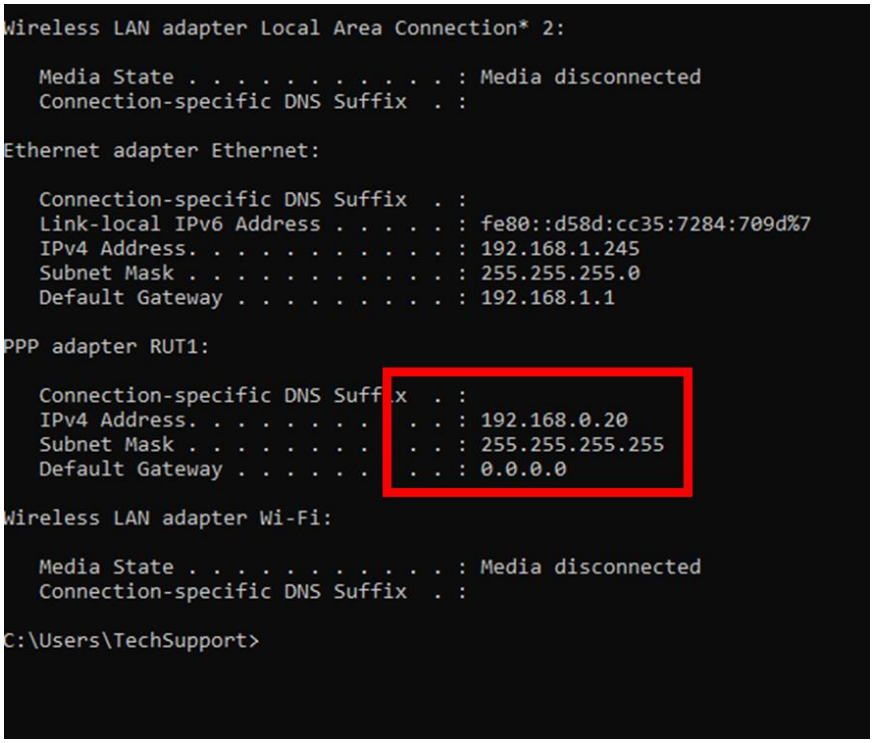


- The Computer is ready to join the VPN: Press connect

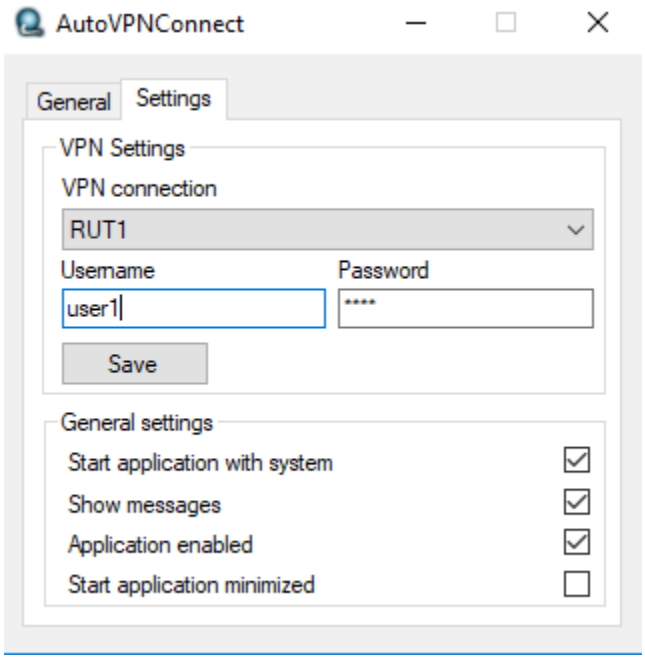




- Using IP config, user can figure out that he is connected to the VPN

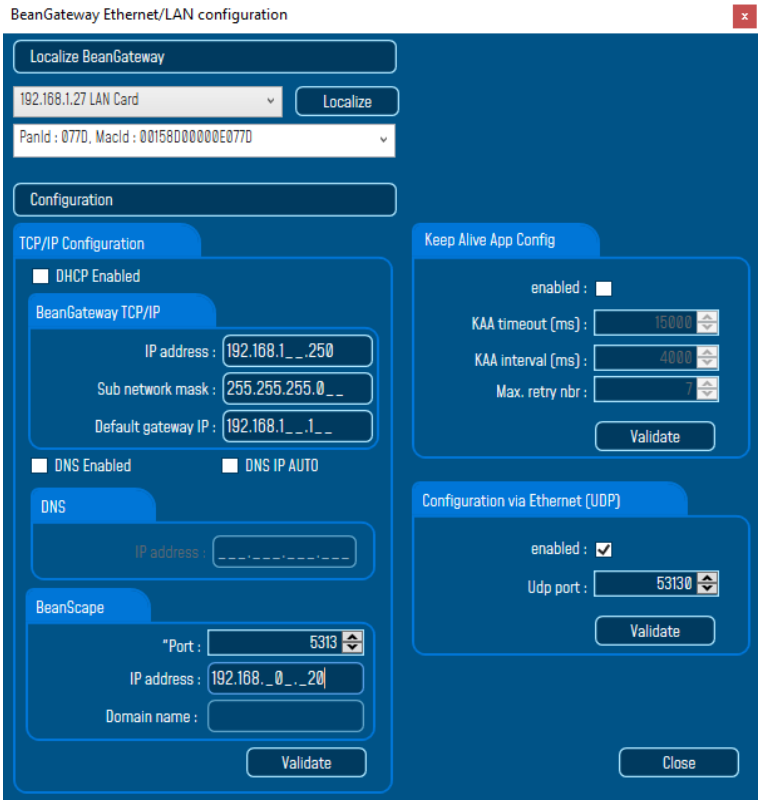


- Windows10 has removed the Auto Redial from the VPN connection, make sure that you Install