Ultrasound Solutions

VIGILANT

Powered by SDT

Quick start Guide

Version 4 – 2024

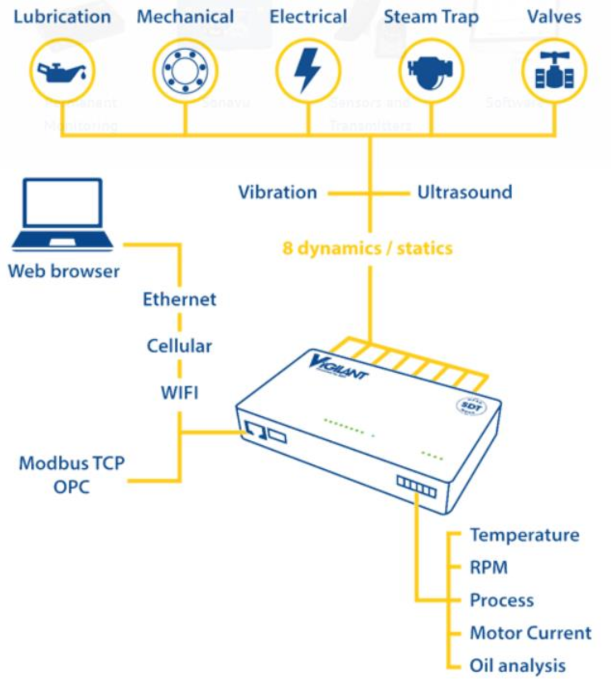
Table of Contents

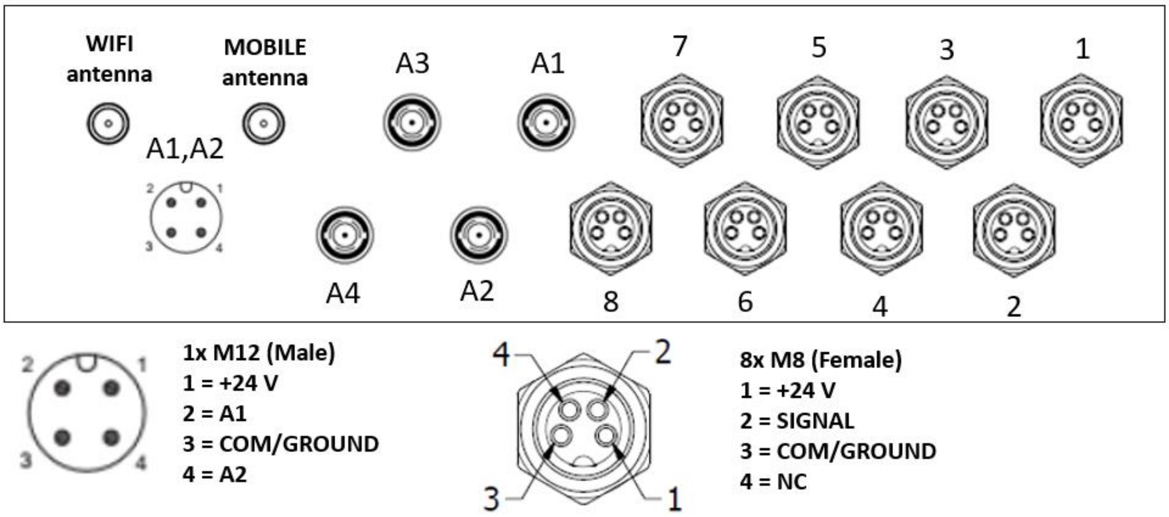
1. Introduction

VIGILANT is a suitable alternative for the permanent monitoring of installations or for the temporary monitoring of critical machines, allowing online monitoring with a quick and flexible installation.

It is composed of a main unit mounted in a rugged plastic carrying case with external connectors. The mobility case includes an internal modem for wireless communications (Wi-Fi-2.4GHz/4G/WAN-LAN). This set allows for quick installation, and is ideal for testing or temporary applications, putting online condition monitoring in portable mode.

The Mobility case has M8 connectors on the rear panel that connect to each analog input, which are specifically designed for most applications requiring both standard IEPE accelerometers and SDT ultrasound sensors (CONMONSENSE RSV 0-10V or RSIE (IEPE)). Other types of industrial sensors, such as tachometers, temperature sensors, requiring an external power supply are also compatible with *VIGILANT*.





1x M12 (Male)
1 = +24 V
2 = A1
3 = COM/GROUND
4 = A2

8x M8 (Female)
1 = +24 V
2 = SIGNAL
3 = COM/GROUND
4 = NC

Rear panel view of the mobility case

2. Product essentials

Once installed:

- The main unit provides an easy access to the device from a web browser.
- Up 8 simultaneous dynamic acquisitions on analog channels plus 4 static analog channels.
- Does not require any external software or database.
- The monitoring mode and the storage strategies are fully customizable by the user. Data are displayed through a web interface which may be accessed from any web browser.
- Adjustable alarm levels, based on different kinds of events and conditions.

