USER MANUAL

Software User Manual

A. Login Procedure

B. Sensor Dashboard (software version 1.5.x)

USER MANUAL

USER MANUAL

USER MANUAL

A. Login procedure iQunet sensor network

The procedure below describes how to connect to the iQunet sensor network via WebRTC. Check section 5 for other connection possibilities.

1. Install a browser which is supporting WebRTC

iQunet strongly advises to use the Google Chrome browser.

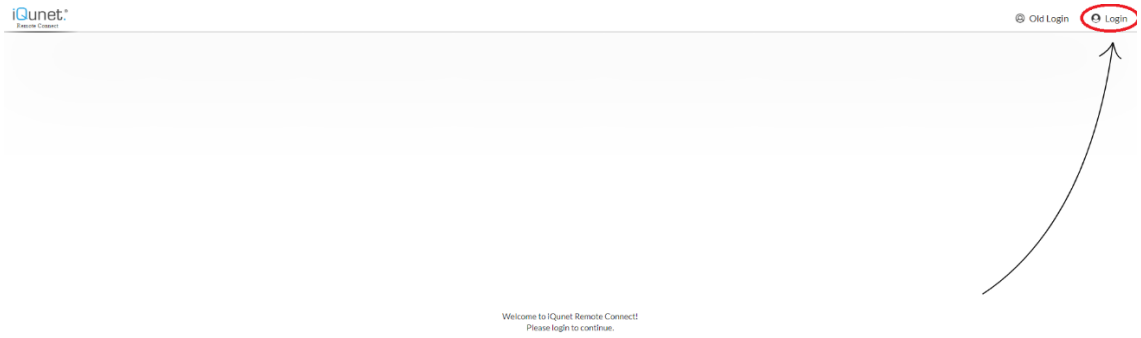
Note: Microsoft will not develop WebRTC for Internet Explorer. Microsoft Edge is WebRTC compatible since it is re-based on Chromium (released January 2020).

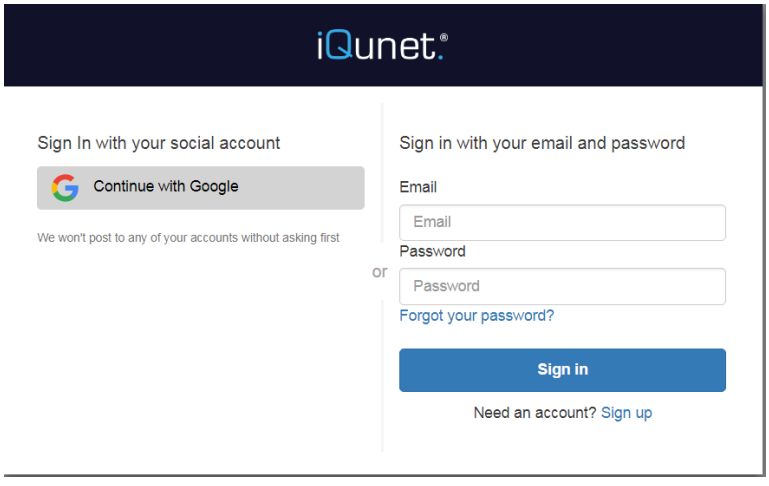
WebRTC is an open framework for the web that enables Real Time Communication in the browser. It includes the fundamental building blocks for high quality communications on the web, such as network, audio and video components used in voice and video chat applications. The WebRTC effort is being standardized on an API level at the W3C and at the protocol level at the IETF.

2. Surf to: connect.iqunet.com

3. Log in with your Google account or create a new account using your email address.

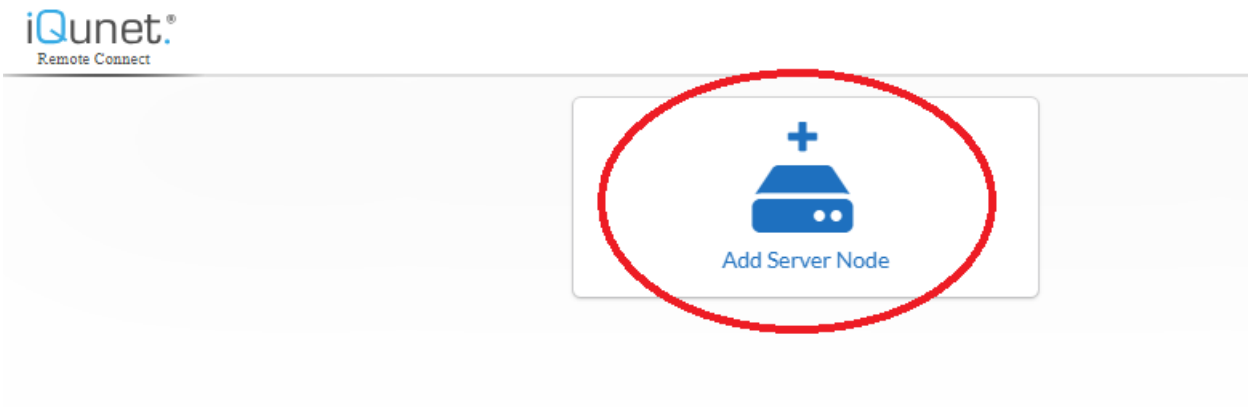
This identification is to verify you are not a web robot. Once logged in, you will not be prompted anymore.



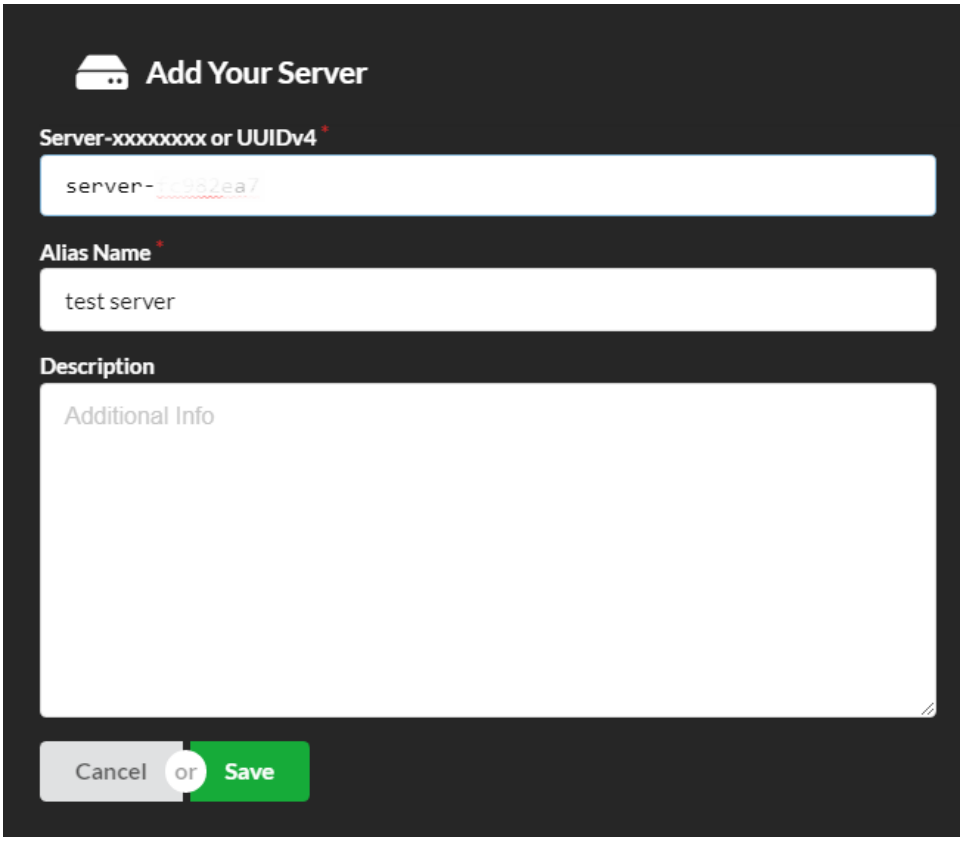


USER MANUAL

4. **Click on "Add Server Node".**

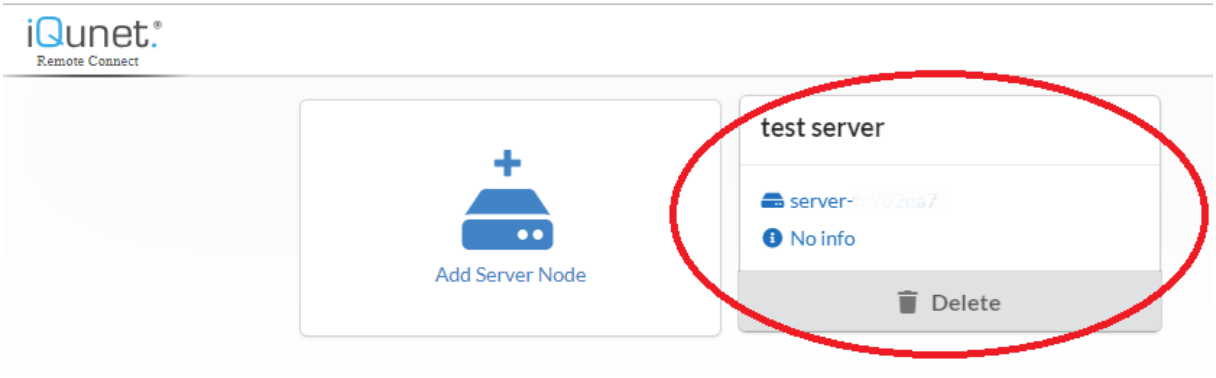


5. **Enter the Sensor Proxy ID (server-xxxxxxxx) and provide an alias name for the server. Click "Save". The Sensor Proxy ID is provided by iQunet.**

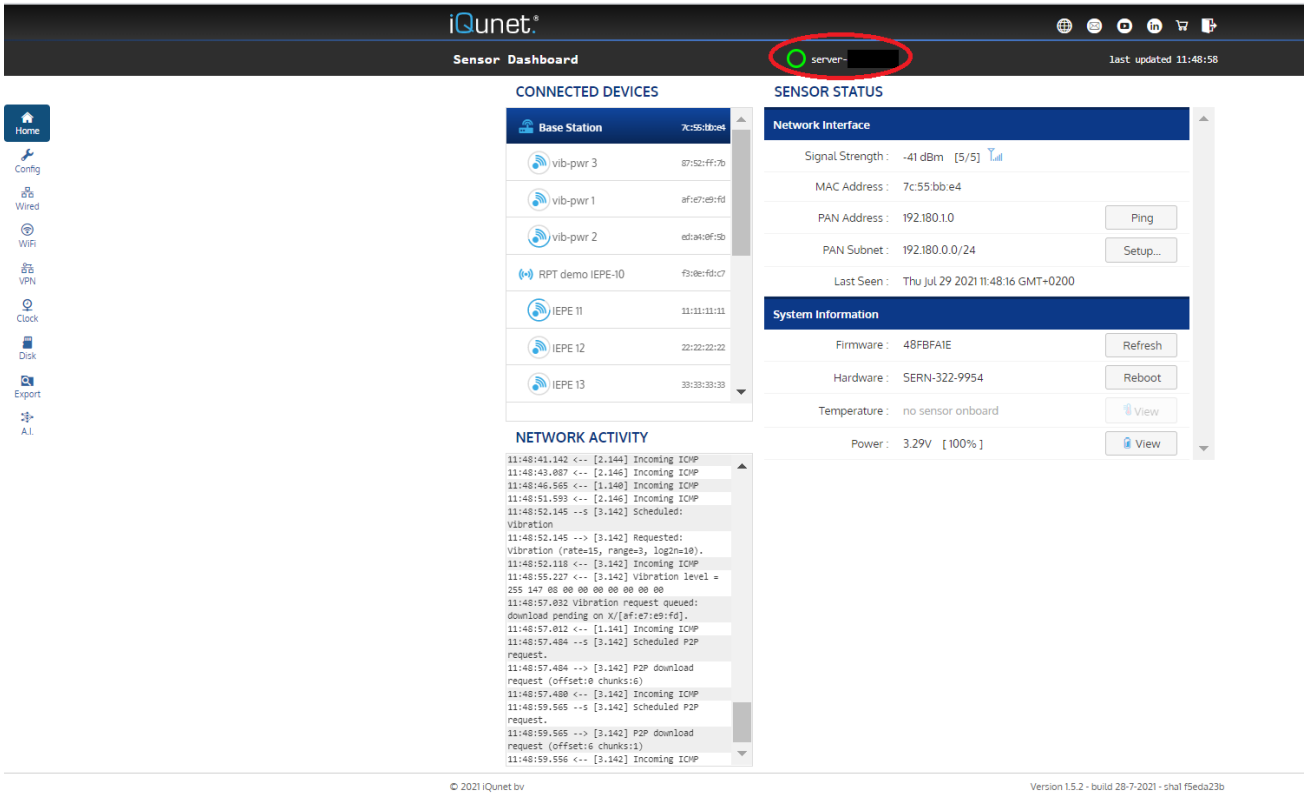


USER MANUAL

6. Click on the created server node to open the iQunet Sensor Dashboard.



7. You are now connected to the iQunet Sensor Dashboard.



USER MANUAL

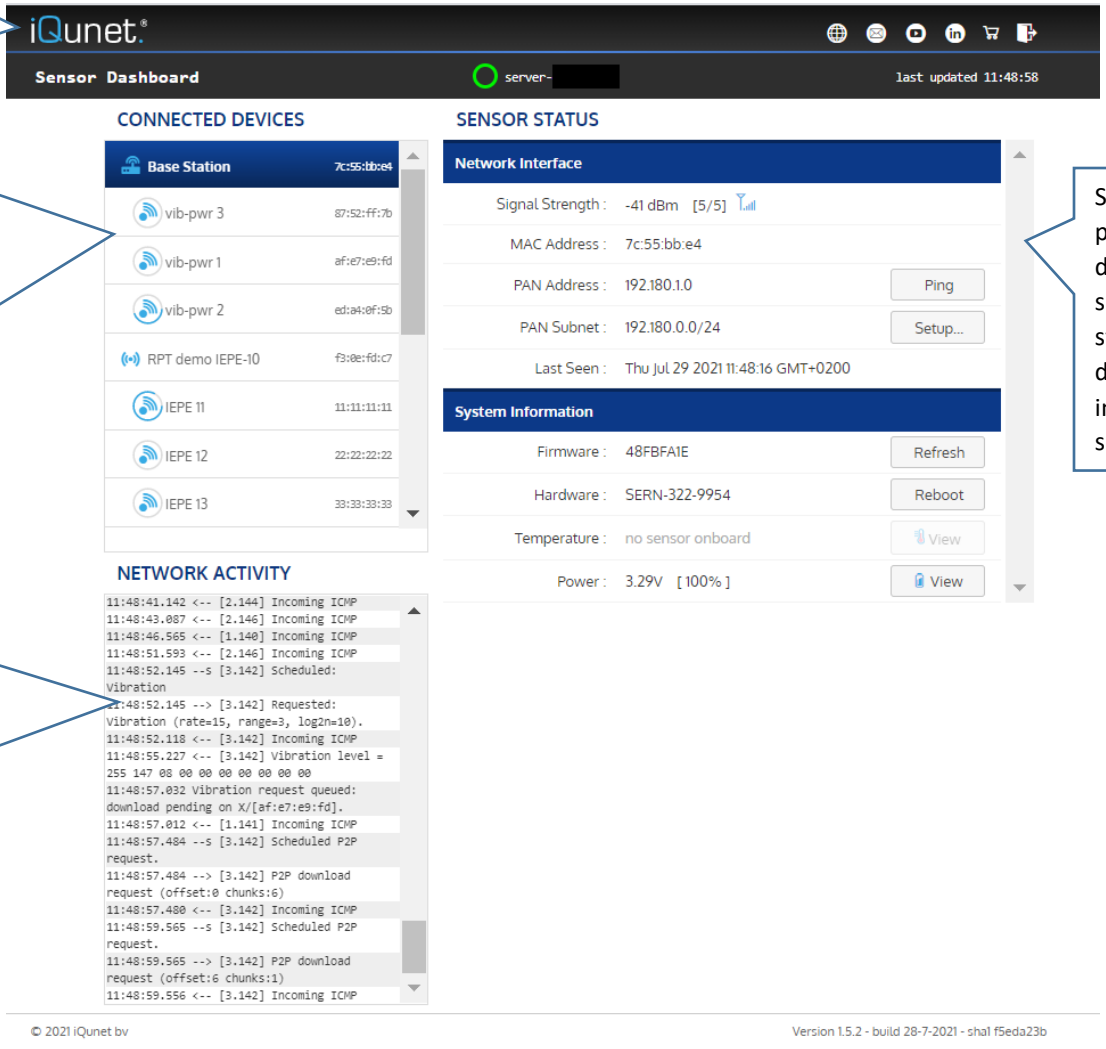
B. iQunet Web GUI: Quick Start Guide

1. General

General information pane

Device pane: list of devices connected to the Base Station. Connected devices can be scheduled for periodic measurements or for a single manually triggered measurement.

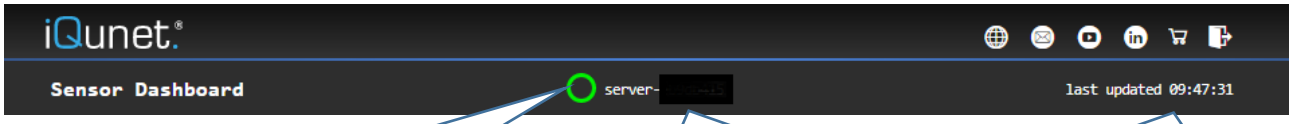
Network activity pane: this pane shows scrolling logs of sensor activity messages (sent and received messages per sensor).



Sensor status pane: this dynamic pane shows sensor status and device depending information and settings.