AutoVPNconnect software after finishing the VPN configuration: https://sourceforge.net/projects/autovpnconnect/



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

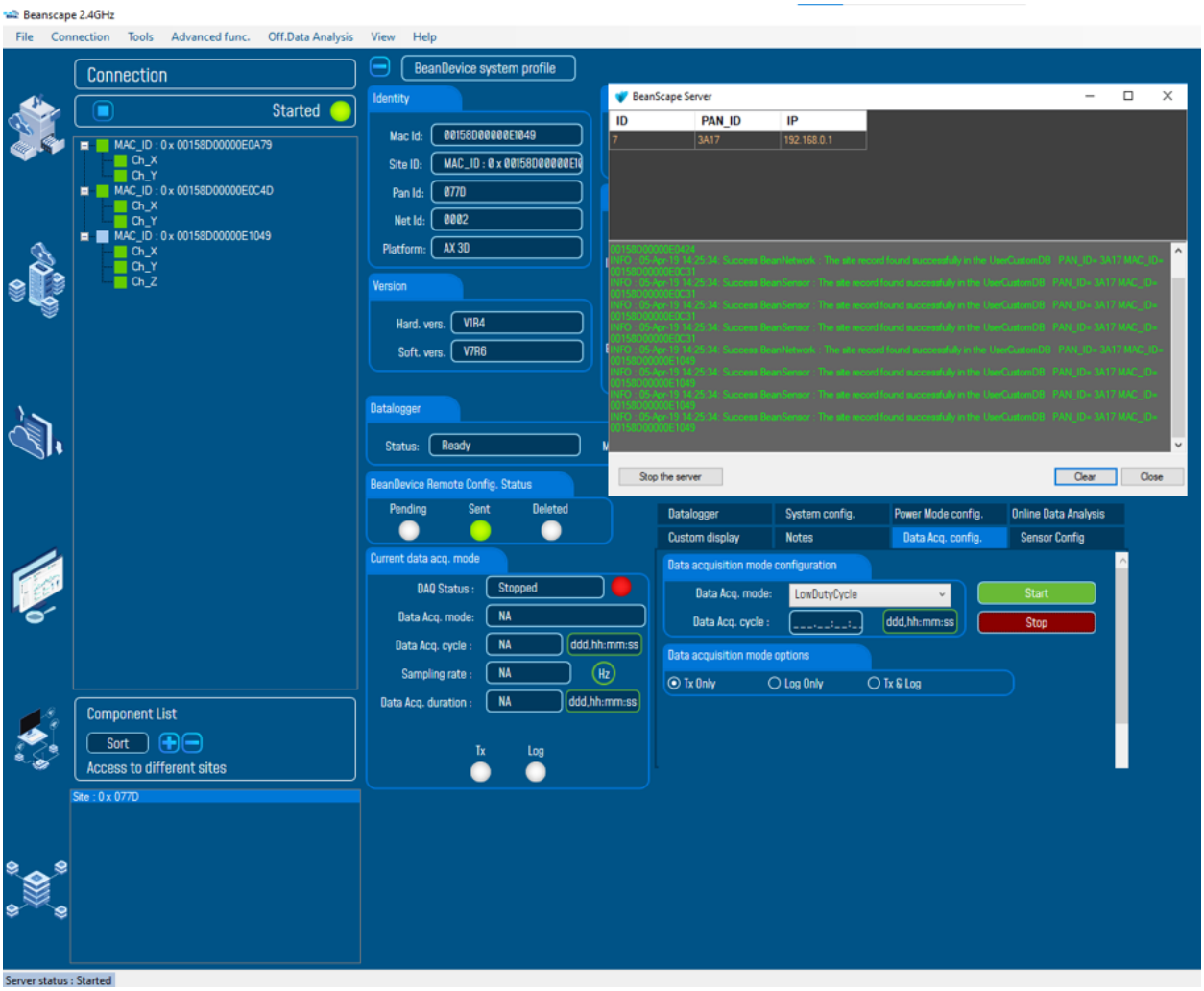


5.4 BEANSCAPE AT THE OFFICE

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

The BeanScape will display the BeanGateway profile.