3. Packing list

- Mobility case.
- *VIGILANT* device, including pluggable terminal blocks for wire connections and DIN rail mounting.
- External AC/DC power adapter.
- External male M8 connectors.
- Wireless 4G/Wi-Fi + antennas, provided with the router (RUT 240, preconfigured by SDT).

4. Power and sensor wiring

As described in the specifications, *VIGILANT* must be powered by a nominal 24 V DC power supply. The Mobility Case includes an external power converter to adapt the AC power mains to the required DC level. The Mobility case has a connector for plugging the +24V DC power supply and an activation switch with indicator light.

⚠ WARNING

Be sure that power is off and remains off until the installation work is complete. Installation should always be carried out with the device isolated from the power supply or any source of electrical power.

The input range for the 8 dynamic channels in the main unit is ±24V Peak. These channels can be used to measure dynamic signals of different types of sensors (accelerometers, proximity probes, ultrasound sensors, etc.). All channels have an integrated IEPE power supply. The inputs are accessible from the back of the Case via connectors.

The Mobility Case also includes a 4-Pin M12 male connector and its corresponding female plug connector. This connector, redirecting to the static inputs (i.e. A1 and A2) can be used, for example, to connect a tachometer.

5. Starting up the device

VIGILANT has a start-up period of a few seconds (about 15 seconds). The *VIGILANT*'s status LED indicates the progress of the start-up.

After a short period in solid white color, the status indicator will start to flash orange. Then, the indicator should turn solid blue, which means the device is already operating successfully. If the status indicator continues to flash red/orange, it may mean that there is a problem with the system.

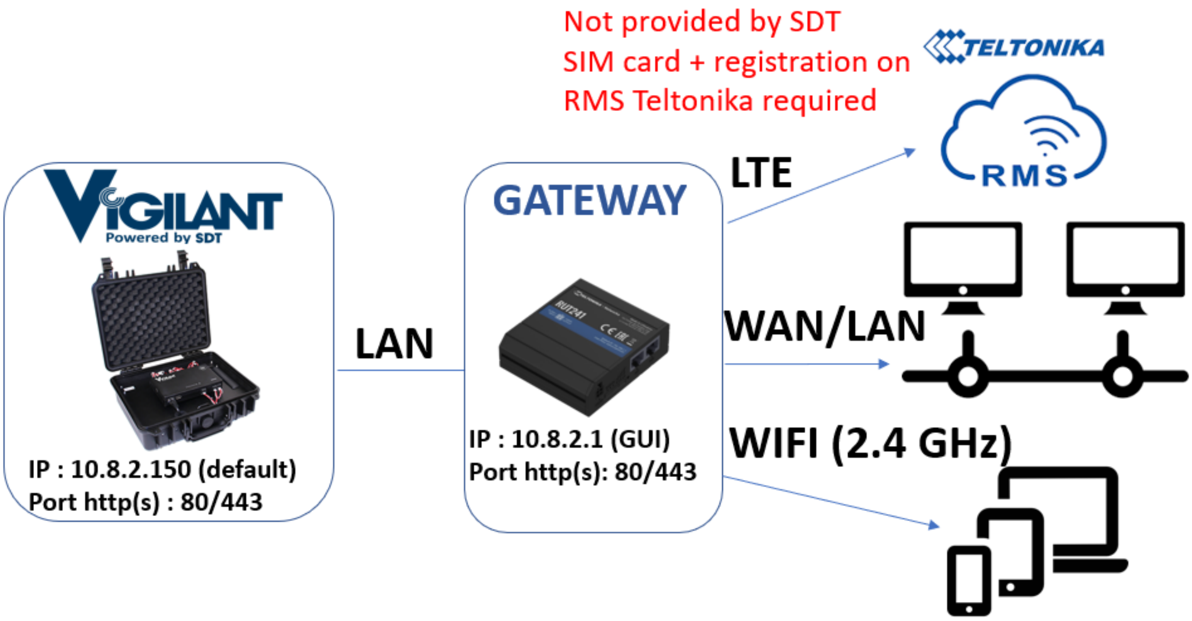
Please refer to the user manual for more details on the meaning of the LEDs.

6. Network configuration

The built-in web server of VIGILANT serves as your gateway to accessing and managing the system. It is designed to work with any standard web browser, ensuring easy accessibility. To facilitate a seamless connection, your PC (acting as the client) must be on the same network subnet as the VIGILANT system.