USER MANUAL

1.1. General information pane



Connection status to the iQunet Server from sensor network.

Green: connected

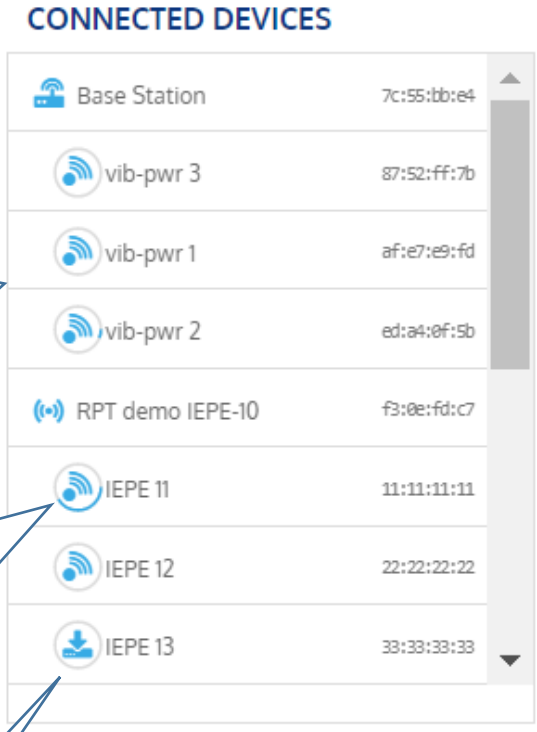
Red: connection lost

Grey: connecting

Connected server

Time stamp of last screen refresh

1.2. Device pane



Devices connected to the Base Station. Once seen by the Base Station, the list remains intact until the device is deleted. Devices losing contact with the Base Station will show no updated network status (see Sensor Status pane) but remain linked with the Base Station (and remain in the list).

The circles around the sensor icons represent a countdown to the next scheduled measurement. When the blue circle becomes completely gray, a new measurement will be started.
These circles only appear for devices currently activated for measuring and sending data on preset time intervals.

When this icon appears, the measurement is being downloaded from the sensor and sent to OPC.

1.2.1. Device pane icons

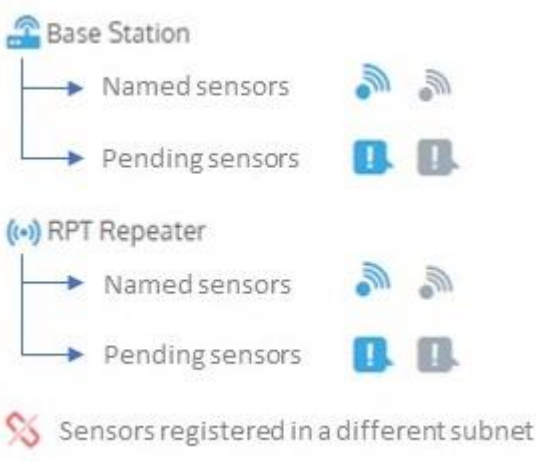
The icons in front of the sensor name provide you with more information regarding the sensor status.

Icon	Explanation
	The sensor is active (normal sensor operation).
	The sensor is active, and a sensor measurement is requested.
	The measurement is being downloaded from the sensor device and sent to OPC.
	The sensor is last seen more than 10 minutes ago by the iQunet Server.
pending	The connection of the sensor to the iQunet Server is pending. The sensor has been seen by the Base Station/Repeater connected to the Server but has not been assigned yet. By (re)naming the sensor (see section 2.1 for instructions), the sensor will become connected to the Base Station/Repeater. If the sensor connection is still pending after 10 minutes, the sensor will be rebooted so it can reconnect itself to its original Base Station/Repeater and corresponding Server where it received a name previously.
pending	The connection of the sensor to the iQunet Server is pending. The sensor has been seen by the Base Station/Repeater connected to the Server but the sensor itself is not active anymore (last seen more than 10 minutes ago). The sensor can be deleted from the "Connected Devices" list if it is not relevant anymore (see section 2.2).
	The subnet of the Base Station has been changed (see section 3.2) and therefore the sensor is now registered in another subnet.

Remark: it can be necessary to refresh the Sensor Dashboard to see the latest sensor status (blue, grey…).

1.2.2. Device pane sensor ordering

The sensors are listed in the following order in the device pane (inside the different groups the sensors are sorted according to sensor mac ID number (00:00:00:00 to ff:ff:ff:ff)):



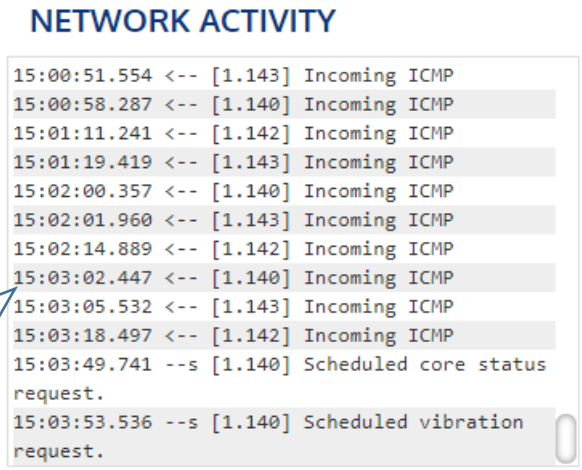
USER MANUAL

1.3. Network activity pane

This pane shows scrolling logs of sensor network messages.

"<- -": incoming messages from connected sensor devices (seen sensors)

"- ->": outgoing messages to the sensor devices (will be received as soon as sensor is awake)

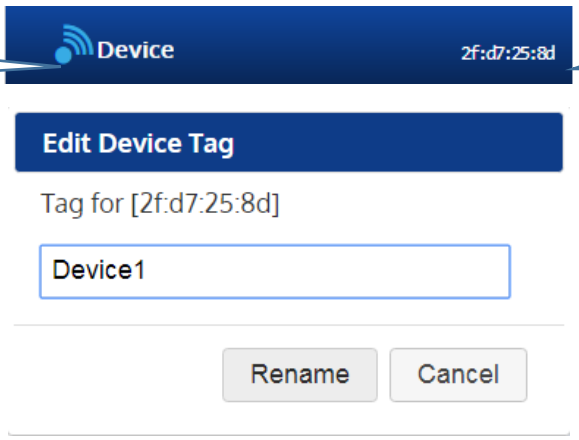


2. General functionality

2.1. Renaming a device

By pressing the icon, a popup appears. The device can be renamed.

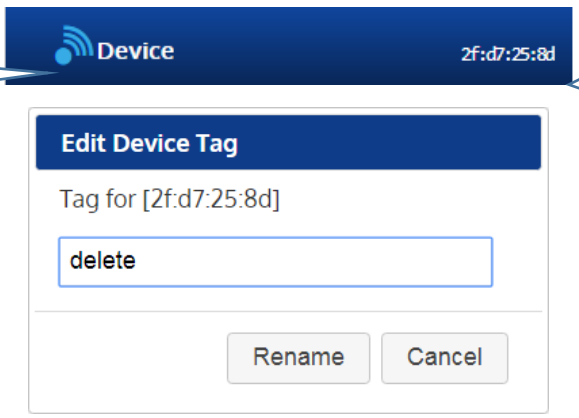
The devices MAC address cannot be altered and remains unique.



2.2. Deleting a device

By pressing the icon, a popup appears. The device can be deleted by renaming it to "delete".

When deleted, the device will be removed from the sensor list. As soon as the battery is activated in the device, the device pops up again in the list and is automatically connected to the closest Base Station in the field when in reach.

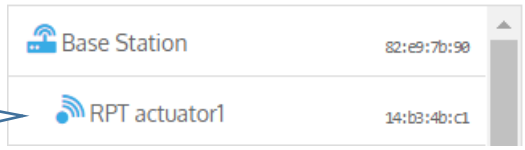


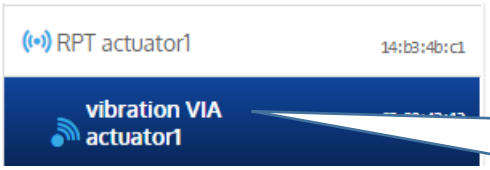
USER MANUAL

2.3. Relaying a device via a Repeater or an Actuator

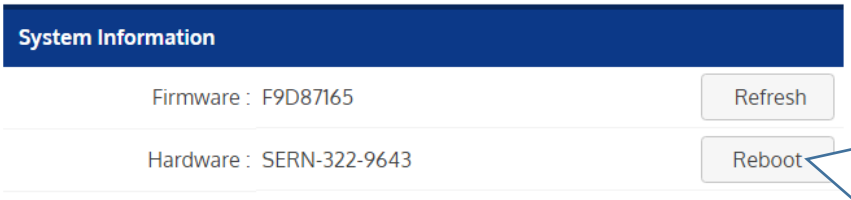
Remark: iQunet recommends **not to use** the relaying with the VIA keyword but rather let the sensors decide automatically for themselves to which Base Station or Repeater they want to connect in function of the signal strength.

To relay sensors via a Repeater or Actuator, simply rename the Repeater or Actuator and start the name with "RPT". The name of the Repeater or Actuator may NOT contain spaces.

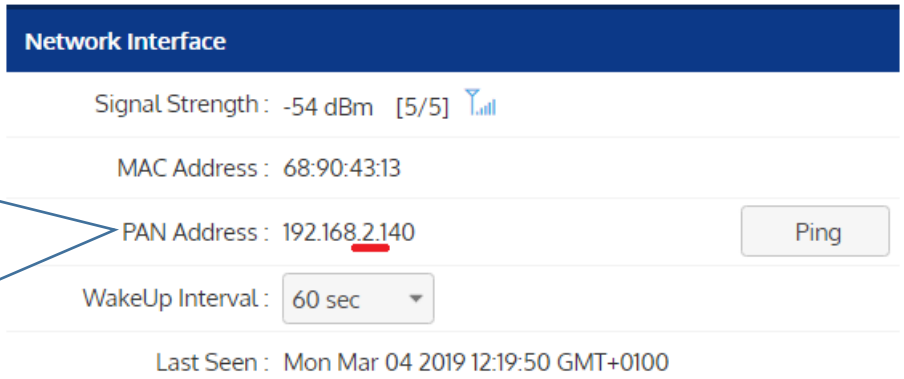




To force the relay of a sensor device via a Repeater or Actuator, type "VIA" after the device name followed by the Repeater or Actuator name.



In the device pane select each device involved in the relaying (Repeater, Actuator and sensors), and press "Reboot" for each of them.



By clicking on each device, check if each Repeater or Actuator has received a new subnet like "192.168.2.xxx", "192.168.3.xxx", etc. In this example, sensor 68:90:43:13 is fixed relayed via Actuator "RPT actuator1" under the subnet "192.168.2".

USER MANUAL

3. Sensor status pane

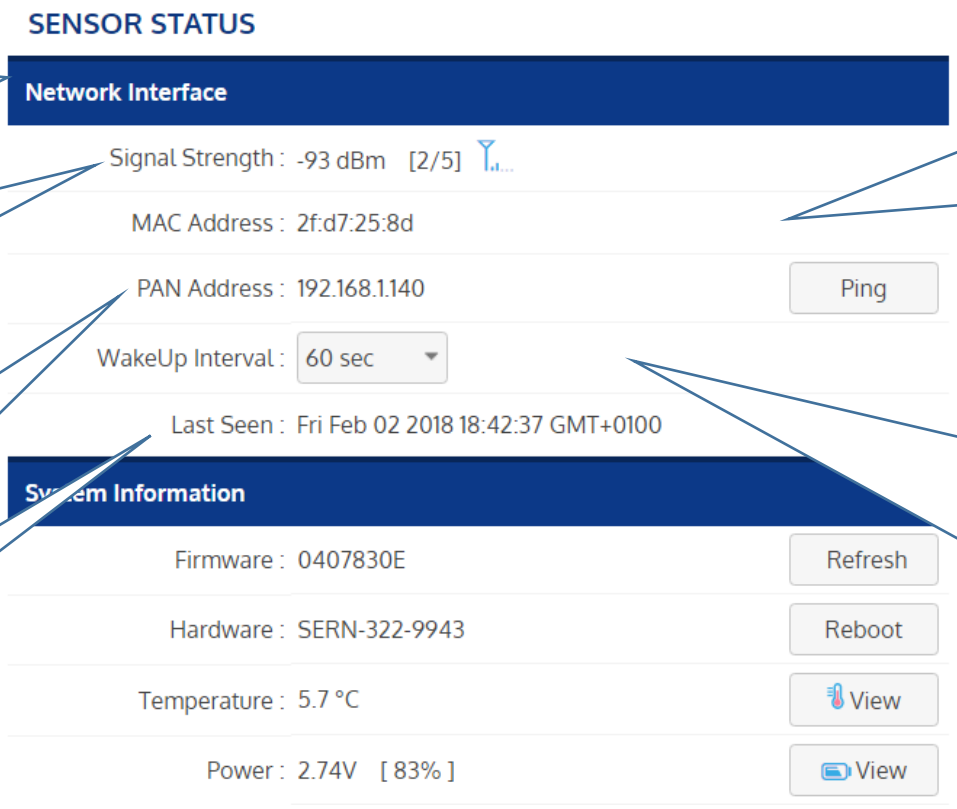
3.1. Network interface pane sensors

Network Interface pane is showing current interface settings from selected device.

Signal strength: current wireless signal strength between device and Base Station (or Repeater).

When connected, the device receives a unique PAN address. This address is used in the network activity log. Ping to check network activity.

Sensors last network contact

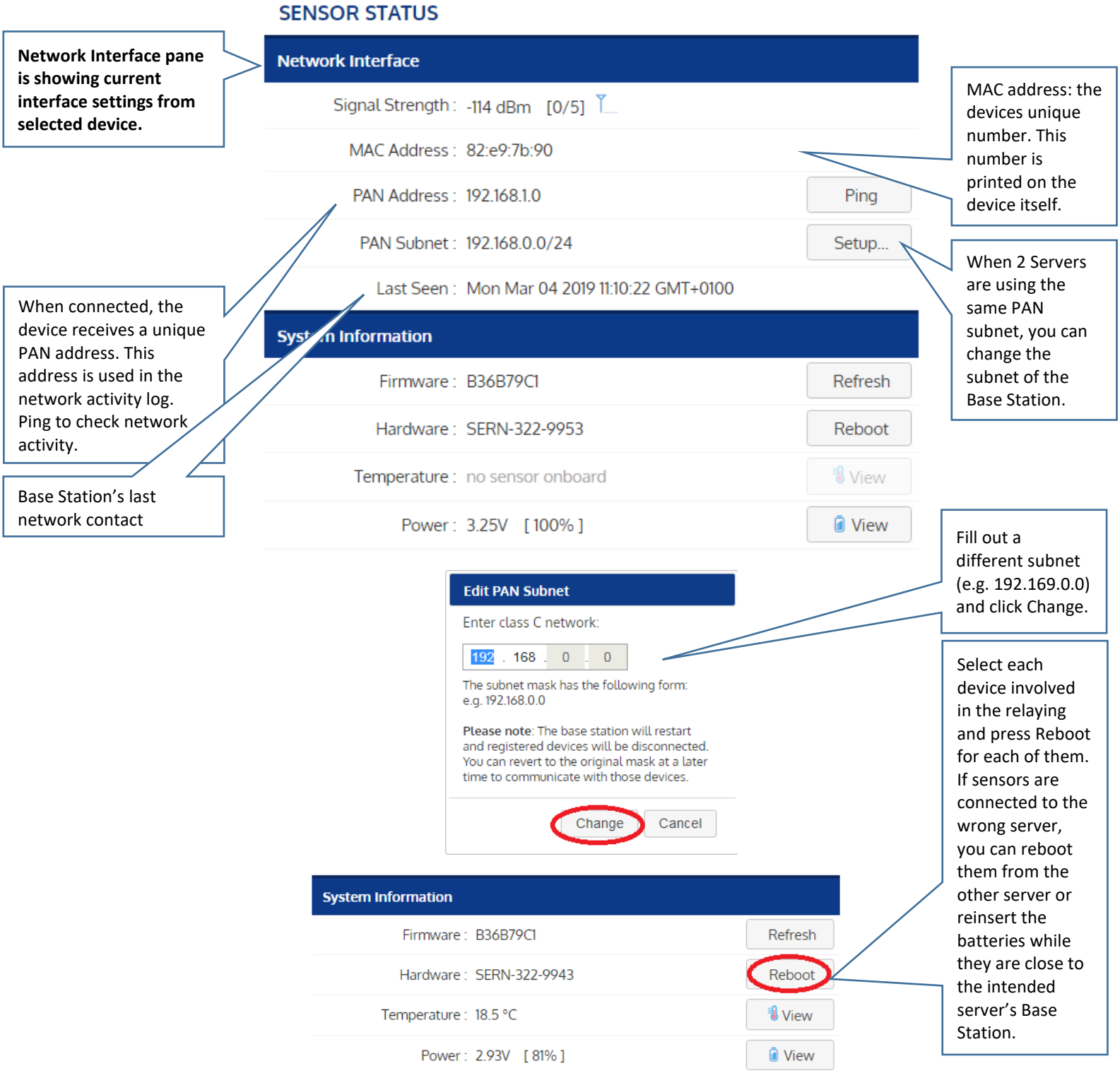


MAC address: the devices unique number. This number is printed on the device itself.

Device wakeup interval: the device will be in iQunet sleep mode for the set time. It will become active at the end of the set time interval. Change interval by changing the number.

USER MANUAL

3.2. Network interface pane Base Station



Network Interface pane is showing current interface settings from selected device.

MAC address: the devices unique number. This number is printed on the device itself.

When 2 Servers are using the same PAN subnet, you can change the subnet of the Base Station.

When connected, the device receives a unique PAN address. This address is used in the network activity log. Ping to check network activity.