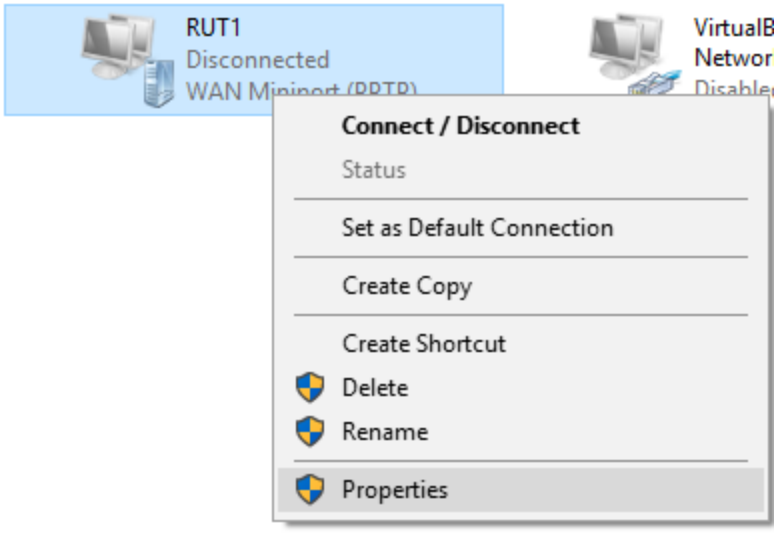
Open the BeanScape Server Window, you can figure out that BeanGateway flow is coming from the VPN server 192.168.0.1