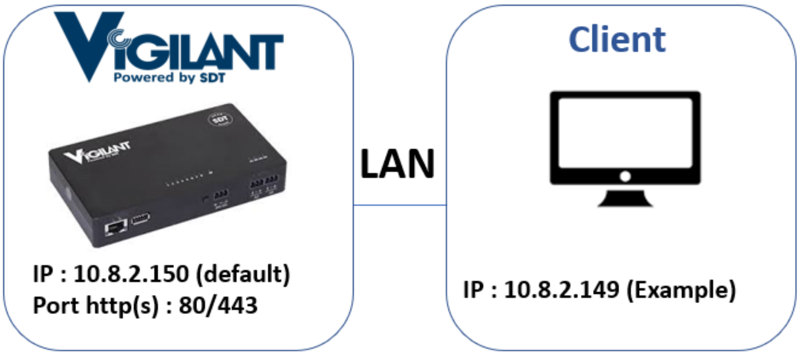
In the standard factory settings (SDT), you should adjust your client device's network settings to align with those of the system. This ensures that both devices are able to communicate effectively. The system is preconfigured to use a default static IP address of either **192.168.0.150** or **10.8.2.150**, which you will use to access the system's web server interface.

Additionally, the Mobility Case includes an optional router, offering versatile networking options to suit various operational needs. For a clear understanding of how to integrate your network, a network integration diagram, pre-configured by SDT, is provided in the figure below:



6.1. LAN

For the standard version, configure your client PC with a compatible static IP address.



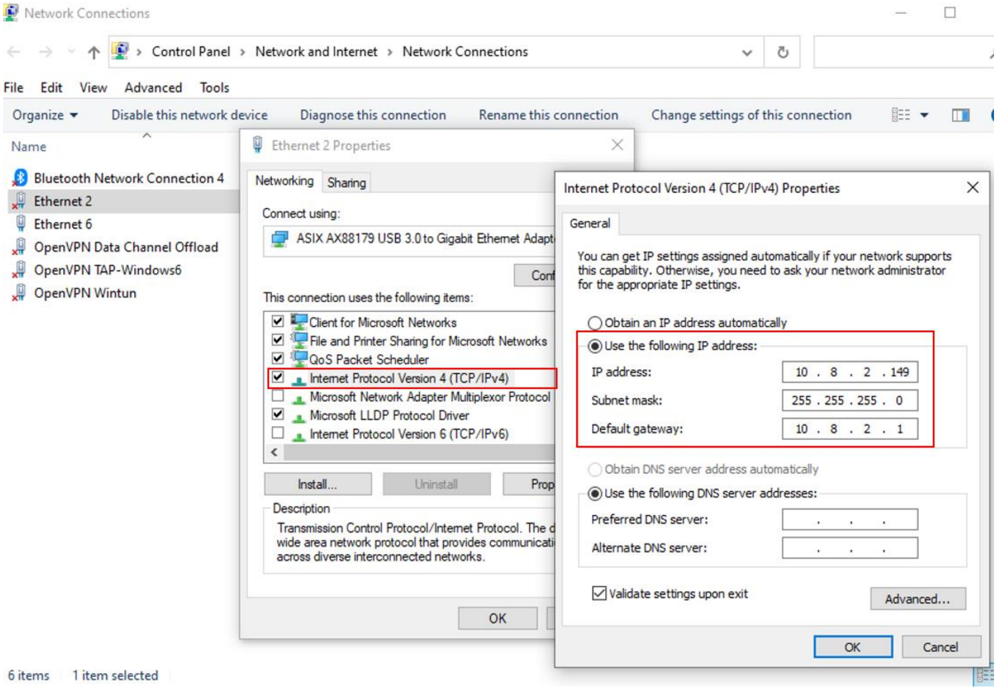
Proceed as follows for joining the LAN network:

- Connect the PC "client" to the VIGILANT with the cable;
- Configure the network, on the client's side (Windows assumed with administrator privileges).

On Windows, press ⊞ + **R** to open the run box, type **ncpa.cpl** + ↵ to open the network connection tool. Identify the corresponding network interface (Ethernet 2 in this example). Users can also access the tool at Control Panel/Network and Internet/Network Connections.

Right click on it, select **Properties** then double click on **Internet Protocol Version 4 (TCP/IPv4)**.