Base Station's last network contact

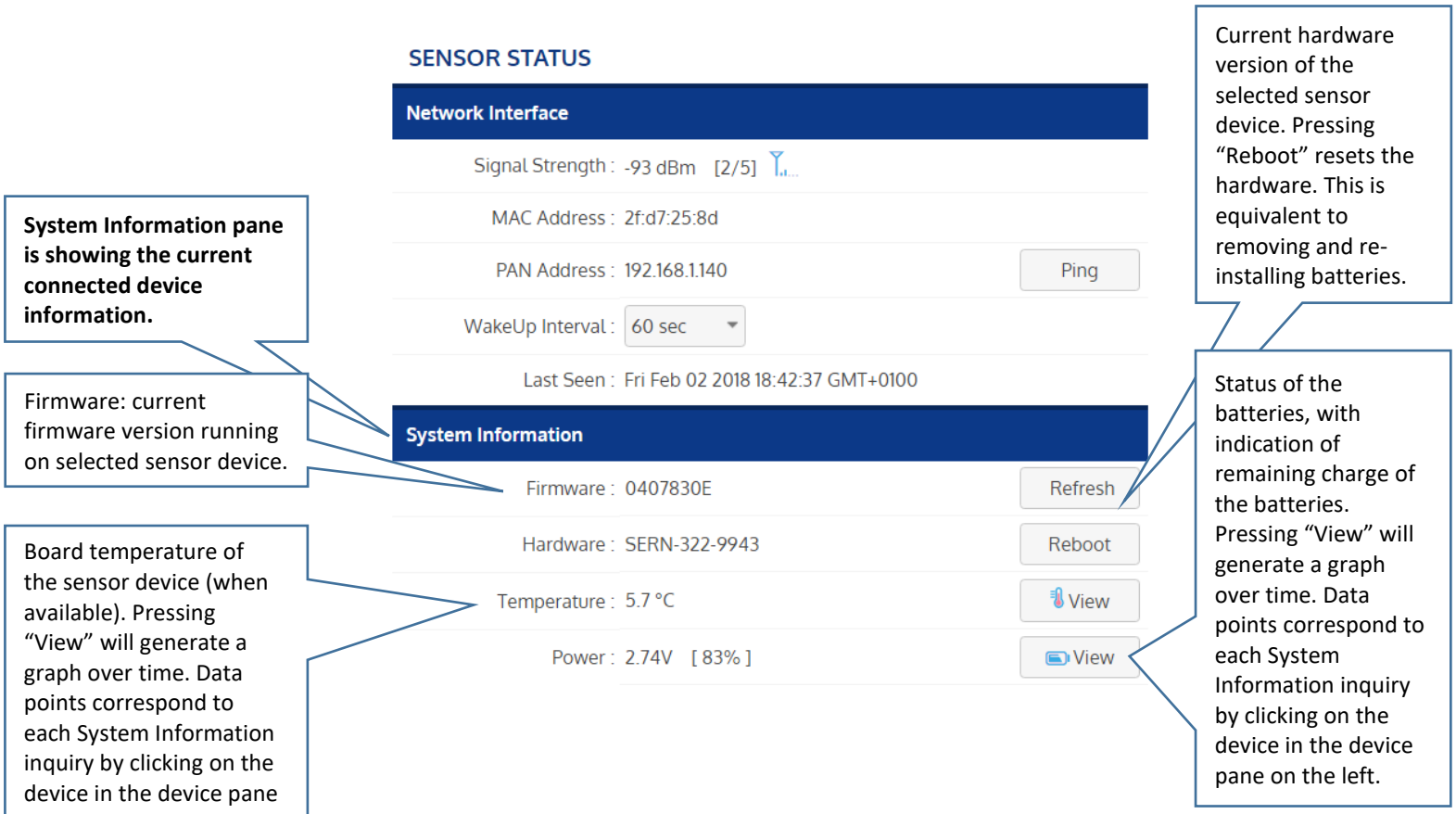
Fill out a different subnet (e.g. 192.169.0.0) and click Change.

Select each device involved in the relaying and press Reboot for each of them. If sensors are connected to the wrong server, you can reboot them from the other server or reinsert the batteries while they are close to the intended server's Base Station.

Remark: a sensor can become "blacklisted" (see the Network Activity pane (section 1.3)) if the sensor continuously jumps back and forth between two Base Stations (2 Base Stations have the same subnet). In this case it is recommended to change the subnet of one of the Base Stations.

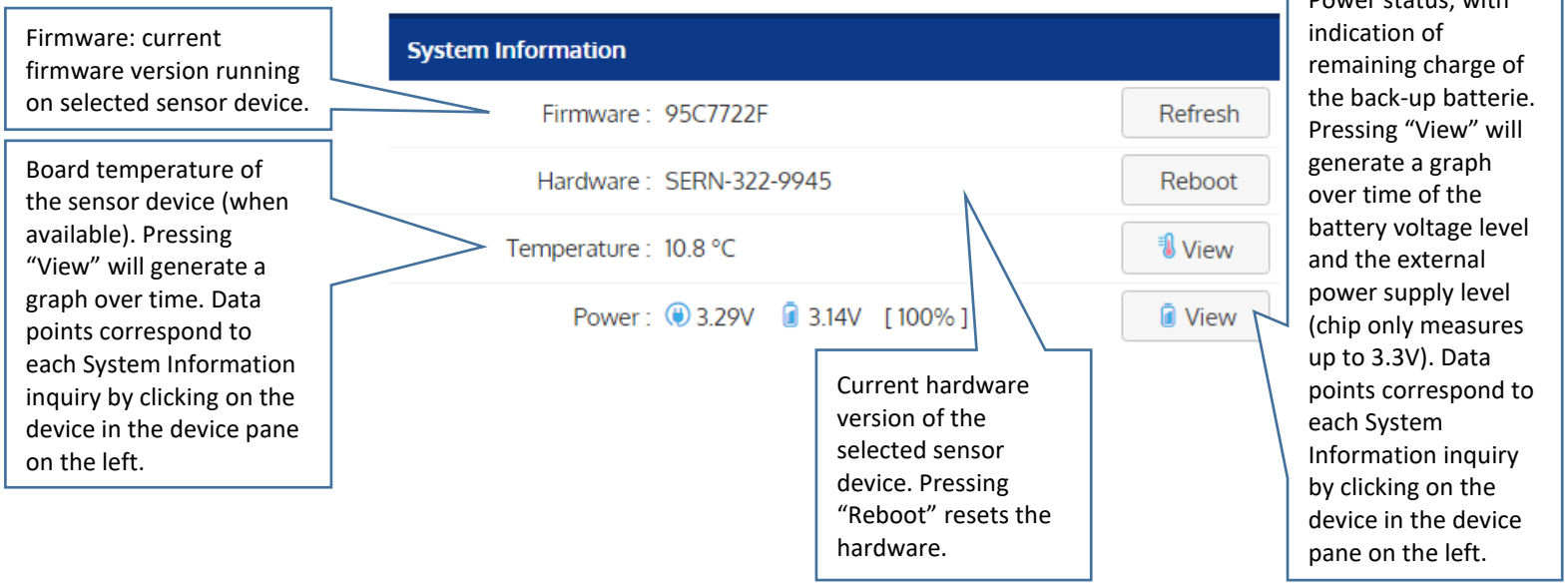
USER MANUAL

3.3. System information pane battery-powered sensors



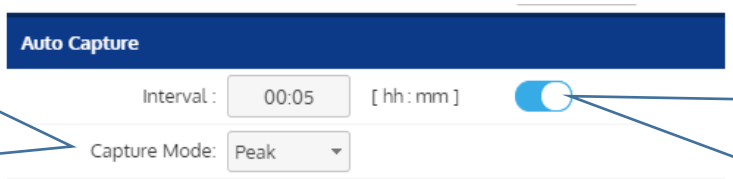
3.4. System information pane 24V Powered Vibration Sensor

The iQunet wireless 24V Powered Vibration Sensor is powered with a 24V power supply (6VDC-60VDC). The sensor also has 1 standard coin cell on board acting as a backup during short power interruptions.



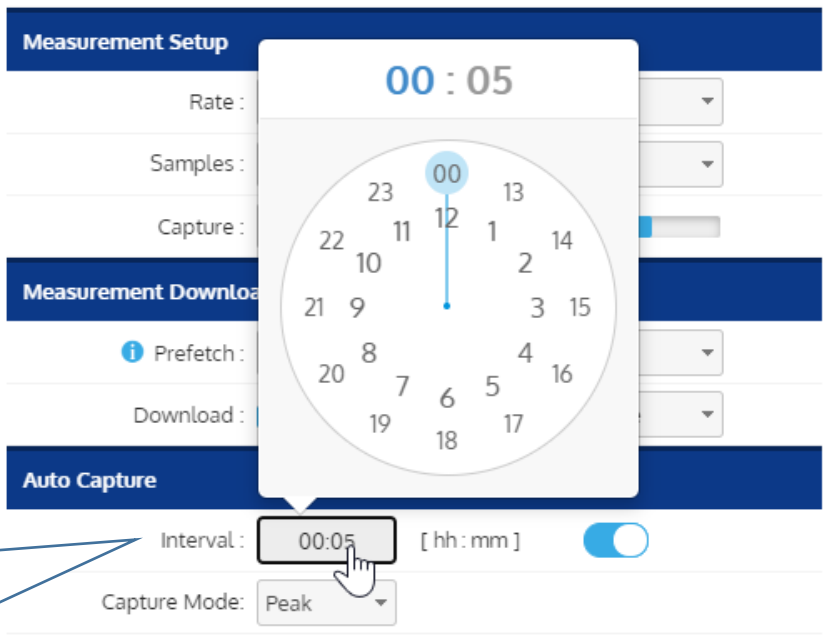
3.5. Auto capture pane

For the event-based sensors (the 24V Powered Vibration Sensor, the Current Clamp and the IEPE Accelerometer), it is possible to change the capture mode from "Peak" (measurement with the highest peak power during the set time interval is saved) to "Instant" (measurement is taken at the end of the set measurement interval).



A sensor device which is enabled for Auto Capture will show this extra pane. To start the periodic sensor measurements, slide the button to blue. The queue interval can now be set.

Select the queue interval in the dial pane. First select the hours by dragging the clock pointer over the desired number. Then repeat this action for selecting the minutes. The device will now become active after the set interval.



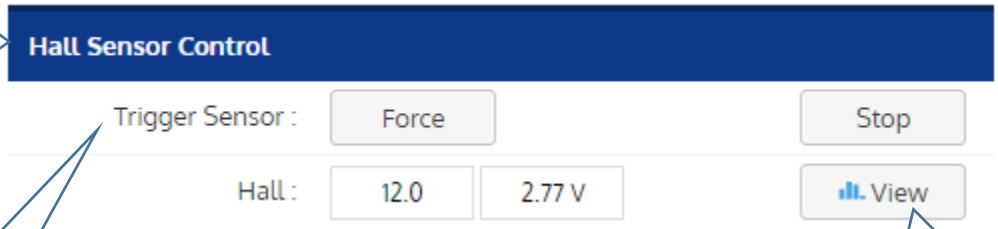
Devices activated for automatic measurements will now show a countdown circle around the sensor icon.

Remark: for the event-based sensors (the wireless 24V Powered Vibration Sensor, the Current Clamp, the IEPE Accelerometer and the MAD Vibration Sensor) the set auto measurement queue interval is also the measurement interval since these sensors will capture vibration or current signals from the moment a measurement is started until a new measurement is started (when used in the "Peak" capture mode).

3.6. Sensor control pane

3.6.1. Hall Sensor control (Proximity Sensor)

Pane appears when selecting a sensor device with a Hall Sensor on board.

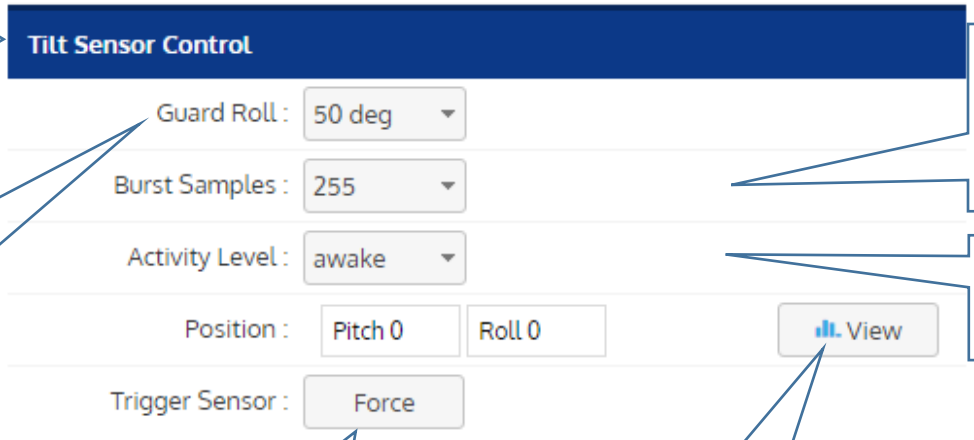


The sensor device can be triggered to start measurements as soon as the device is awake (see wakeup interval). Clicking "Force" starts the burst of measurements. "Stop" will interrupt the measurements triggered earlier.

Field values are combined with the measuring voltage at that time (for calibration purposes). The burst of measurements can be viewed in a graph by pressing "View".

3.6.2. Tilt Sensor control (Inclination Sensor)

Pane appears when selecting a sensor device with a Tilt Sensor on board.



Maximum allowed roll before initiating an alarm. If the set value is surpassed, the connected Actuator device will be triggered.

Select the number of samples in a measurement burst.

Required activity level to wake up the sensor.

The sensor device can be triggered to start measurements as soon as the device is awake (see wakeup interval). Clicking "Force" starts the burst of measurements. The measurement will stop after the chosen number of burst samples.

When active, Roll and Pitch values are visualized. The recorded burst of measurements can be viewed in a graph by pressing "View".

3.6.2.1. Activation of the roll guard

The guard of the inclination roll parameter works instantaneously in combination with the Actuator. For the Actuator to enter the standby mode for the roll guard, the Inclination Sensor needs to make a measurement first (click “Force”). This is the same whether the Actuator works as a repeater or not.

To check this functionality, you can perform the following test (if possible, perform the test on a table first).

Remark: make sure to perform this test only when the Actuator is connected to the mains otherwise the UPS function will start working and the batteries will drain.

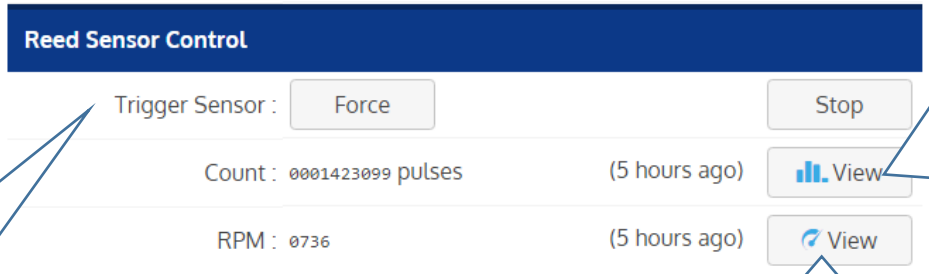
- Connect the Actuator to the mains with the USB charger. It is not necessary to insert the batteries.
- Place your multimeter in the outside front contact of the Actuator and measure the resistance. You will detect a normal closed contact when the Actuator is on.
- Insert the batteries into the Inclination Sensor. The sensor will wake up (check the messages in the network activity pane). The “device” will appear in the device list. Keep the sensor values as set initially.
- Click “Force”. The Inclination Sensor will start measuring within 60 seconds (the wake-up interval as set in the sensor information pane on the top). You can lower the wake-up interval setting but this is not necessary since it will take some time before the sensor learns to wake up every 3 seconds effectively for example.
- Make some roll and pitch movements with the Inclination Sensor. The sensor will show changing values in the two “position” fields in the Sensor Dashboard. After measuring the set number of samples (e.g. 32), the sensor has proven to be active and is now armed to guard the roll of the sensor.
- Roll the sensor over the set guard roll angle (positive or negative). The message “actuator message 01” will appear in the network activity pane. The Actuator is then switching the contact to open (see the readings on your multimeter).
- Return the sensor to a safe position after 10 to 30 seconds. The sensor will send the “actuator message 00” to inform the Actuator that everything is safe again. The Actuator contact will be closed again.

The guard of the roll angle is always on, even if the Inclination Sensor looks asleep. There is no need to trigger the sensor again. In this way there will be little use of the batteries.

Note that the Inclination Sensor is optimized to be mounted on vibration machinery. A minimum vibration level is needed to keep the sensor awake internally. If the sensor doesn’t detect any vibration, the machinery is assumed to be not active, and the sensor will go in ultra-deep sleep mode. As soon as there is a minimum activity (see the set activity level), the sensor will switch on. Setting the activity level to none will prevent the sensor from going to deep sleep mode. The sensor will then always be active, even at night or when not in use. This will use unnecessary battery lifetime. The sensor batteries will drain quickly in this case.

USER MANUAL

3.6.3. Reed Sensor control (Proximity Switch Sensor)



Pane appears when selecting a sensor device with a Reed Sensor on board.

The sensor device can be triggered to start measurements as soon as the device is awake (see wakeup interval). Clicking "Force" starts the burst of measurements. "Stop" will interrupt the measurements triggered earlier.

The number of magnetic pulses is counted continuously. When the sensor is active, pulses are shown in this field. The counts are shown in a graph by pressing "View".

Revolutions per minute value based on the count of magnetic pulses. When the sensor is active, rpm values are shown in this field. The rpm values are shown in a graph by pressing "View".

3.6.4. Vibration Sensor control

Pane appears when selecting a sensor device with an Acceleration Sensor on board.

Select the sampling rate.