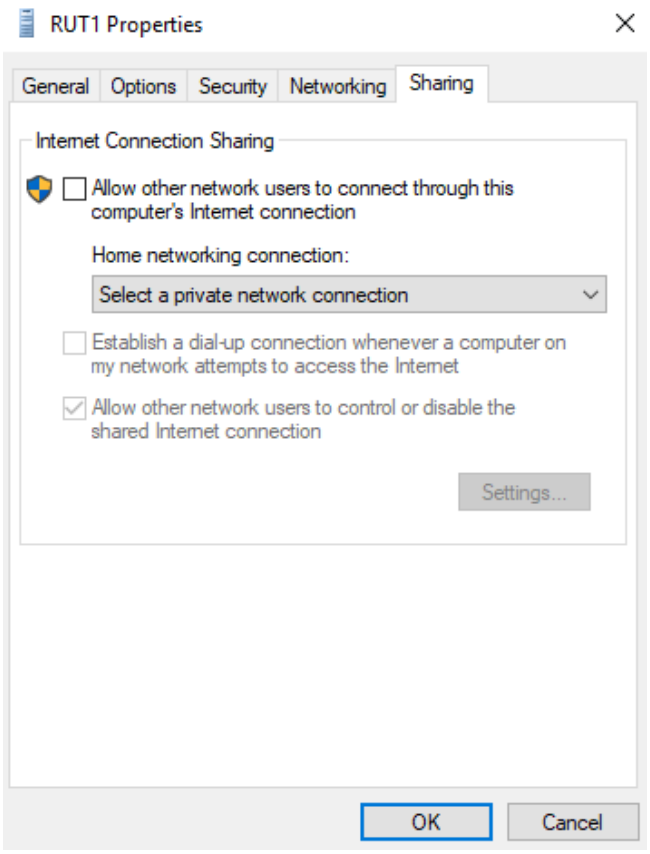
5.5 DATA CONSUMPTION

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

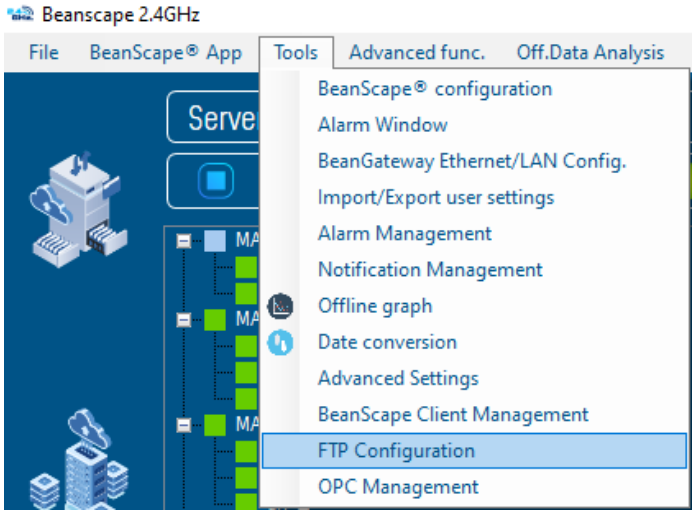


6. FTP SYNCHRONIZATION

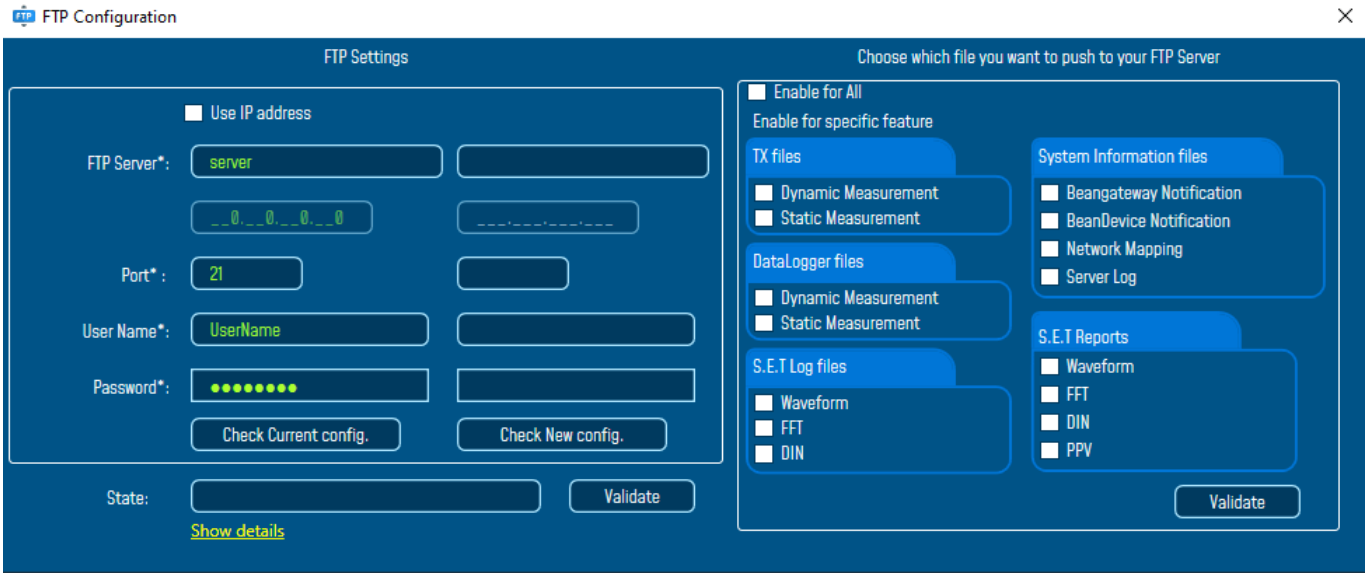
In some costumer cases, users prefer transferring Log files stored on their computers to a distant FTP Directory.

6.1 USING BEANSCAPE FTP FEATURE

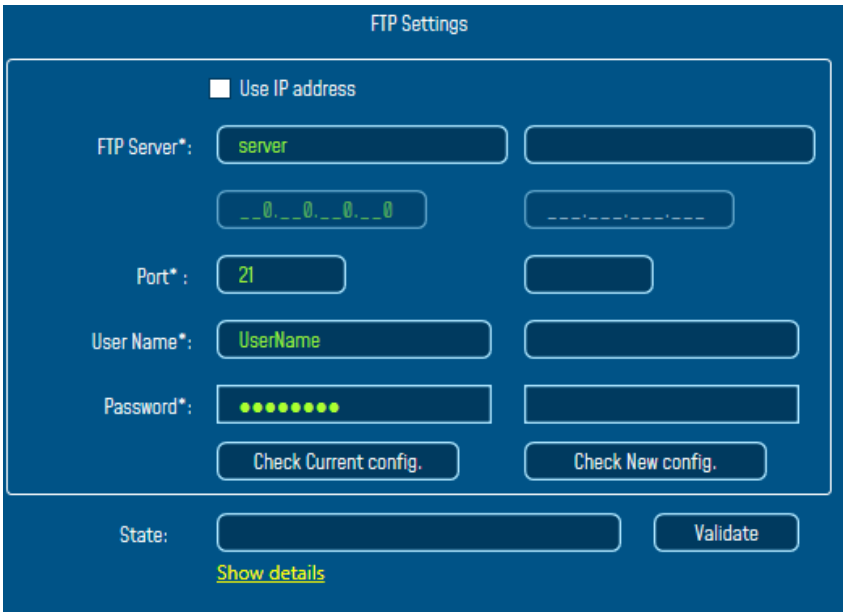
The user has the ability to send all his measurement data log files to the FTP Server through the FTP feature.