Assign the network settings, as shown in the image below:



Network Connections

Control Panel > Network and Internet > Network Connections

Ethernet 2 Properties

Connect using: ASIX AX88179 USB 3.0 to Gigabit Ethernet Adapt

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- □ Internet Protocol Version 6 (TCP/IPv6)

Description: Transmission Control Protocol/Internet Protocol. The d wide area network protocol that provides communicati across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 8 . 2 . 149

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 8 . 2 . 1

○ Obtain DNS server address automatically

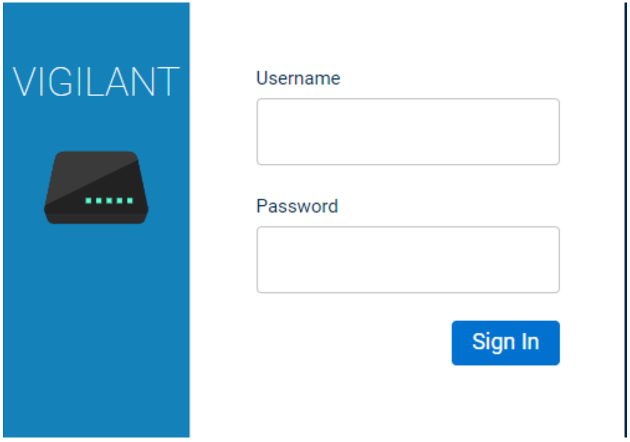
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☑ Validate settings upon exit

- Check **Validate settings upon exit** then press **OK**;
- Open a tab in your web browser, then type **10.8.2.150** to access the GUI



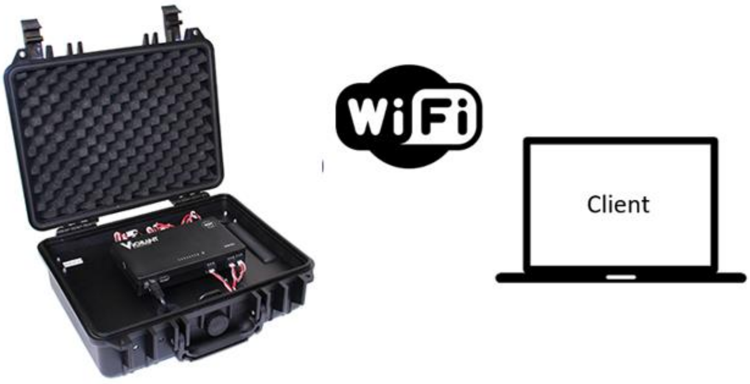
- Sign in as User: **Admin**, Password: **(see label attached to the unit**) to start configuring the system.

Certain units may be configured with a different default IP address (192.168.0.150). If you are setting up or troubleshooting network connections and encounter issues, adjust the network settings on your PC (ex: 192.168.0.149) to align with this factory configuration.

6.2. WIFI connection (Mobility case only)

The router included in the Mobility Case (or available as an option), is preconfigured by SDT to generate its own WIFI network (2.4 GHz only).

Proceed as follows:



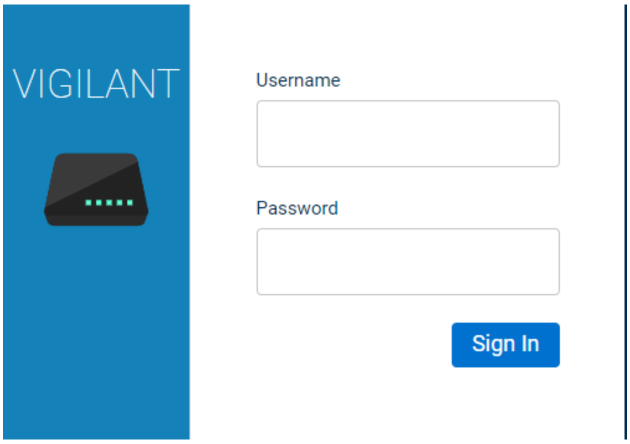
To connect to *the GUI* using Wi-Fi, follow these steps:

- Power on the system;
- Plug the Wi-Fi antenna provided in the package into the corresponding connector of the router;
- On the Client PC, scan and connect to the following WIFI access point:

  ```
  SSID: VIGILANT
  Encryption: WPA2-PSK
  WIFI PASS: MQUdWNOm
  ```

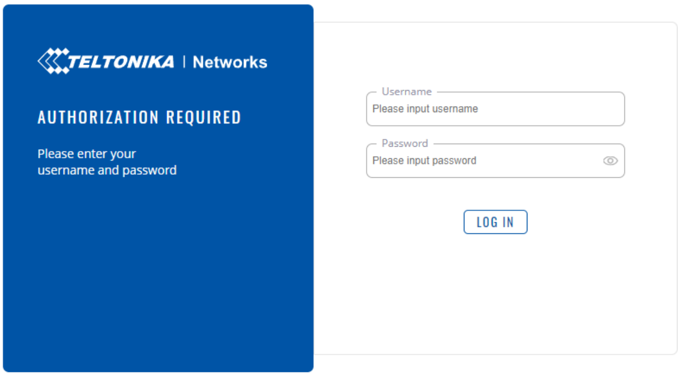
  The PC will automatically obtain an IP address in the LAN network.