Select the number of samples.

By pressing "REC", the vibration measurement is triggered with the set parameters.

Select 1, 2, or 3 measurement axes in the dropdown menu.

Select the desired dynamic range of the sensor in the dropdown menu. Check the RMS values of the last month in the Statistics pane (see section 3.6.4.2) to find out which range is best suited. Keep the range as low as possible for optimal accuracy.

Check if vibration level is high enough for download (see section 3.6.4.3).

Select a number of samples to make an antecedent RMS calculation for the vibration measurements. If the RMS value is below threshold, the full sensor download is aborted (see 3.6.4.3).

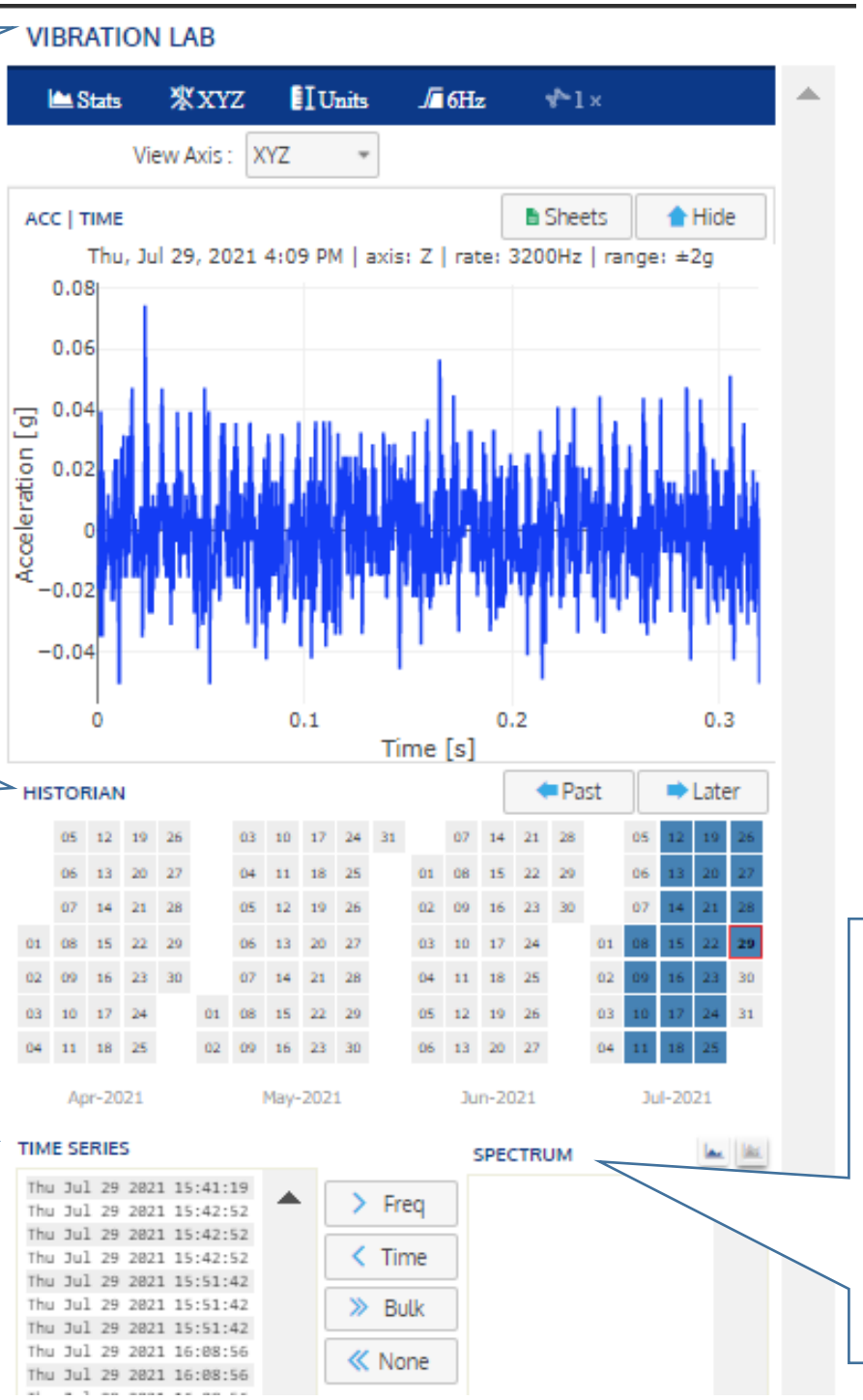
Progress of automatic download

Select the high pass cut off frequency to remove the DC component and the low frequency noise in the RMS signal. See section 3.6.4.3 for more information.

A full measurement is downloaded when the RMS is above threshold. See section 3.6.4.3.

3.6.4.1. Vibration Lab

Vibration Lab pane shows basic analysis of measured vibration signals.

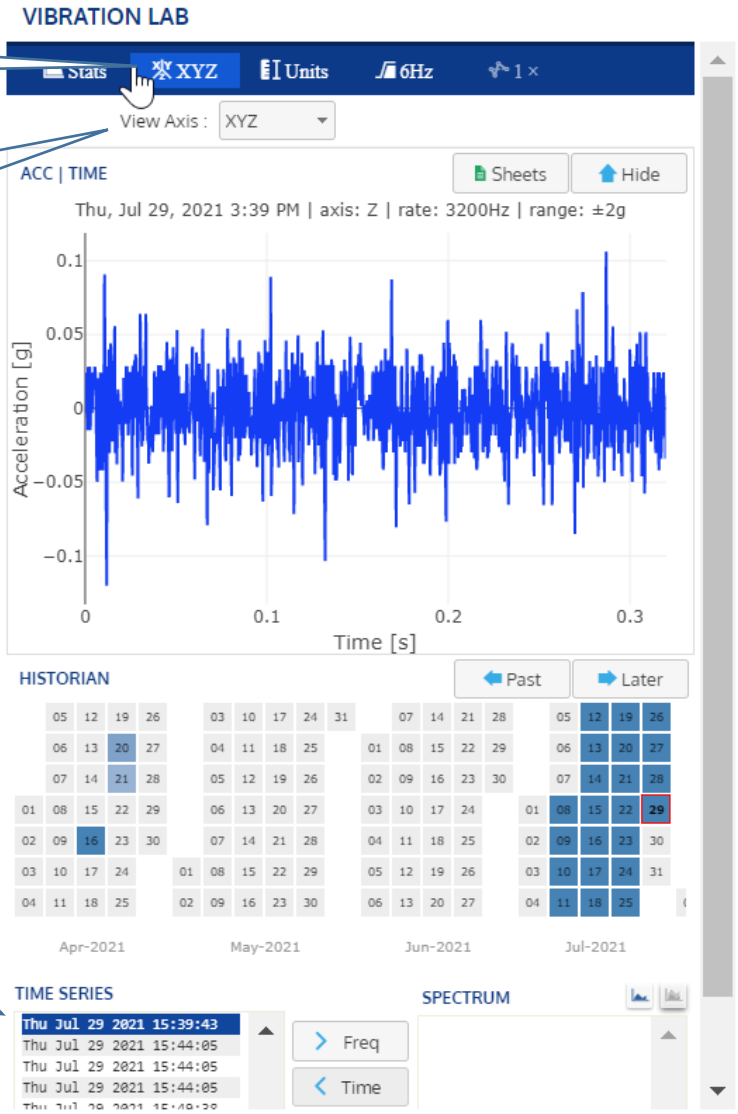


Measurements saved in the iQunet OPC historian. Click on the date to see the available measurements.

Time Series box: selecting 1 measurement in this box will show the respective time series graph. Select multiple time signals by dragging the mouse pointer. Click “Freq” to add the selected measurements to the box on the right. When only 1 measurement is selected, clicking “Freq” will automatically show the spectrum plot. Click “Bulk” to add all measurements to the box on the right.

Spectrum box: select 1 measurement to show the spectrum of this measurement. Drag over the list to select multiple items for removing them back to the left box (click “Time”). Click “None” to remove all measurements in this box.

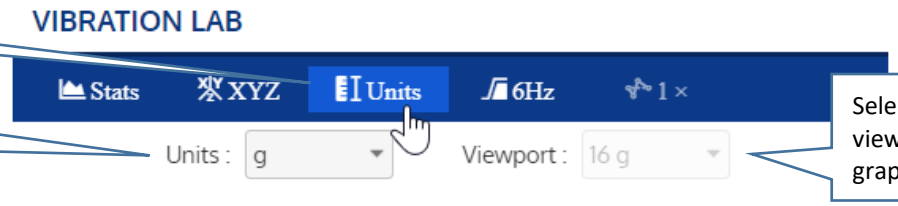
USER MANUAL



"XYZ" view axis filter tab

Select the measurement axis of which you want to see the measurements.

Selecting "XYZ" as the view axis will show all measurements of the selected day. Selecting "X" will only show the X axis measurements and similarly for selecting "Y" or "Z".



"Units" tab

Select graph units: g or mm/s.

Select predefined viewport settings to alter graph format.

USER MANUAL

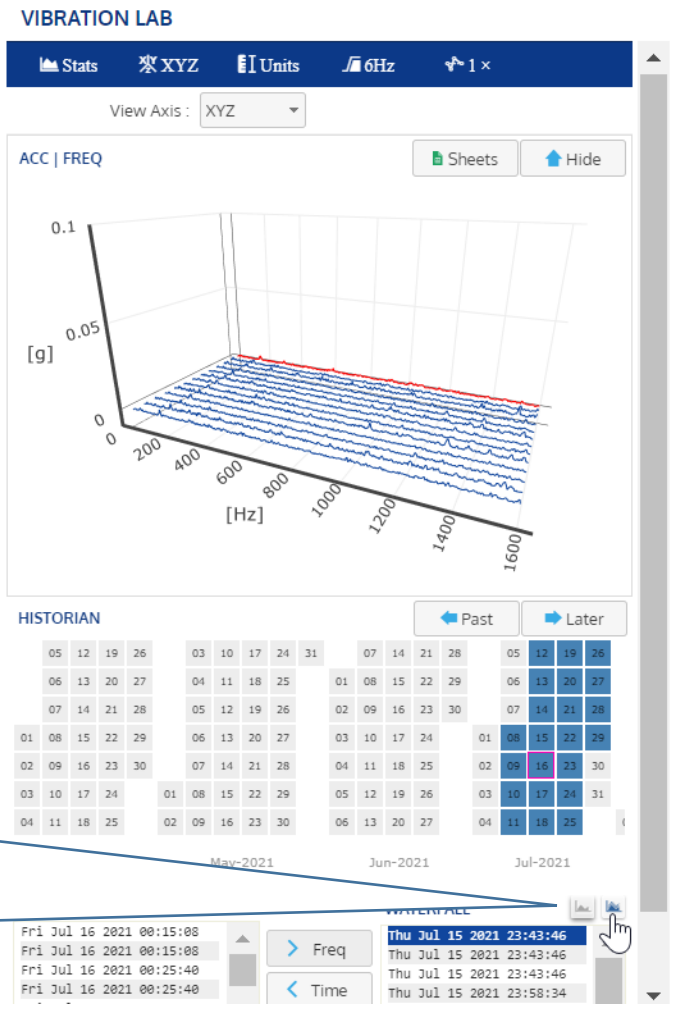
"6Hz" High Pass Filter tab

Select the high pass cut off frequency to remove the DC component and the low frequency noise in the RMS signal. See section 3.6.4.3 for more information.

Enable/disable 1/f flicker noise detrending (only for velocity spectra).

"1X" averaging tab

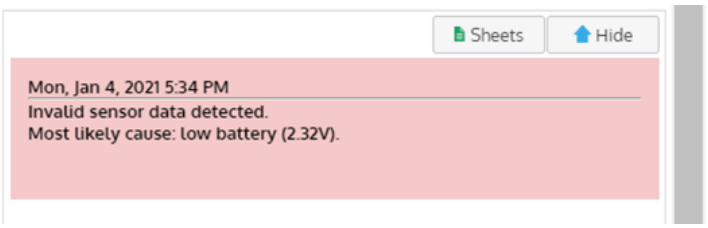
Enable/disable DFT averaging and select the number of averages. DFT averaging will decrease the noise level at the cost of a loss in resolution.



Clicking on the "Waterfall" icon changes the graph view from 2D to 3D. The graph now shows the combined spectra of all measurements from the spectrum box in a trending waterfall graph. Clicking on the "Spectrum" icon changes the view back to 2D mode.

3.6.4.1.1. Invalid data detection

The Sensor Dashboard will provide a warning in the Vibration Lab graph area instead of the plotted graph if the measurement you selected for plotting is not valid. The most likely cause of this invalid data is a low battery level.



3.6.4.2. Statistics pane

USER MANUAL

STATISTICS shows the recorded RMS, Kurtosis and MAD values during a selected time interval.

"Units" tab

Select the desired units: g or mm/s (acceleration/velocity).

Select the RMS, Kurtosis or MAD statistic.
Remark: the MAD statistic is only available for the MAD Vibration Sensor.

Select or unselect an axis by clicking on the colored square.

Select a start and end date in the proposed lists to create a graph. Click on a date in the historian to select a specific start or end date. Click on "Update" to update the graph. Click "Full" to select all available data. Click "Month" to select the data of the past month. Click "Week" to select the data of the past 7 days.

"6Hz" High Pass Filter tab

Select the high pass cut off frequency to remove the DC component and the low frequency noise in the RMS signal. See section 3.6.4.3 for more information.

3.6.4.3. Auto measurement and prefetch explained

Below is the explanation of the automatic vibration measurements and the correct use of 'prefetch' and RMS.

NOTE: RMS threshold does <u>not</u> apply for manually recorded vibrations with the REC button.

Automatic vibration measurements must be enabled, as shown above in section 3.5. The prefetch settings can be found and edited on 3 different places as shown in Figure 1 to Figure 3.

Note that the HPF value of 6Hz might not be the best setting. The choice of HPF value will be discussed below. Also, threshold=none is not recommended as explained below.

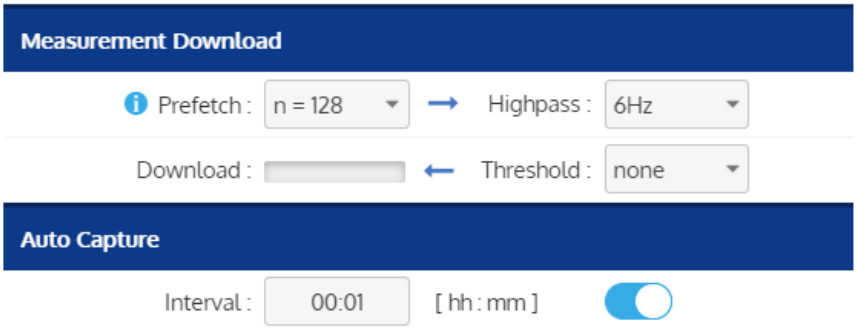


Figure 1: auto measurement setup and prefetch settings in vibration pane

Figure 2: prefetch settings in statistics lab pane

Figure 3: prefetch settings in vibration lab

These settings should be understood as follows:

1. The queue interval is 1 minute, so every minute a new measurement is started.
2. After a measurement is completed by the sensor, 128 'prefetch' samples (set in the vibration pane) are downloaded from the sensor.
3. The RMS value is calculated on these 128 samples (the "prefetch").
4. If the RMS value is larger than the threshold, the full vibration data is downloaded from the sensor. If not, all axes are suspended.
5. The threshold is 0g (none), so besides the 128 prefetch samples the full 1024 sample data is always downloaded in this case.

A very important parameter is the RMS high pass filter. This filter removes the DC offset (gravity) and the low frequency noise from the RMS signal (see Figure 4).

USER MANUAL

The RMS value is the power in all frequency bins above the HPF cut-off frequency. The images below (Figure 4 and Figure 5) are taken with no vibrations, just gravity and the sensor noise floor are seen.

However, with very few samples, such as in the case of a prefetch value of 128 samples, part of the DC offset and low frequency noise (plus the startup transient of the compression algorithm) may leak into higher frequency bins, due to the coarse resolution of the DFT. This can be seen below in Figure 5, for 128 prefetch samples. It can be seen here that an HPF value of 3 Hz is too low for a correct RMS value. In this case a better choice would be 6Hz or even higher.

Remark: The HPF cut-off frequency setting can be changed at any time to improve the interpretation and analysis of the DFT graphs (DFT graphs are always recalculated after each setting change). The HPF setting however has no influence on the data stored on the iQunet Server.