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

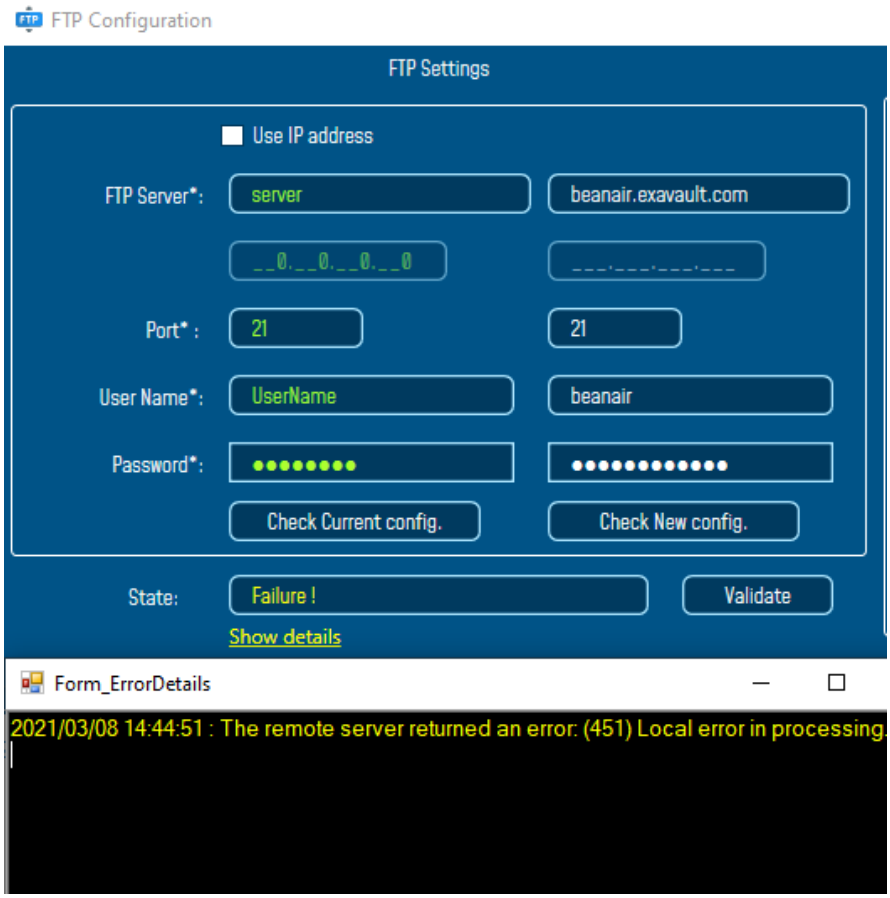


You should connect to your FTP server before setting up the FTP configuration on the BeanScape software.

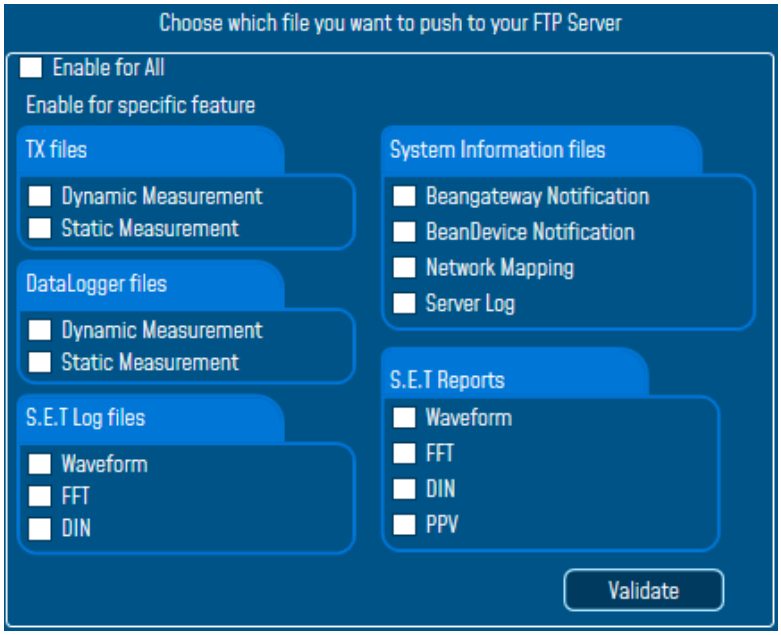


- **FTP Server:** Enter your FTP Server DNS or IP address by checking use IP address checkbox
- **User Name:** Enter your FTP user name
- **Password:** Enter your right FTP password
- **Port:** By default, the FTP port is 21, you can change it also
- **Check New Configuration:** click on check new configuration 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.