  Once connected, users can also scan the network with an IP scanner freeware to better understand the network configuration;
- Type the *default* IP address **10.8.2.150 or 192.168.0.150**, in your web browser to access the GUI:



- Sign in as User: **Admin**, Password: **(see label attached to the unit**) to start configuring the system.
- (Advanced settings for IT) Open a new tab in your web browser to reach out the router configuration page at the following IP address.

  ```
  Router IP address: 10.8.2.1 or 192.168.0.1
  User: admin
  Password: SnE9qica
  ```



TELTONIKA | Networks

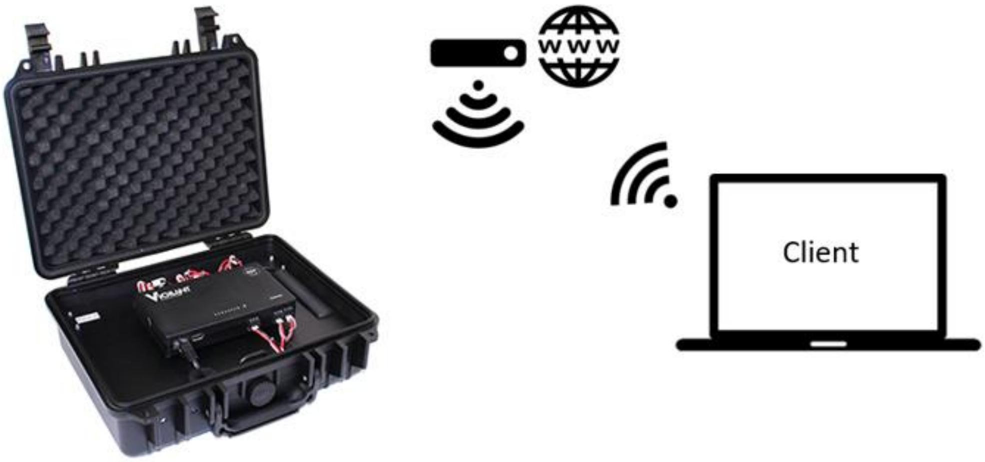
AUTHORIZATION REQUIRED

Please enter your username and password

Username: Please input username

Password: Please input password

Note: The router can also be configured to join an existing Wi-Fi. Once connected to the router's page, go to Network/Wireless, scan for an existing Wi-Fi, type the password, then press "save and apply".



Please refer to the manufacturers' website at https://wiki.teltonika-networks.com/view/RUT240 for further information.

The RUT 240/241 accessory module acts as a gateway between different networks and must be configured by you, according to your network architecture. Further information on the router Teltonika RUT 240/241 module is available at:
https://teltonika-networks.com/downloads/en/rut240/RUT240-Datasheet.pdf

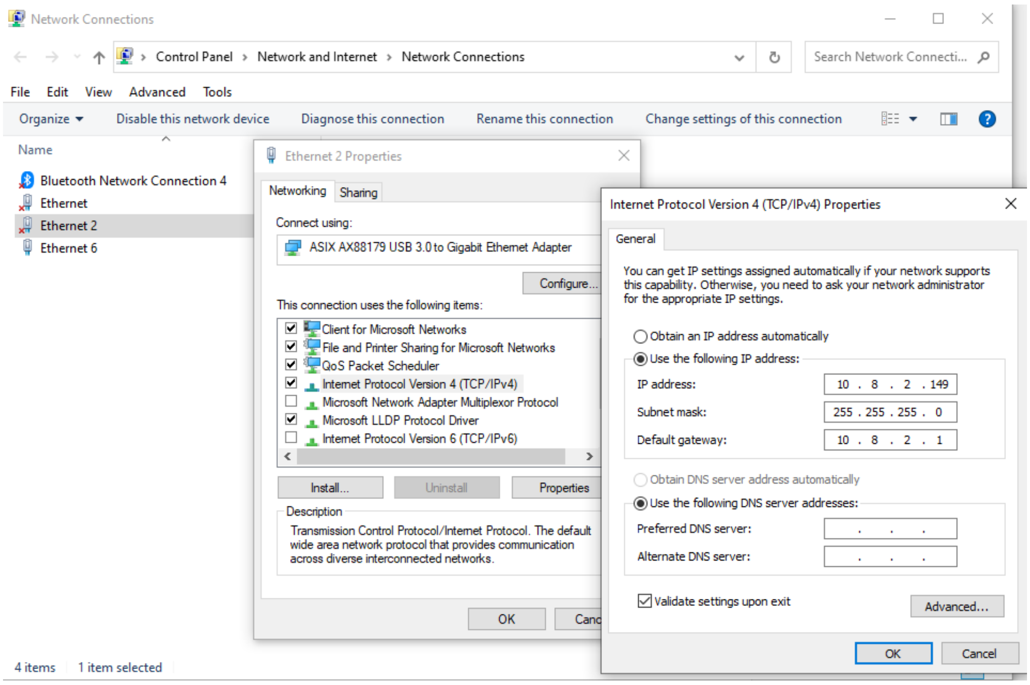
6.3. WAN connection

By default, the external Ethernet connector of the Mobility Case is connected to the WAN interface of the router. Therefore, VIGILANT connected in the LAN cannot be directly accessed via this Ethernet connection.