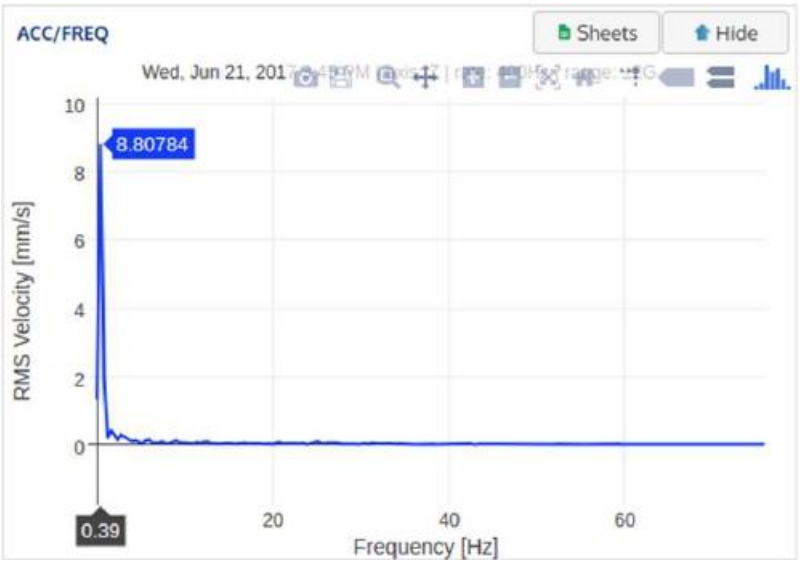


Figure 4: choosing the best setting for the high pass filter

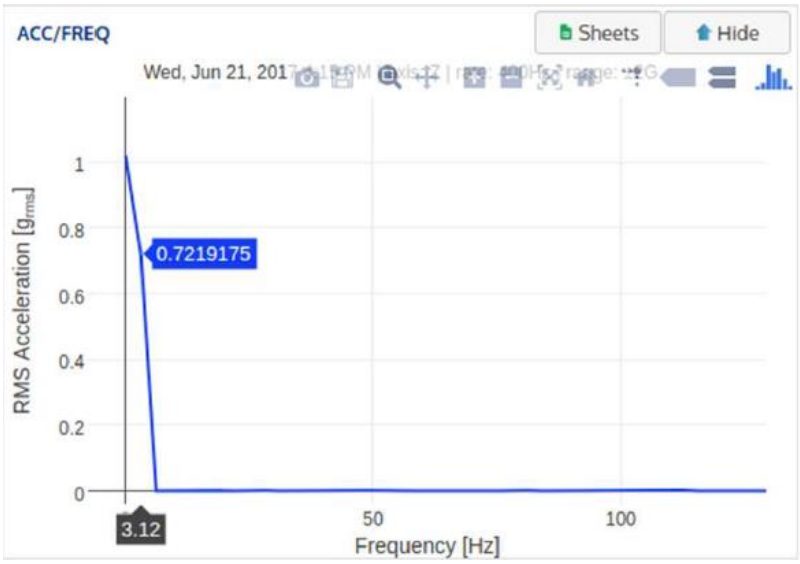


Figure 5: choosing the best setting for the high pass filter

USER MANUAL

iQunet recommends using the settings in the following table, based on the selected number of prefetch samples.

Table 1: recommended high pass filter settings

Number of prefetch samples	HPF value
256	6Hz or higher
128	12Hz or higher
64	25Hz or higher
32	50Hz or higher

Finally, to conserve battery power, it is important to set the threshold value to something higher than 0g (none) to prevent full downloads when the DUT is not active. It prevents the complete download of the 1024 samples in the example above. The result is that the battery lifetime may be extended at least one order of magnitude, since 10 times less data must be transmitted.

Clicking the information icon will show the flowchart of the Auto Capture procedure. The values in the flowchart change dynamically with the vibration/prefetch settings in the panes.

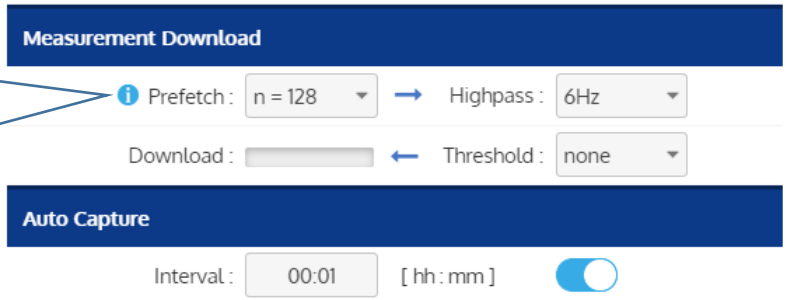


Figure 6: vibration pane

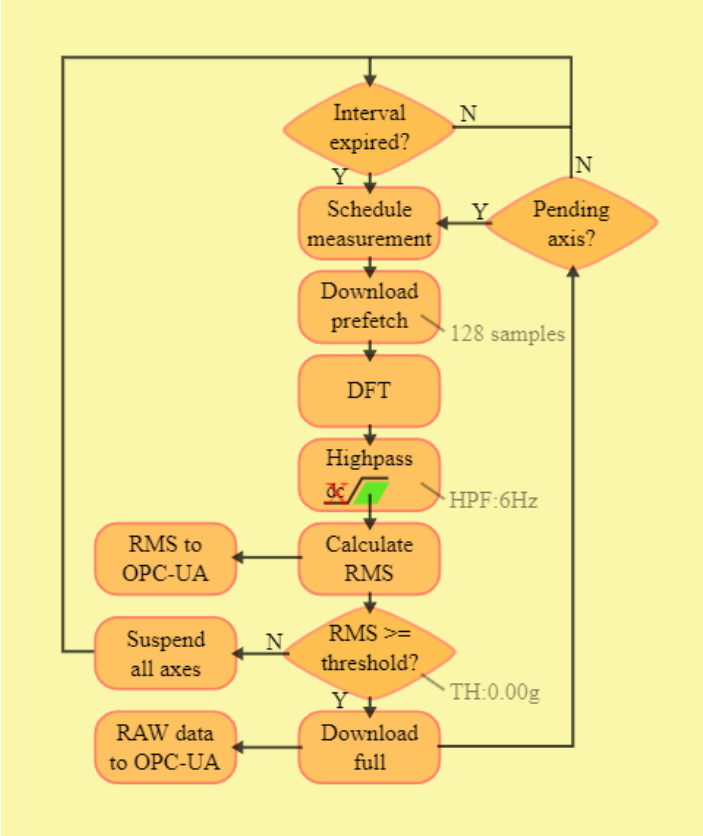
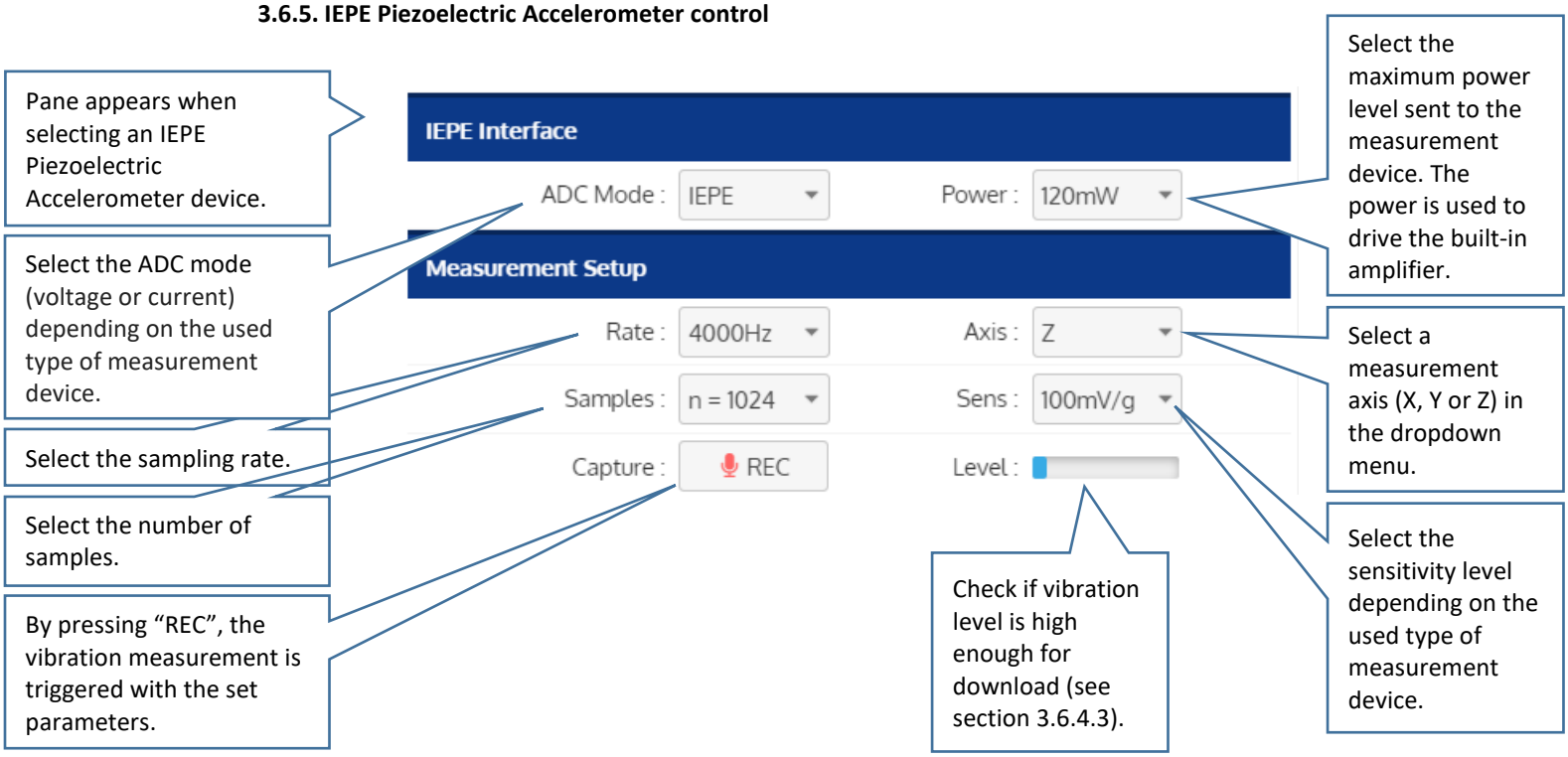
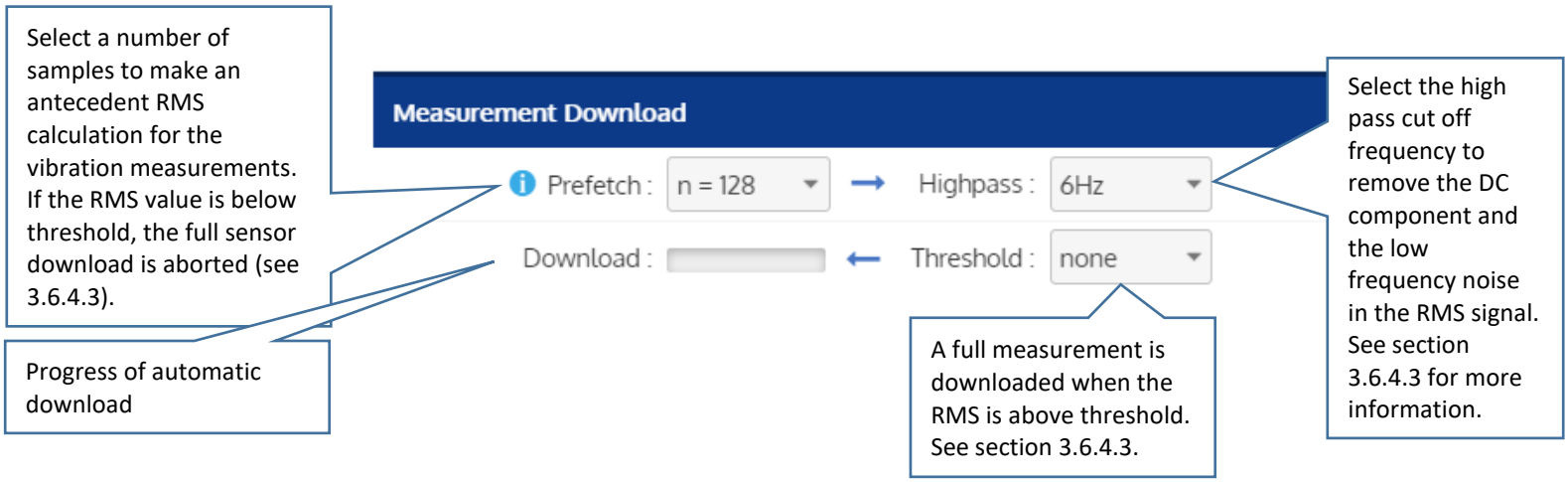


Figure 7: How data is sent to OPC UA and unwanted measurements are suspended (e.g. if the DUT is inactive)

3.6.5. IEPE Piezoelectric Accelerometer control

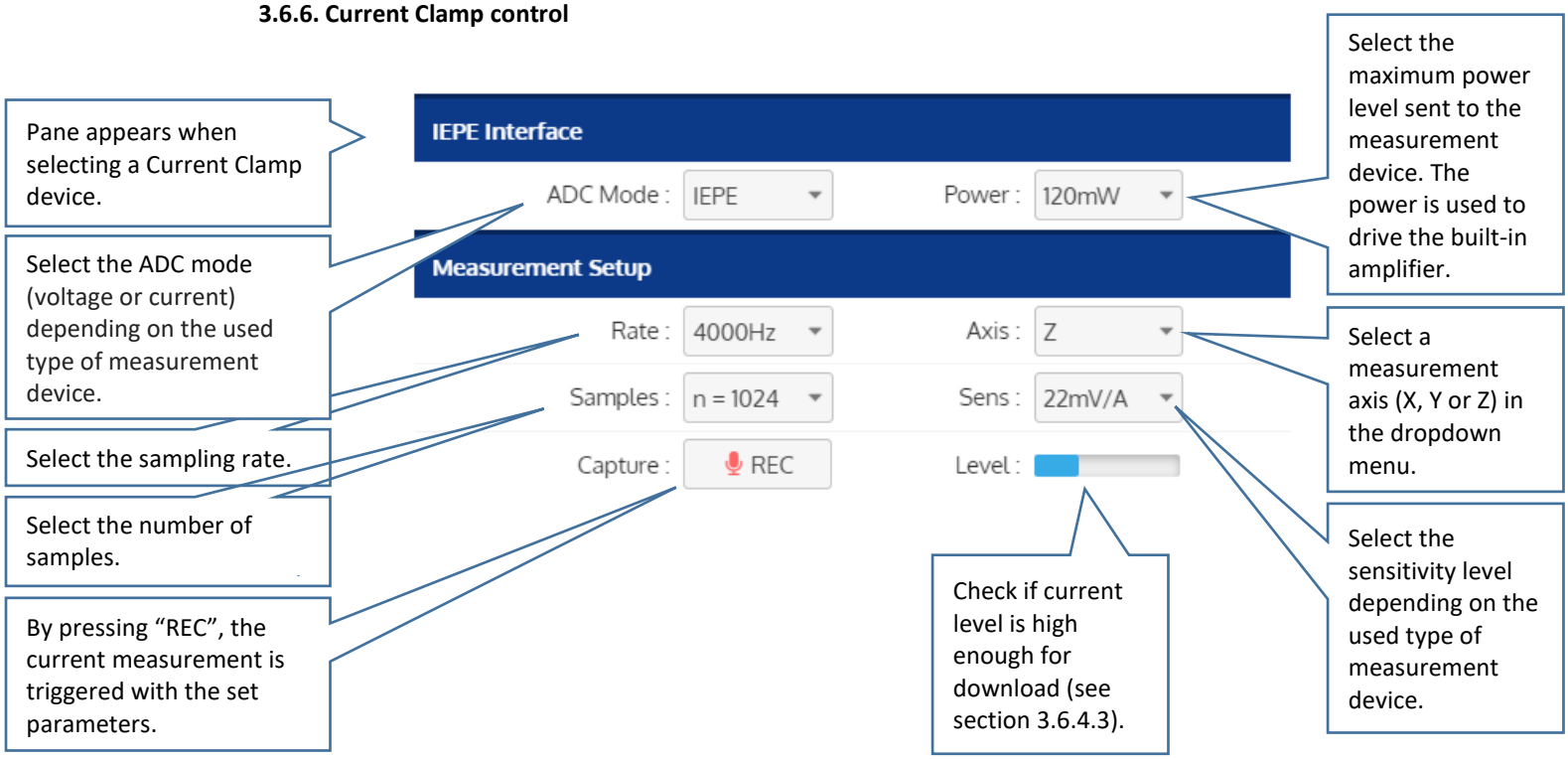


USER MANUAL

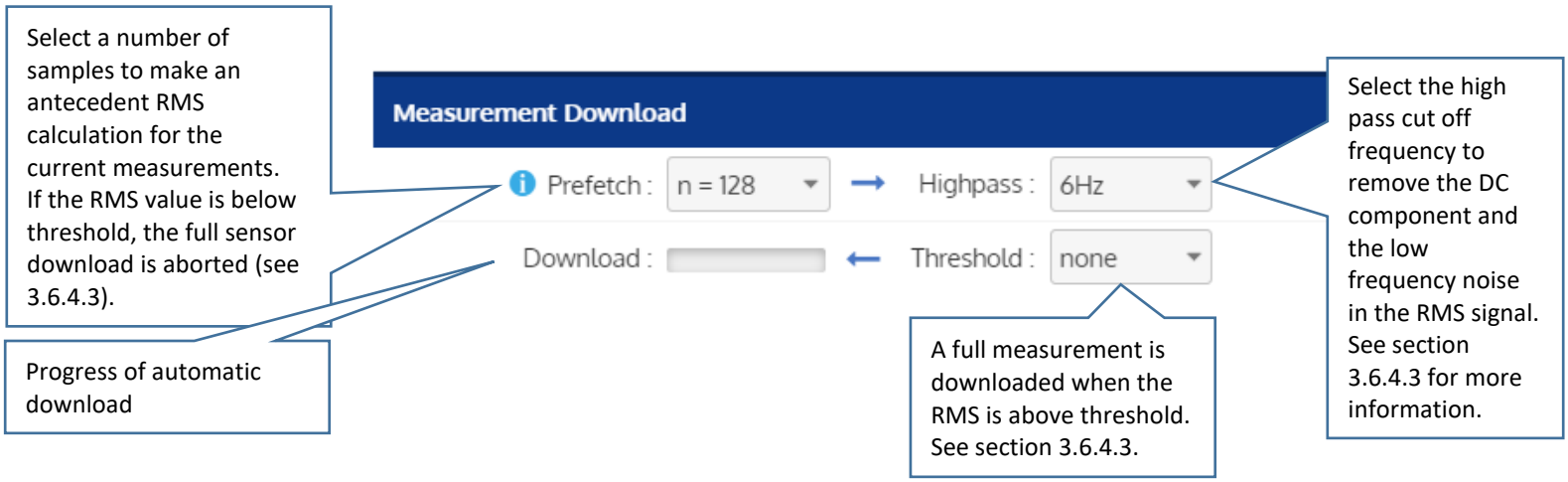


The Vibration Lab, Statistics pane and prefetch RMS calculation function in the same way as described in sections 3.6.4.1 to 3.6.4.3 for the regular Vibration Sensor.