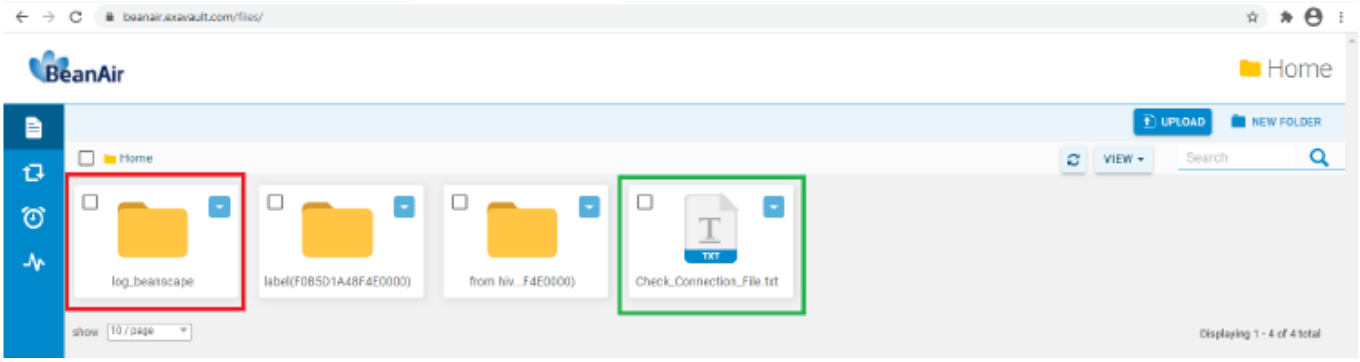
If the connection was failed, please click the Show details link to see the cause of the issue.



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.