Refer to Section 6.2 for detailed instructions on how to access the router's configuration page. Adjust the WAN settings according to your specific needs:

- Static IP Configuration: Set a static IP address and configure necessary port redirection for point-to-point access.
- DHCP Mode: Enable DHCP mode and configure port redirection to integrate with an existing network architecture.
- WAN as LAN: Configure the WAN port to function as a LAN port for direct connectivity scenarios.

If the router’s WAN interface is used as a LAN port, VIGILANT should be directly accessible at either 10.8.2.150 or 192.168.0.150, depending on your setup. Based on the previous section, the user can still configure the network interface, as follows:



Network Connections

Control Panel › Network and Internet › Network Connections

Search Network Connecti...

- Bluetooth Network Connection 4
- Ethernet
- Ethernet 2
- Ethernet 6

4 items | 1 item selected

Ethernet 2 Properties

Connect using:

ASIX AX88179 USB 3.0 to Gigabit Ethernet Adapter

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- □ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 8 . 2 . 149

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 10 . 8 . 2 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☑ Validate settings upon exit

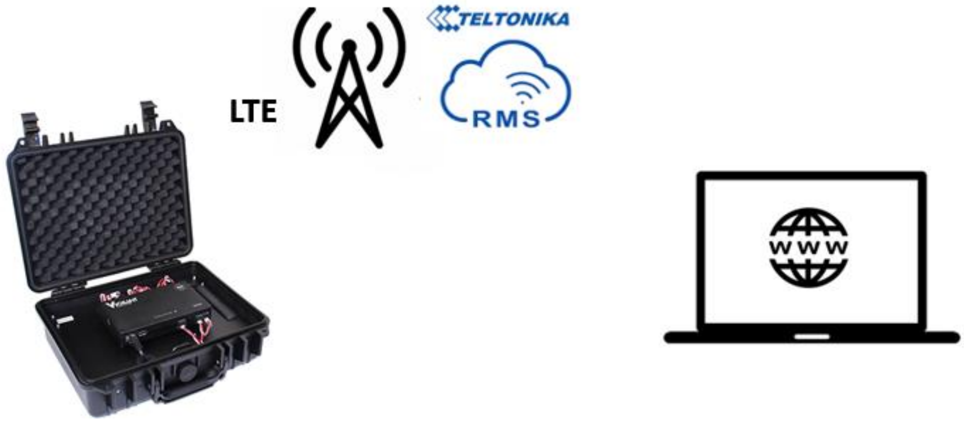
When using DHCP mode, ensure there is a DHCP server on the network to assign IP addresses automatically. Utilize a IP scanner (available here) to locate the unit within the network.

For seamless network integration, it’s advisable to consult your IT department. They can assist with adjusting network settings and ensuring secure and efficient connectivity.

Changes in the network configuration for both the PLC and the router could compromise default access. SDT advises consulting with network specialists.

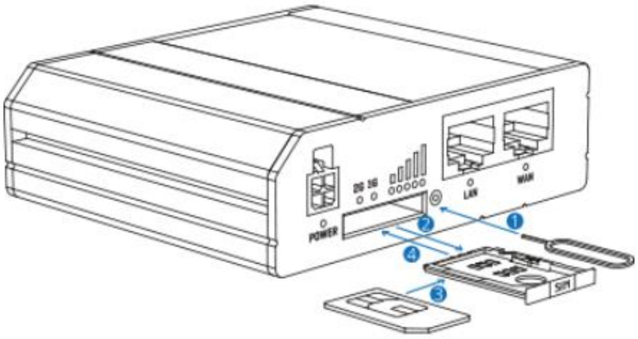
6.4. Mobile connection (access point in WI-FI required for the initial settings)

The GSM 3G/4G mobile connection enables remote access to the GUI in areas where other network accesses are unavailable. A SIM card with an active data plan from any Internet Service Provider (ISP) as well as an account on the Remote Management System platform (https://wiki.teltonika-networks.com/view/RMS) are required.