3.6.6. Current Clamp control

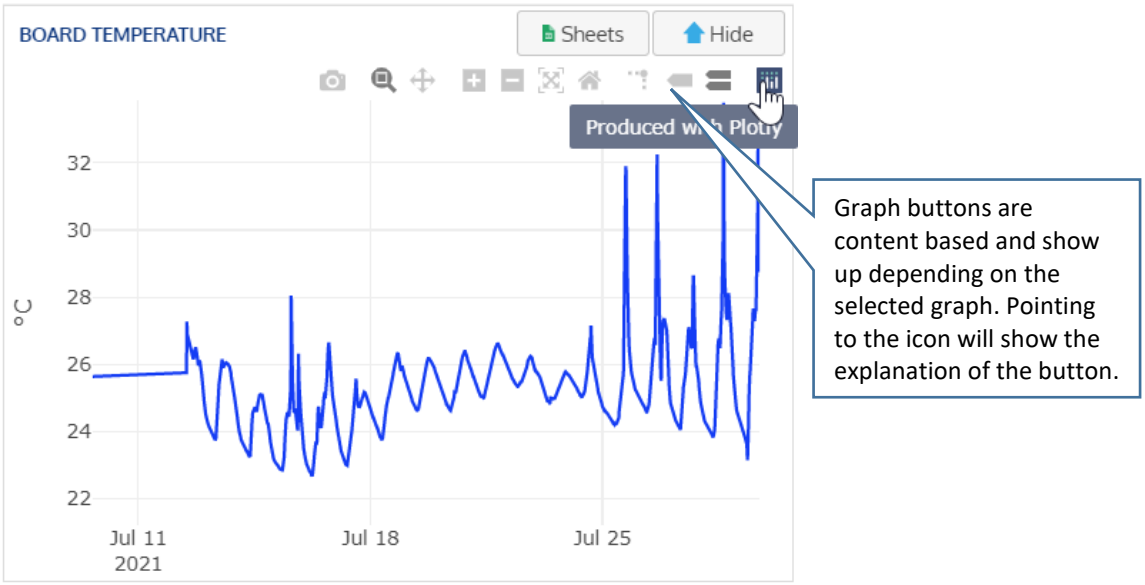


USER MANUAL



The Vibration Lab, Statistics pane and prefetch RMS calculation function in the same way as described in sections 3.6.4.1 to 3.6.4.3 for the regular Vibration Sensor. The only difference is that the Vibration Lab is renamed to Current Monitor and that the used units are current (A) and charge (A.s) instead of acceleration (g) and velocity (mm/s).

3.7. Content based graph settings



USER MANUAL

4. Export of data

4.1. Using OPC UA functionality

By connecting to the embedded OPC UA Server on the iQunet Server that is connected to the Base Station, you can read the data gathered by the iQunet sensors. Data is stored for a longer period, but the oldest data will be overwritten when the memory is full. It is strongly advised to install an OPC UA historian server to save the data permanently. Please contact your network administrator for more information on how to access the data. By connecting an OPC UA client to the running iQunet OPC UA Server, you can read the data as it is gathered by the sensors. The graphs in the iQunet Dashboard are using the same OPC UA data from the same source. Figure 8 and Figure 9 show the same temperature data on the iQunet Dashboard and in the OPC UA client.

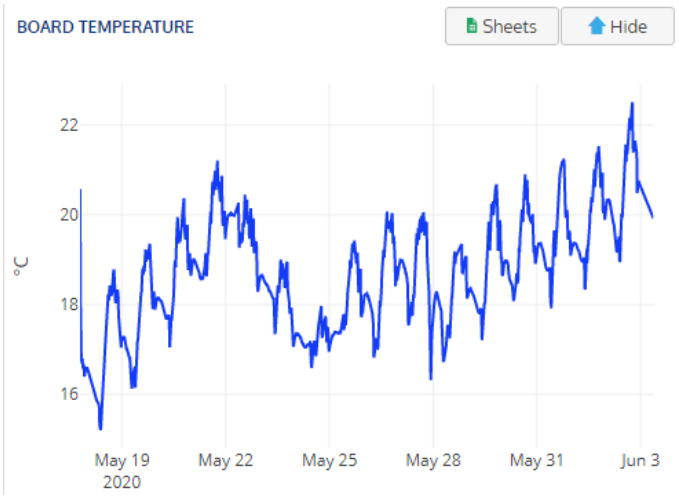


Figure 8: OPC UA data (board temperature) viewed in the iQunet Dashboard

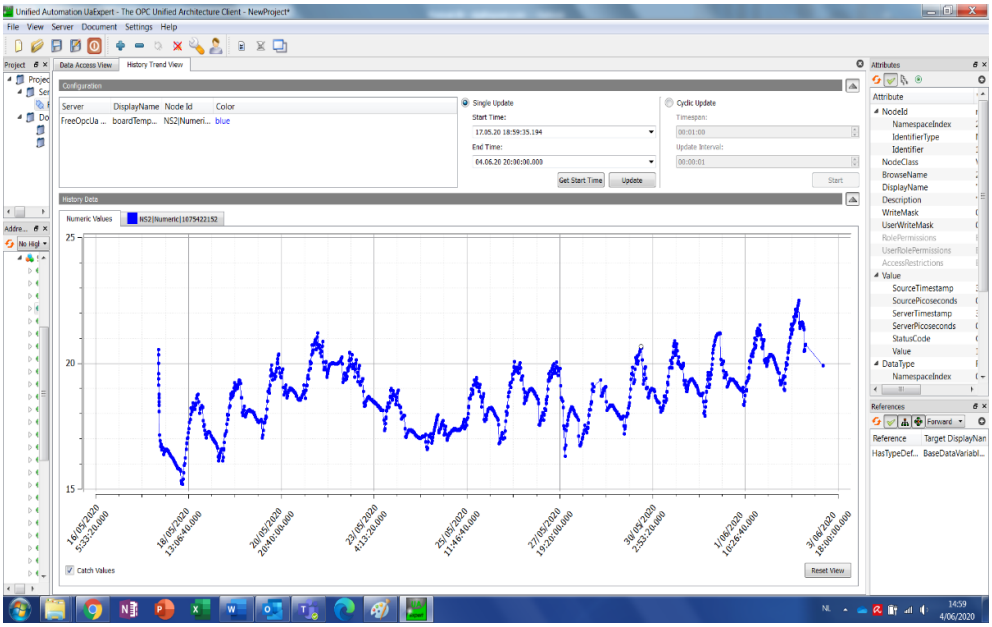


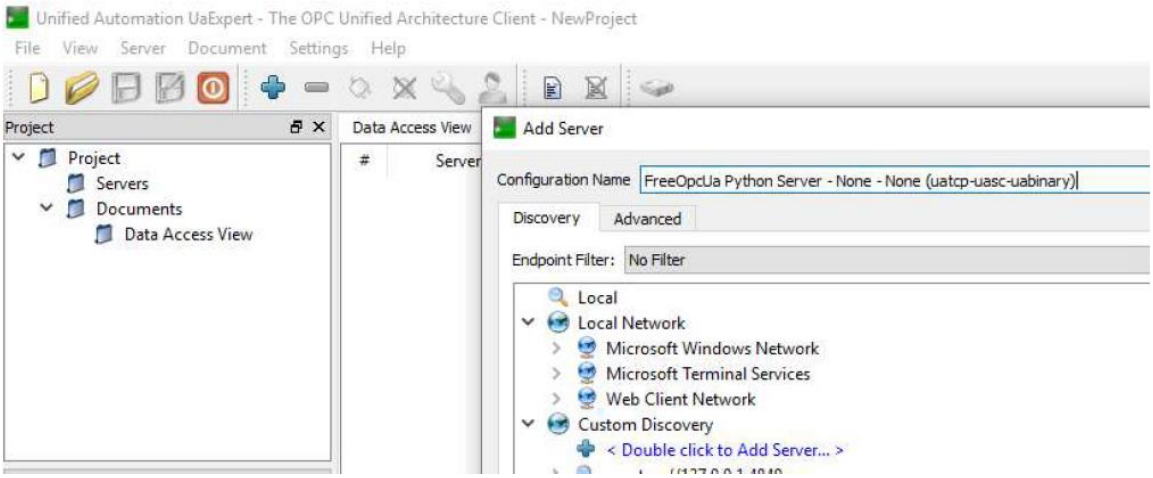
Figure 9: OPC UA data (board temperature) viewed in an OPC UA client

USER MANUAL

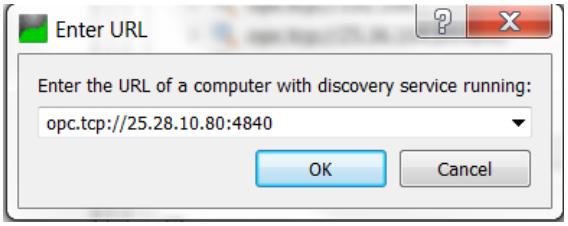
4.1.1. Setting up OPC UA client

For test purposes it is possible to set up an OPC UA client with free OPC UA client software.

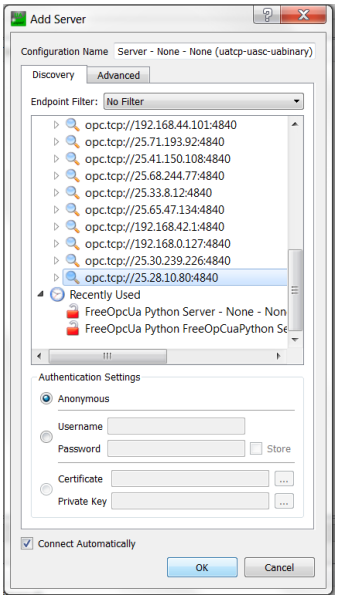
1. Download the free OPC UA client software and install it from the following link: https://www.unified-automation.com/products/development-tools/uaexpert.html.
2. Open the UA Expert software and add a new server by selecting “Add” in the Server tab. Double click on “Double click to Add Server”.



3. Edit the URL to e.g. opc.tcp:// 25.28.10.80:4840 (see also section 5.2) and click OK.

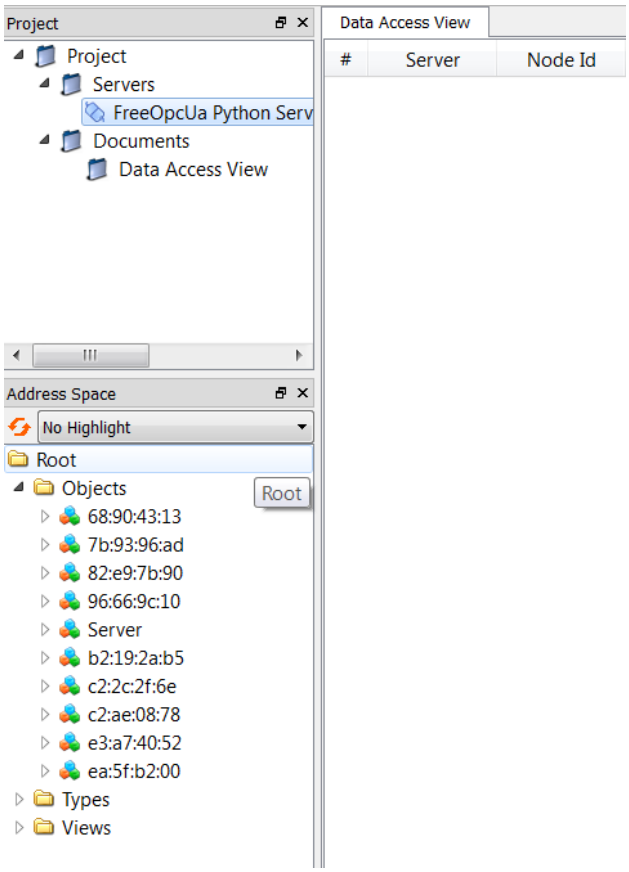


4. Select your added server in the list and click OK. If necessary, thrust the certificate of the iQunet Server.

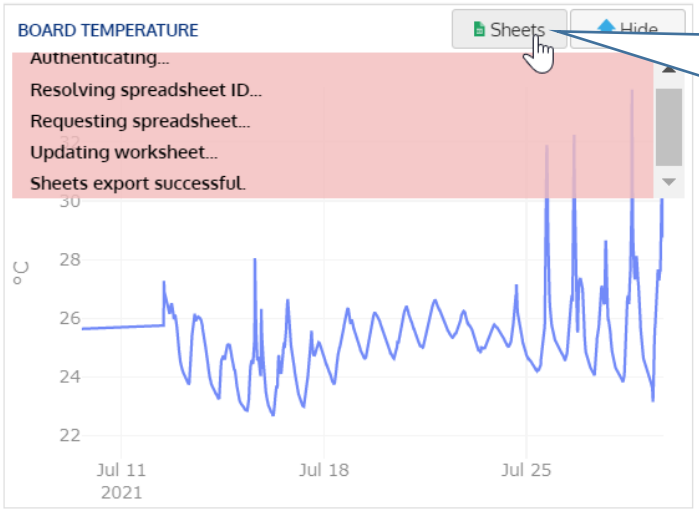


USER MANUAL

5. All connected iQunet sensors will appear in the object list.
6. Browse the attributes of the sensors by clicking on the tags.



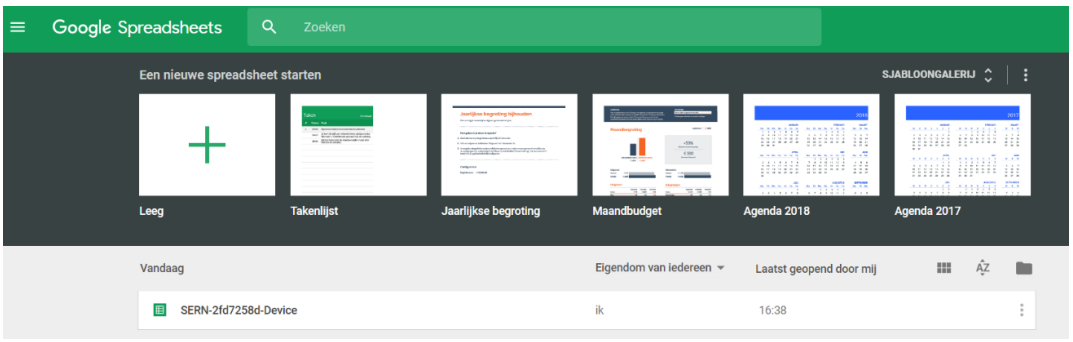
4.2. Using Google Sheets Export functionality



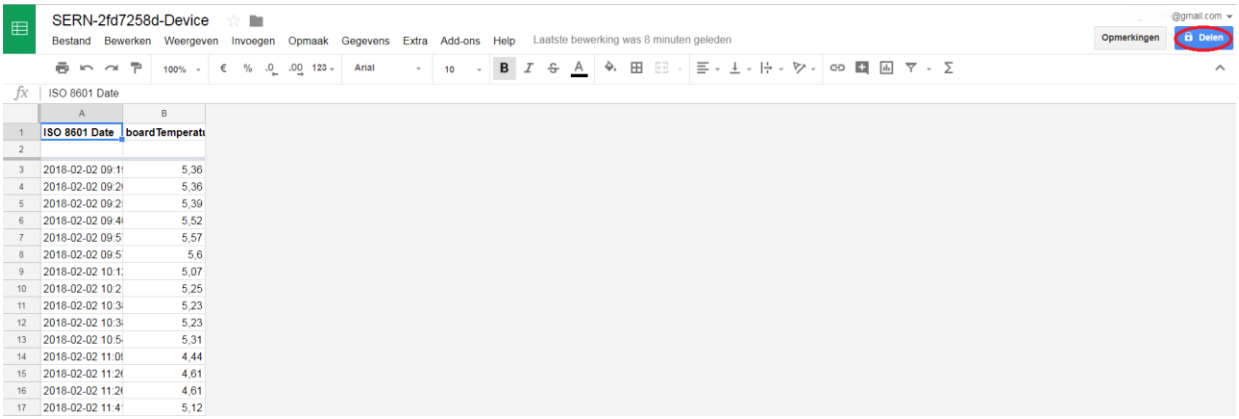
Pressing “Sheets” exports the OPC data to Google Sheets. By pressing the button again, the same sheet is updated with new values.

USER MANUAL

By clicking “Sheets”, a Google spreadsheet is created in the account you used to identify yourself at login.



Go to Google Sheets, and you will see the file you created from this sensor by clicking the “Sheets” button. The data is updated every time you click the “Sheets” button in the same graph. Exporting new data parameters of the same sensor will create new tabs in the same file.

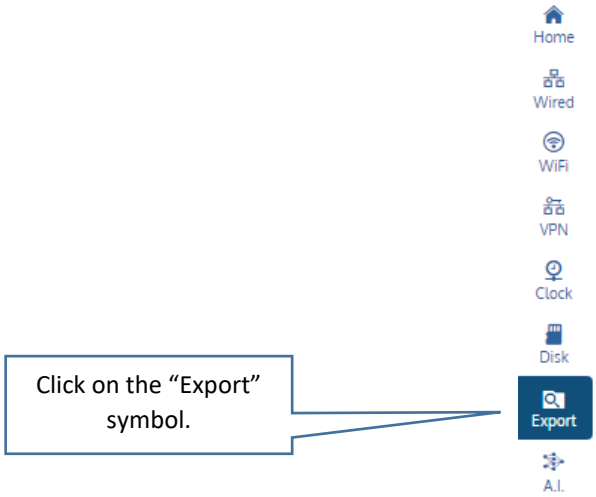


Open the file you created, and you can explore the data points or use plug-ins to analyze the data. Share the file with others by clicking the right upper blue button. Shared files will also be updated with new data once created. It is also possible to save the data in Microsoft Excel format.