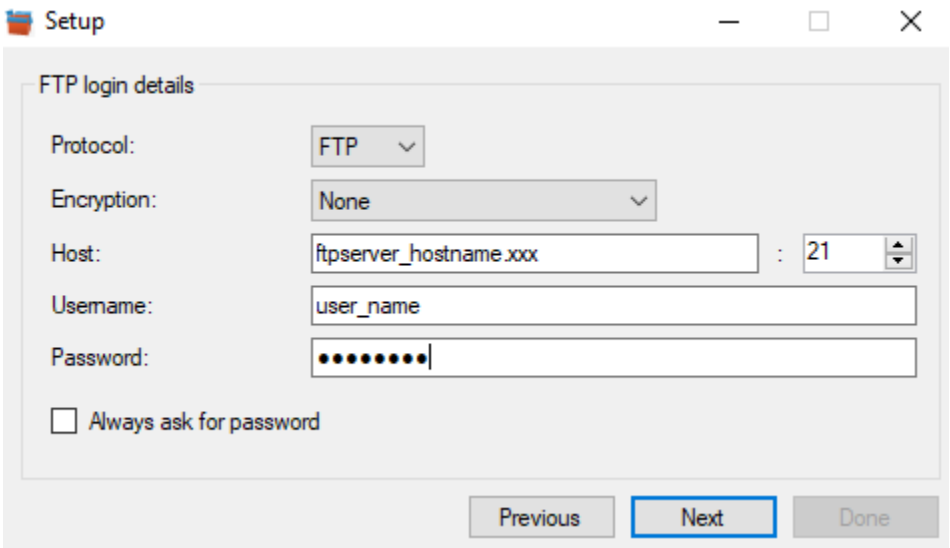


Watch the FTP Configuration video

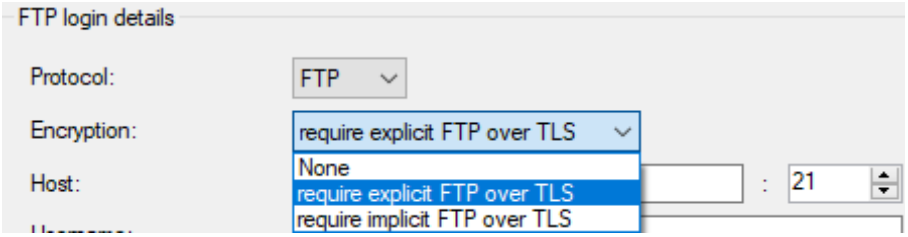
6.2 USING THIRD PARTY FTP SOFTWARE

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/

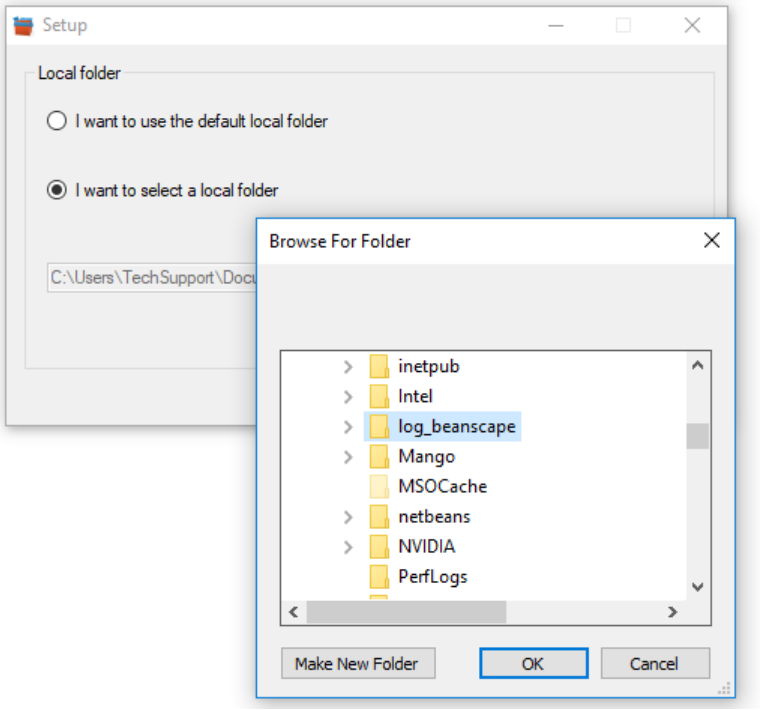
- After the installation, use the suitable language and setup the FTP parameters:



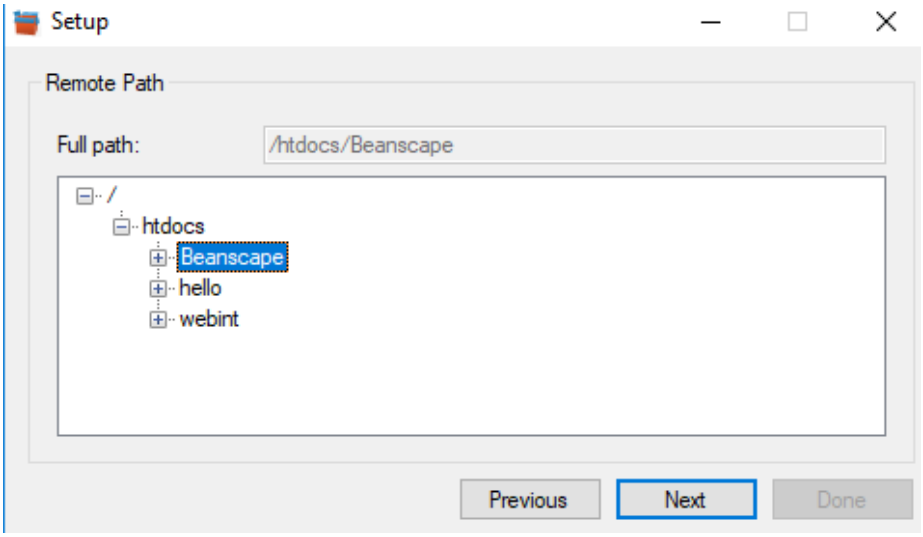
- If you prefer using TLS encryption, select the suitable option from the List below:



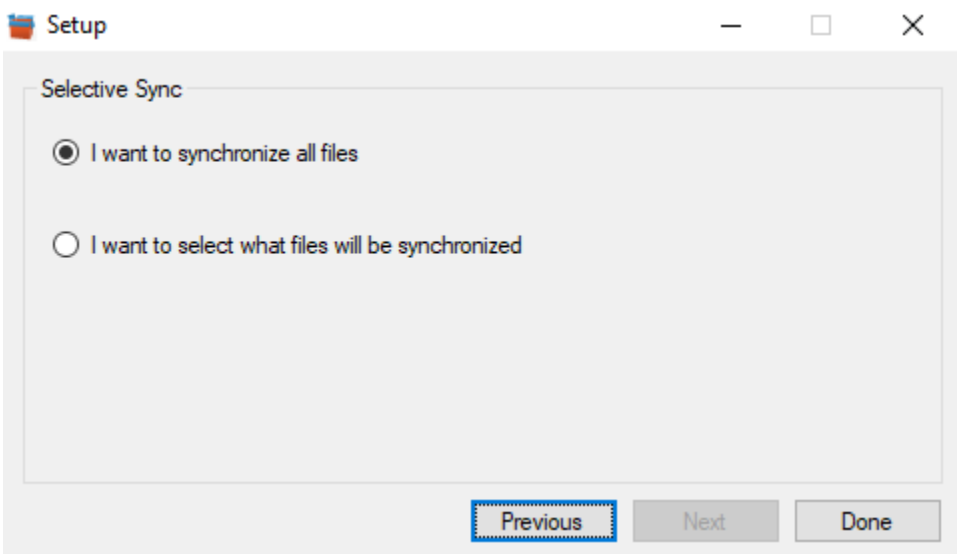
- Select the local directory used for the BeanScape Log files to be synchronized via FTP



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

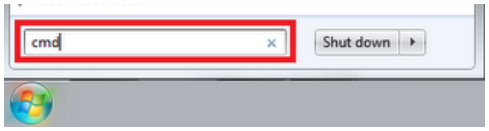


- Before finishing the setup, you have to configure the software to synchronize all files and directories in your Local Folder or precise which data should be synchronized.



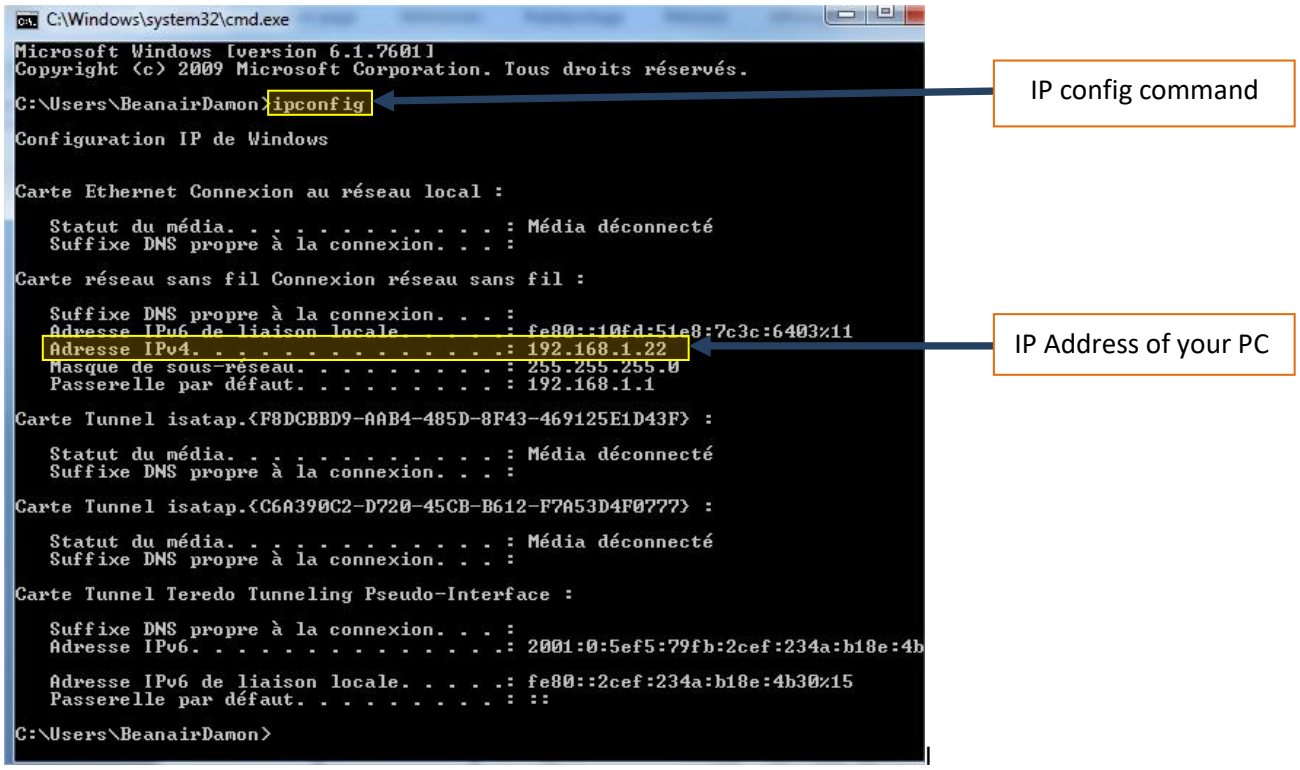
7. TROUBLESHOOTING

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 finded 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.



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