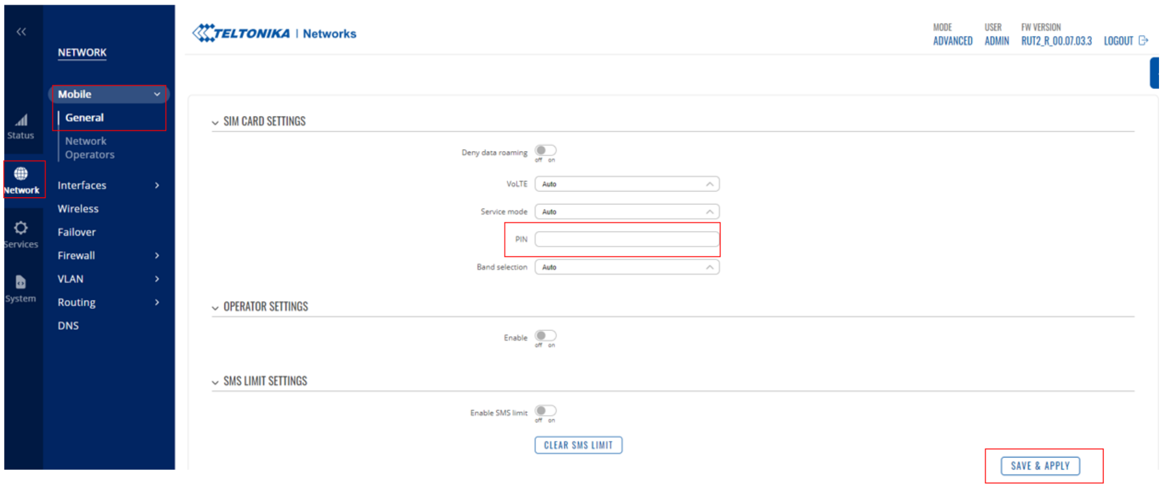


To do so, follow these steps:

- Open the mobile case or the steel enclosure to access the RUT 240/241 Teltonika module;
- Remove the module from the Din rail then eject the SIM holder with a paper clip. Insert the SIM card according to the picture below:



- Connect the GSM main antenna, provided in the package, to the router (in case of mounting in a steel enclosure, the antenna must be outside the box);
- Log in to the router’s configuration page. To access the router’s web interface, open a new tab then type ***10.8.2.1*** or **192.168.0.1**
- To activate the mobile network, Go to Network/Mobile/General;
- Type the PIN code of the SIM card and press “SAVE & APPLY”.



MODE ADVANCED USER ADMIN FW VERSION RUT2_R_00.07.03.3

SIM CARD SETTINGS

Deny data roaming: off on

VoLTE: Auto

Service mode: Auto

PIN:

Band selection: Auto

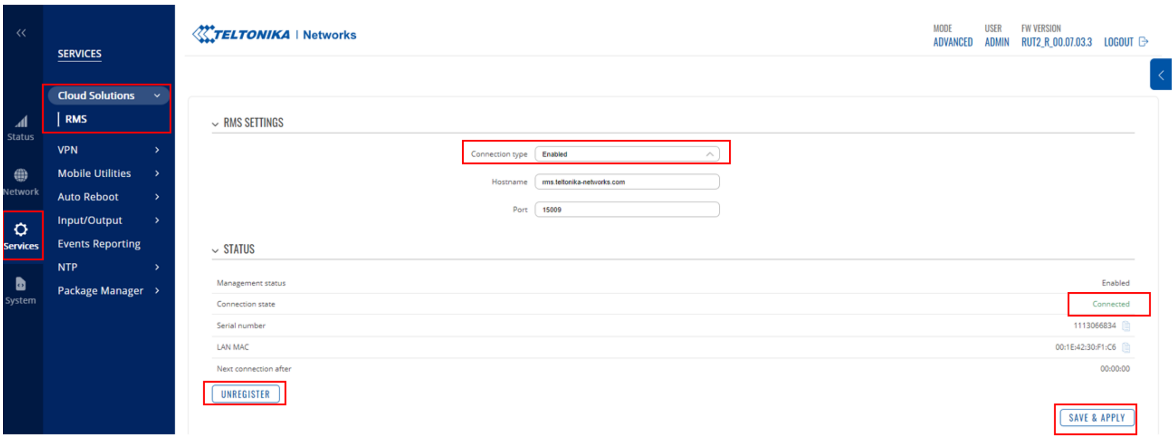
OPERATOR SETTINGS

Enable: off on

SMS LIMIT SETTINGS

Enable SMS limit: off on

- Go to Status/Overview then check if the Widget “INTERNAL MODEM” reads “Connected”. If not, please enable the mobile network interface in Network/interfaces/General;
- In Services/Cloud Solutions/RMS, select **Enable**, press **register**, then connect to RMS.