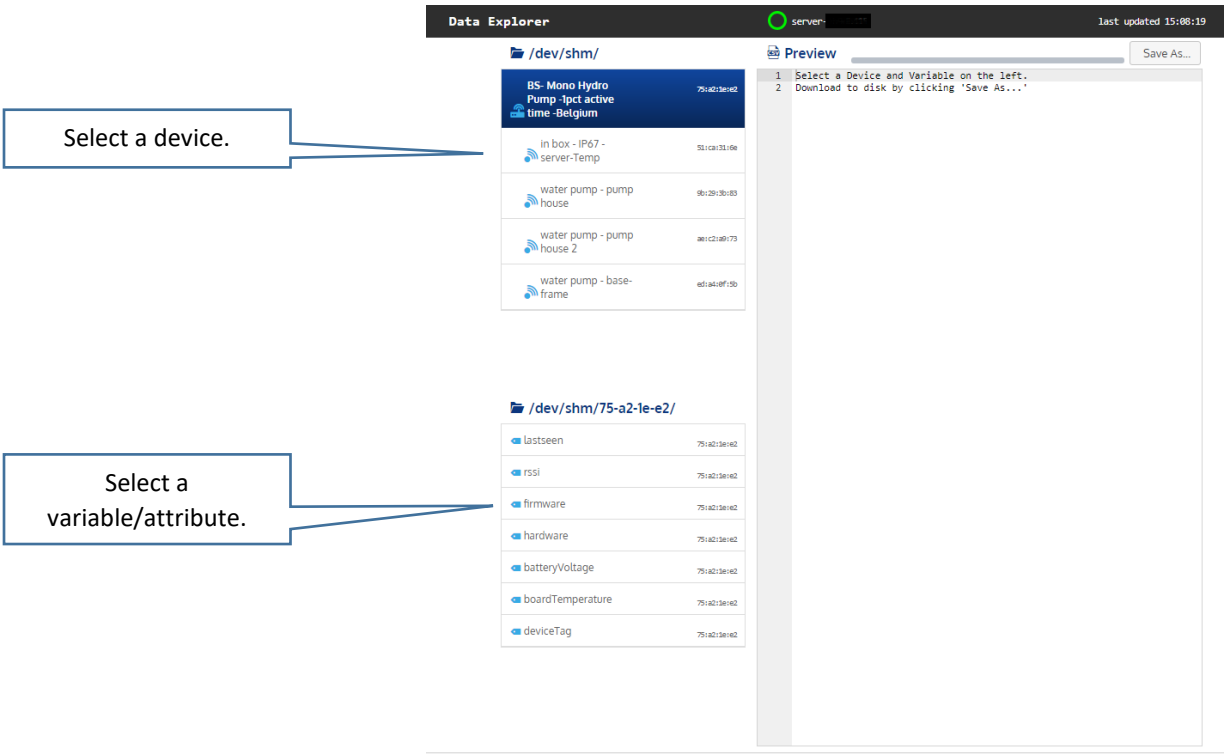
USER MANUAL

4.3. Using Data Explorer Export functionality

Open the “Data Explorer” functionality by clicking on the “Export” symbol on the left-hand side in the Dashboard.

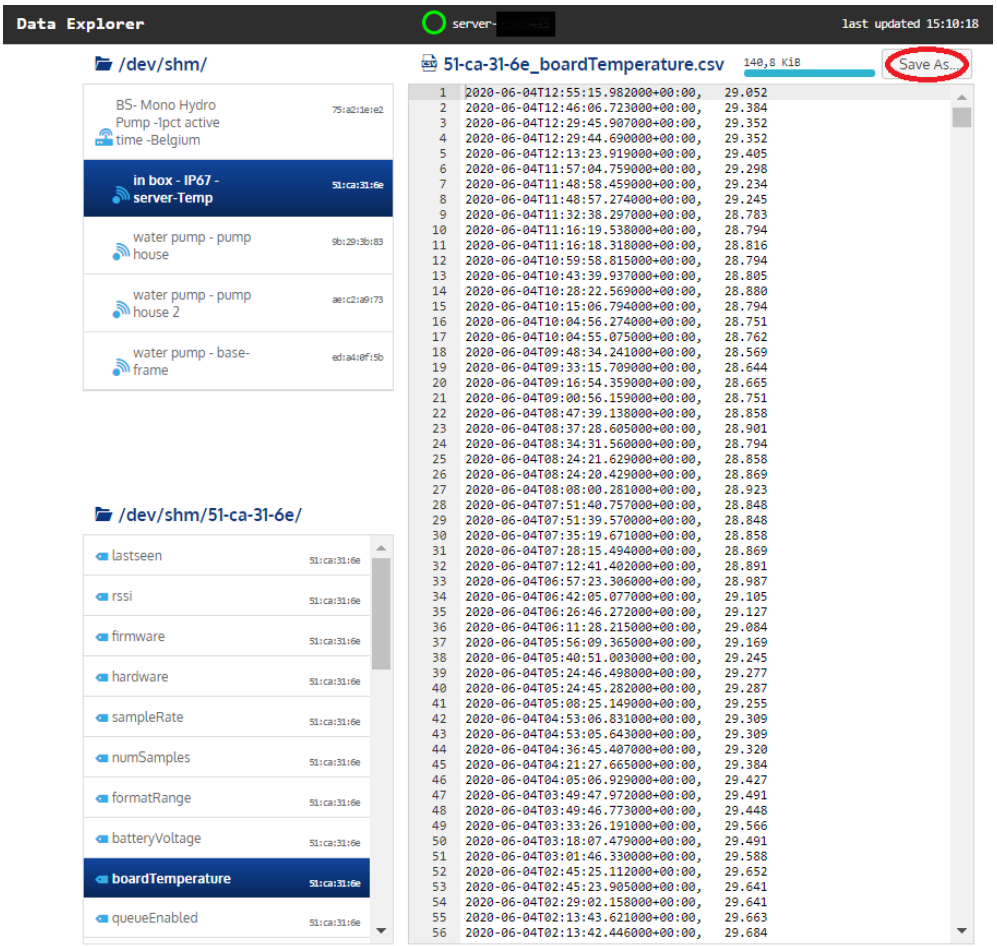


Select a device and according attribute on the left.



USER MANUAL

The data for this attribute will be loaded in the text box on the right in a csv format. Click on “Save As…” to download the data as a .csv file. For large amounts of data, the data loading might take a few minutes.



4.4. Using APIs

4.4.1. General

GraphQL is a query language for APIs and a server-side runtime for executing queries by using a type system that is defined for the data. GraphQL is not tied to any specific database or storage engine and is instead backed by the existing code and data. GraphQL is typically served over HTTP via a single endpoint which expresses the full set of capabilities of this service. This contrasts with the REST APIs which expose a suite of URLs each of which exposes a single resource. Many different programming languages support GraphQL. A GraphQL spec was open sourced in 2015 and is now available in many environments and used by teams of all sizes. Some introductions can be found on http://graphql.org/.

Features:

- Syntax highlighting
- Intelligent type ahead of fields, arguments, types, and more
- Real-time error highlighting and reporting
- Automatic query completion
- Run and inspect query results

USER MANUAL

4.4.2. Starting with APIs

Before starting, we strongly recommend reading the “learn” section on the GraphQL website: http://graphql.org/learn/.

All APIs can be reached via http://xxx.xxx.xxx.xxx:8000/graphql where “xxx.xxx.xxx.xxx” refers to the current iQunet Server IP address (see section 5.3). Please note that all documentation is included and can be found in the Documentation Explorer on the right-hand side.

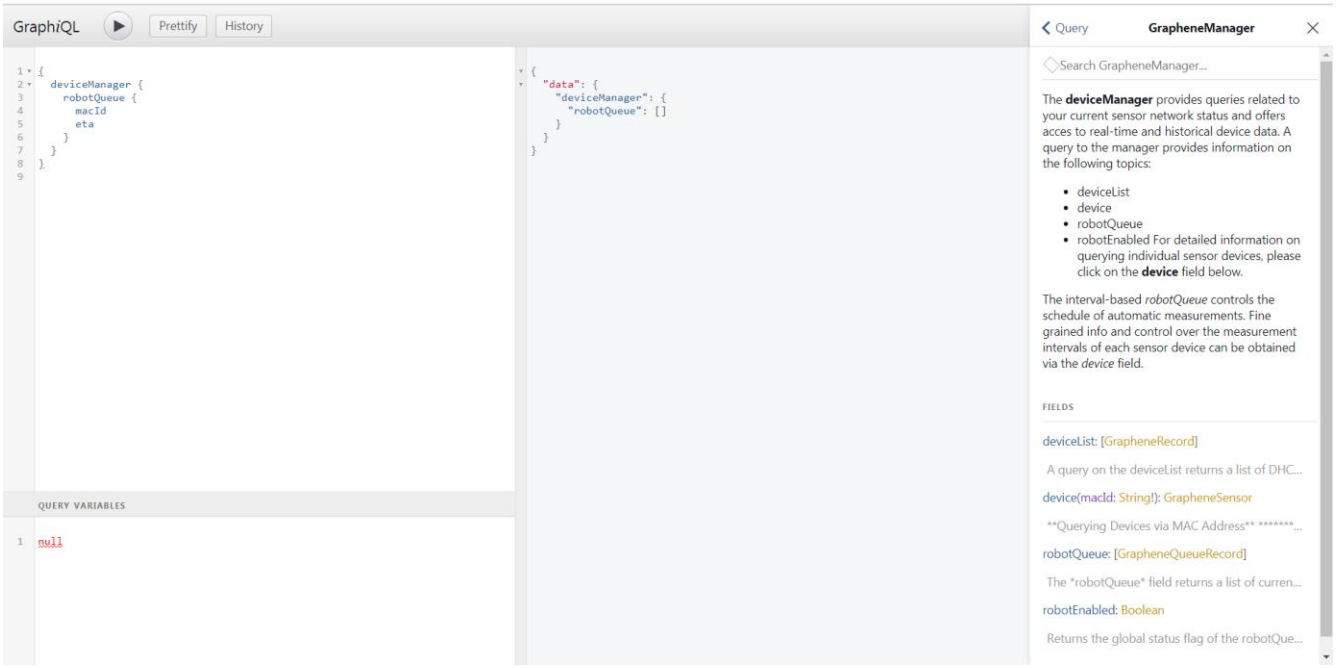


Figure 10: The iQunet graphical interactive in-browser GraphQL IDE (Integrated Development Environment)

Remark: it is also possible to use a client library to access the GraphQL Server. A list of all available GraphQL libraries can be found here: https://graphql.github.io/code/.

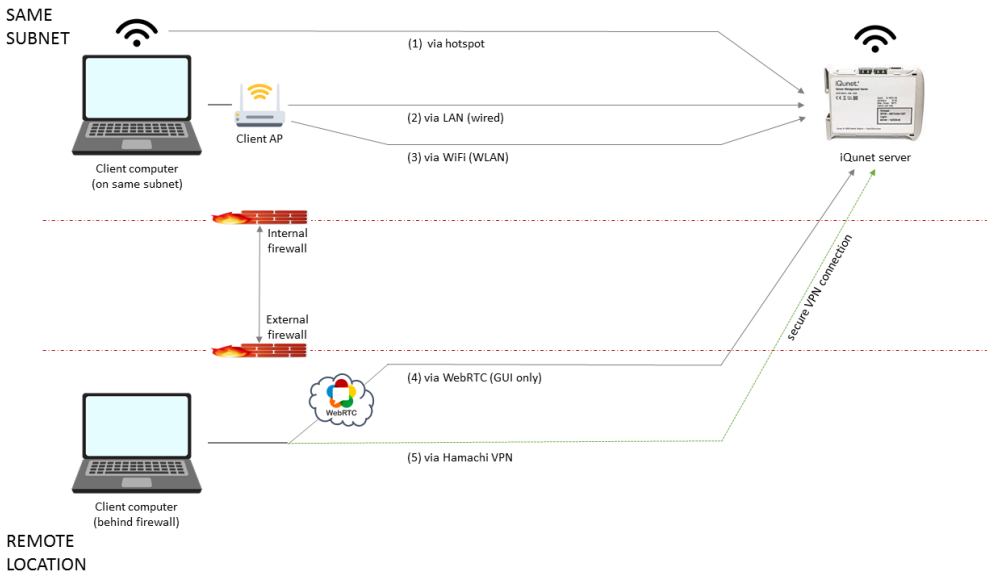
USER MANUAL

5. Connection to the iQunet Server

After connecting the iQunet Server to the 230V mains and if available to the network, there are several options to connect to the Server (see figure below):

1. Via WiFi hotspot (section 5.1). The IP address of the Server is always 192.168.42.1. An active network connection is optional.
2. Via local/direct access (LAN) where Server and client server are on the same subnet (section 5.2).
3. Via WiFi /WLAN (section 5.3). An active wireless network connection is required.
4. Via WebRTC (connect.iqunet.com). This only works for the Dashboard GUI. An active network connection is required. This procedure has already been described in section A.
5. Via Hamachi commercial VPN (section 5.4). An active Hamachi network is required.

Remark: section 5.5 describes which network connection (LAN, hotspot, or WiFi) takes precedence in connecting to the iQunet Server.



On all listening interfaces, the ports are fixed: 8000 for the Sensor Dashboard and GraphQL, 4840 for OPC UA, 9001 for the supervisor (pw: admin/admin) and port 22 for SSH.

5.1. Hotspot

5.1.1. Connect to hotspot

A WiFi hotspot is automatically created once the iQunet Server is connected to the 230V mains (even without connection to the network). A reboot of the server can be necessary if the hotspot does not become active immediately.

Remark: if the "Auto Off" option of the hotspot is enabled; the hotspot will only become active if there is no other active network connection available (wired or wireless). See section 5.1.2 for more info on the "Auto Off" mode.

To use the hotspot's WiFi network on your PC, select the hotspot in your network center (SERN-xxxxxxxxxxxx) and click Connect. The hotspot's password is the Sensor Proxy ID (also used for the connection to WebRTC in section A). This ID is written on your iQunet Server (e.g. server-xxxxxxxx).

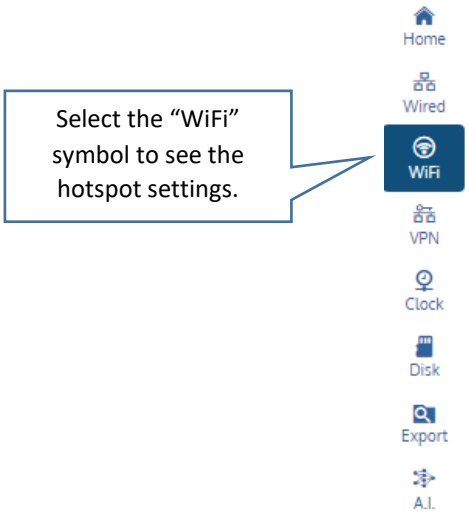
The IP address of the server is always 192.168.42.1. Once connected to the hotspot network, you can use this IP address to make a direct access connection to the server by browsing to http://192.168.42.1:8000/dashboard/app (see section 5.2 for more information). You can also use the server's IP address to set up an OPC UA client or to access the GraphQL APIs (see sections 4.1.1 and 4.4.2).

When the iQunet Server is connected to the network, you can also connect via WebRTC as explained in section A.

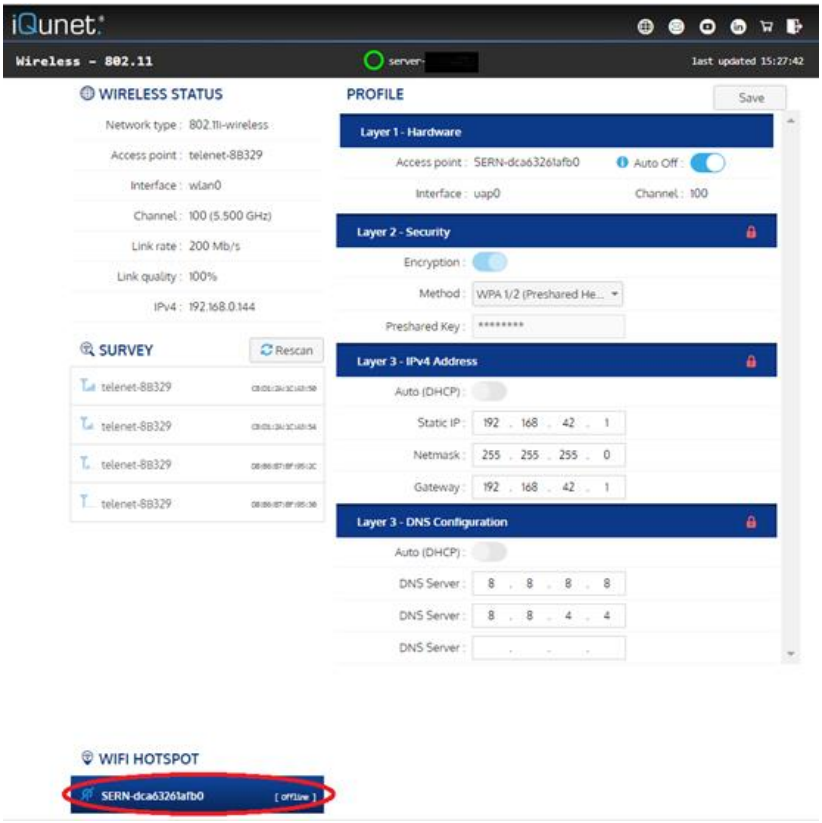
5.1.2. Turn off hotspot

Connect to the iQunet Sensor Dashboard via WebRTC (see section A) or via direct access (http://192.168.42.1:8000/dashboard/app). 0pen the "Wireless – 802.11" panel to see the hotspot settings by clicking on the "WiFi" symbol at the left-hand side on the Dashboard.