MODE ADVANCED
USER ADMIN
FW VERSION RUT2_R_00.07.03.3

RMS SETTINGS

Connection type: Enabled
Hostname: rms.teltonika-networks.com
Port: 15009

STATUS

Management status	Enabled
Connection state	Connected
Serial number	1113066834
LAN MAC	00:1E:42:30:F1:C6
Next connection after	00:00:00

https://rms.teltonika-networks.com/

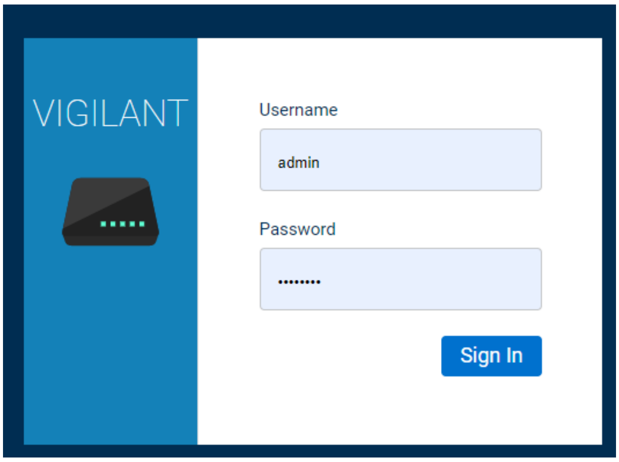
The router (SN and MAC address) must be registered to the RMS service to enable the Remote Management System. On the day of installation, once the router is connected to the Internet go to Services/Cloud Solutions/RMS. The service might be deactivated (Stand-by mode) in case of prolonged inactivity.
Please refer to the manufacturers’ website at https://wiki.teltonika-networks.com/view/RUT240 for further information.
Certain routers may require a firmware update to function properly or to ensure compatibility with recent features or security updates. To check for firmware updates and learn how to update your router, visit: RUT240 Firmware Downloads.

7. Configuration of the main unit

VIGILANT comes with an embedded web-based user interface that can be accessed from any operating system, including tablets and smartphones. The following steps describe the practical way to access to the configuration interface:

- Type the IP address of the unit or the public internet address indicated in the TCloud option. Read previous points for more information.

- Assuming a correct network configuration, the web browser will show the login screen:


VIGILANT

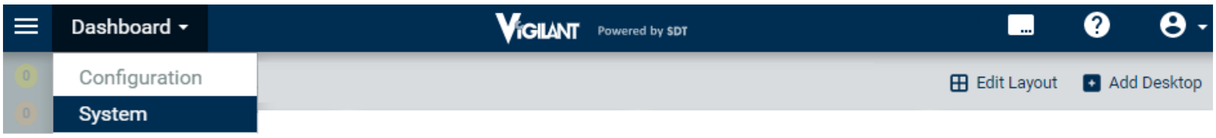
Username: admin

Password: ••••••••

Enter the username and password and click on "Sign in". By default, *VIGILANT* comes with a default password. It is recommended to change the default password and to create new users and permissions:

Username	Password
admin	Provided in the package

- Congratulations, you are now connected to the web-server. You can access the advanced options from the menu in the upper left corner of the application:



IMPORTANT

NOTE: Depending on your configuration, the Dashboard might be empty or prefilled using a downloadable template. To be quickly operational, users can download a predefined template at http://ftp.sdt.be/pub/Products/VIGILANT/Template/

This template provides a convenient starting point, ensuring that you can swiftly configure your settings without delay

Template *VIGILANT* *password: sdtdealer*

- You can change the IP address and other network configuration settings from the System menu. You can also create and delete users and perform other system administrator actions using the System web service.

- You can use the Configuration menu to configure your measurements: define machines, sensors, points, measurement parameters, and much more.
- From the Dashboard menu, once a new configuration is applied, you can access data recorded by the equipment. Please, refer to the user manual to learn how.

ⓘ IMPORTANT

The web application has been designed for use with Google Chrome. Although it should work correctly with any RSS standard compliant browser, some features may behave differently in different browsers.

8. Support and contact details

ⓘ IMPORTANT

VIGILANT has a reset button available next to the power connector. If necessary, press it for 5 seconds or more, and you will reset the equipment to factory settings. Please note that after restoring the settings, the IP address will become the following, and will not be compatible with the modem's logic network: ***192.168.0.150 or 10.8.2.150***

SDT North America

Toll Free: 1-800-667-5325

Phone: 1-905-377-1313

7677 County Road 2

Cobourg ON K9A 0X4,

Canada

Email: info@bevigilant.io

Web page: https://bevigilant.io

SDT International

Phone: +32 (0) 2 332 32 25

Bd. de L'Humanité 415

B-1190, Brussels

Belgium

Email: info@sdtultrasound.com

4	CMA 2024/05/08	Clarification of network parameters	RGO
3	CMA 2023/01/30	Major changes in network settings	GGI
2	CMA 2022/11/07	New rear panel	RGO
1	CMA 2021/06/24	Original version	RGO
Ver.	**Editor**	**Nature of modification**	**Verified**