USER MANUAL



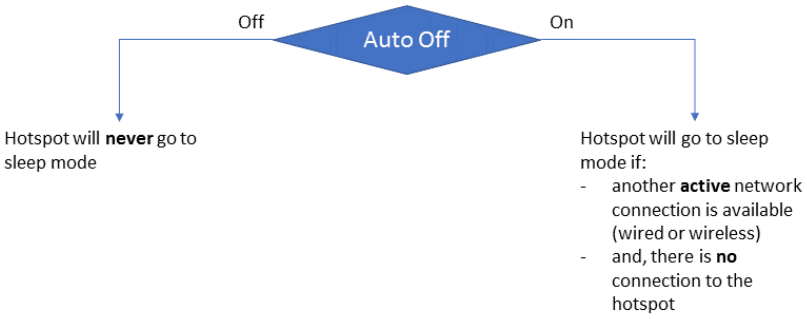
In the “WIFI HOTSPOT” section you can find the state of the hotspot (active/offline) and the hotspot’s network name (SERN-xxxxxxxxxxxx). Click on the hotspot’s name (SERN-xxxxxxxxxxxx) to see more details on the hotspot network.



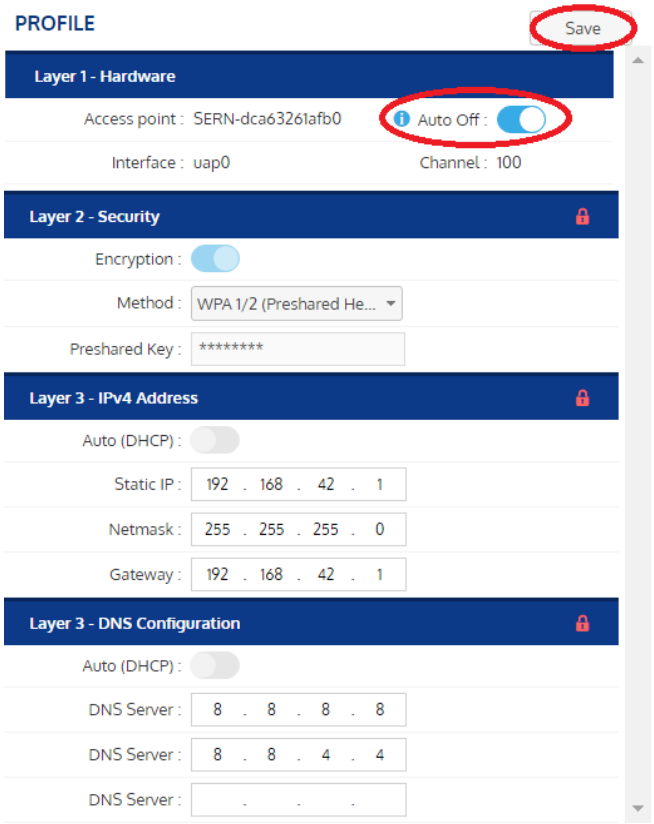
To turn off the hotspot, the user can activate the auto sleep mode of the hotspot by enabling “Auto Off” in the hardware layer. Slide the slider to the right and click the Save button in the upper right corner. When enabled, the hotspot will automatically turn off after maximum 10 minutes if another active wired or wireless

network connection is available. If the other network connection drops down, the hotspot will become active again.

Important remark: the hotspot will not turn off when there is still someone connected to it.

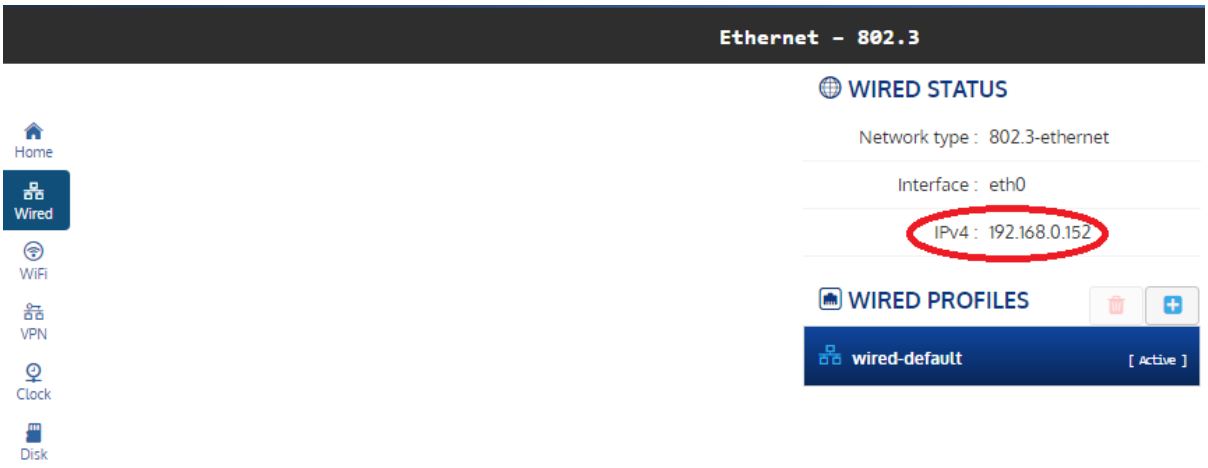


The other network settings shown below are not user adaptable.

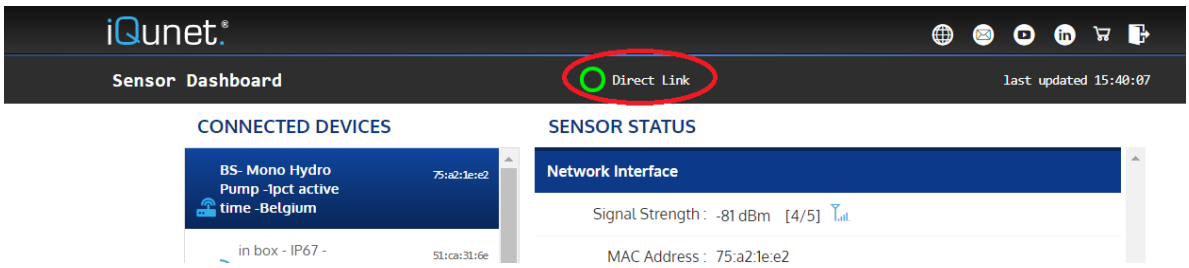


USER MANUAL

5.2. Direct Access setup (local access/intranet)



1. Open the "Ethernet – 802.3" panel by clicking on the "Wired" symbol on the left side.
2. Copy the network IPv4 address of the running iQunet Server.
3. Copy the address into http://xxx.xxx.xxx.xxx:8000/dashboard/app and open it in your Chrome browser.
4. From a computer in the SAME network and subnetwork you will now have direct access to the iQunet Server.
5. If the connection is established, "Direct Link" will appear next to the green circle instead of the server name "server-xxxxxxxx".



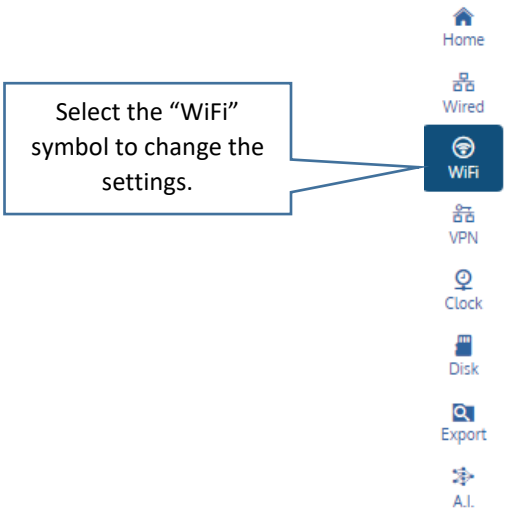
5.3. WIFI setup

Important remark 1: you can either use the hotspot functionality (a wired internet connection is not required) or a wired connection to the internet (either via a network in the neighborhood, or via a wired mobile MiFi connection) to establish the wireless connection. The wired connection can be disconnected once the Wi-Fi connection is established.

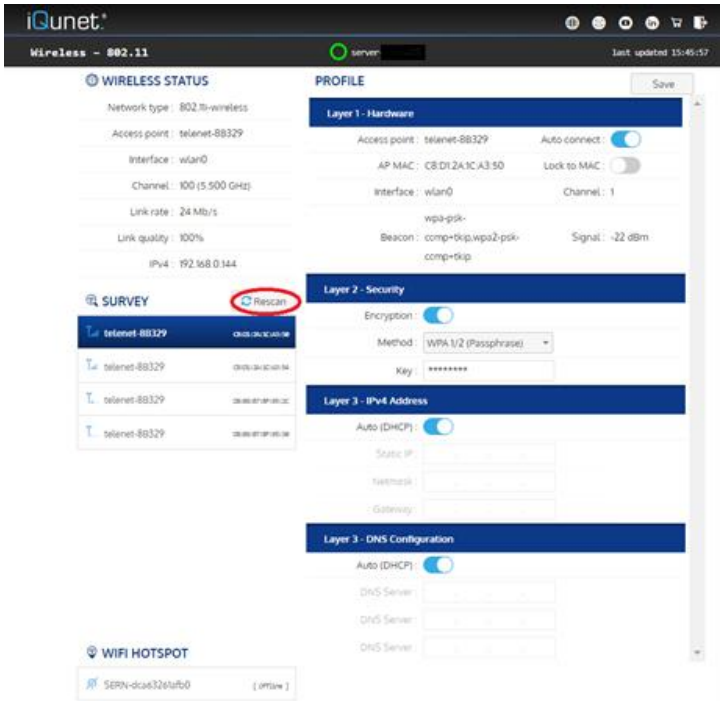
Important remark 2: if you are using multiple simultaneous connections, the Ethernet interface will have precedence over the Wi-Fi interface. The Ethernet interface is the preferred connection. The Wi-Fi interface can be used if Ethernet is not available.

USER MANUAL

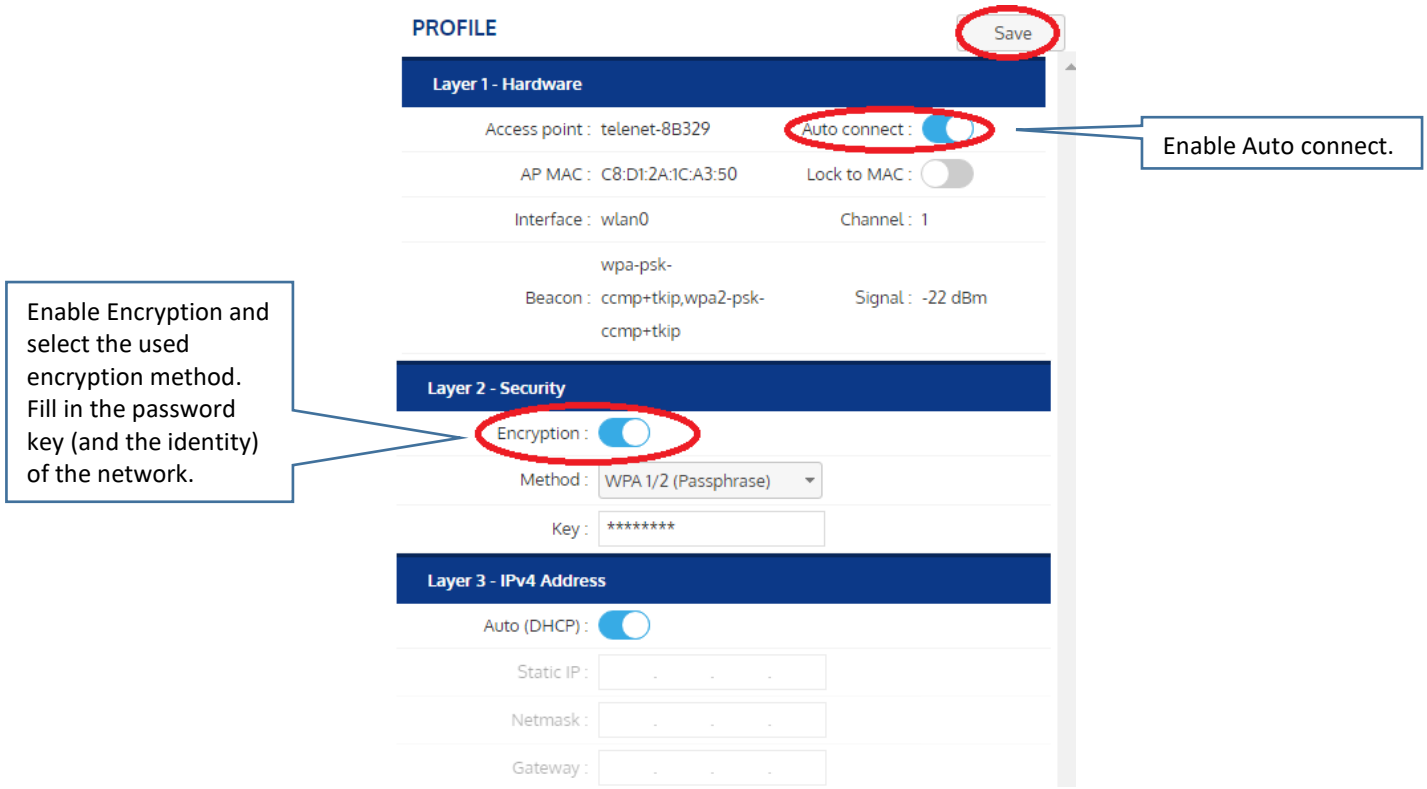
Browse to the iQunet Sensor Dashboard via WebRTC (see section A) or via direct access to the hotspot (http://192.168.42.1:8000/dashboard/app). For more information on the connection to the hotspot see section 5.1.1. Open the “Wireless – 802.11” settings by clicking on the “WiFi” symbol on the left side.



Rescan for wireless networks in the “SURVEY” section. Select the wireless network you want to connect with. Enable the encryption.



USER MANUAL



Now press the “Save” button on top of the pane.

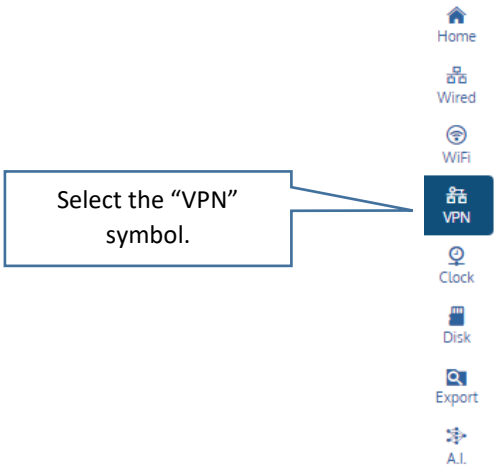
Enable the “Auto Off” option of the hotspot in the “Wireless – 802.11” control panel so the hotspot will be disabled immediately when a Wi-Fi connection is detected (see section 5.1.2 for more information on how to turn off the hotspot).

If you are using a wired connection, disconnect the Ethernet cable.

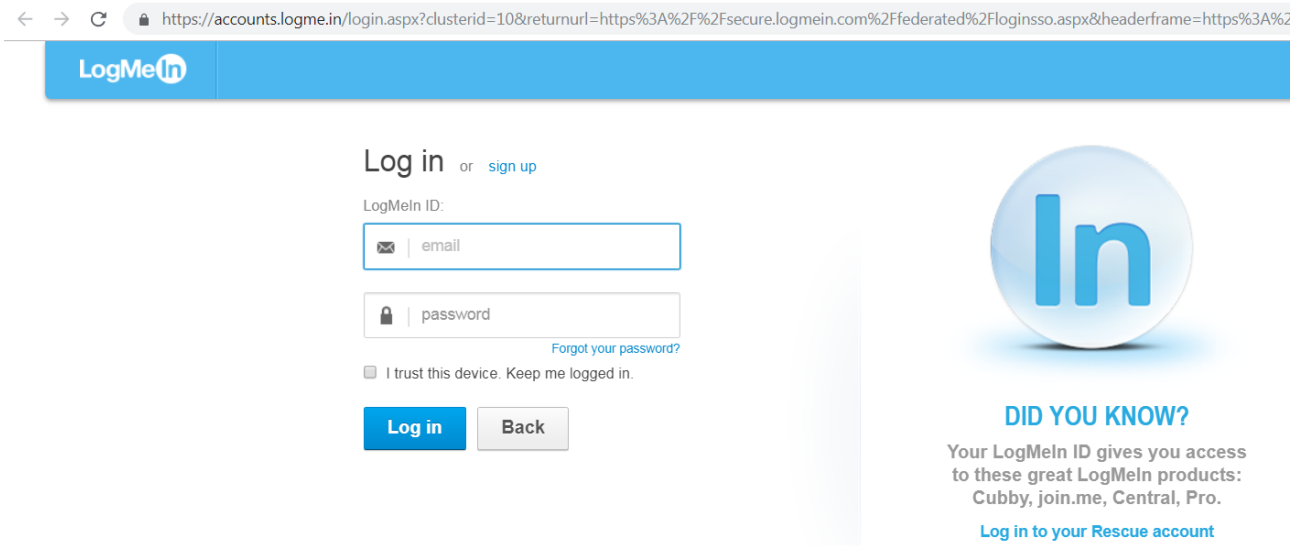
Put the iQunet Server with the connected Base Station on the desired spot in reach of the selected Wi-Fi network.

5.4. Hamachi VPN

In the “Hamachi – VPN” section you can join an existing VPN network. Open the “Hamachi - VPN” panel by clicking on the “VPN” symbol on the left side.

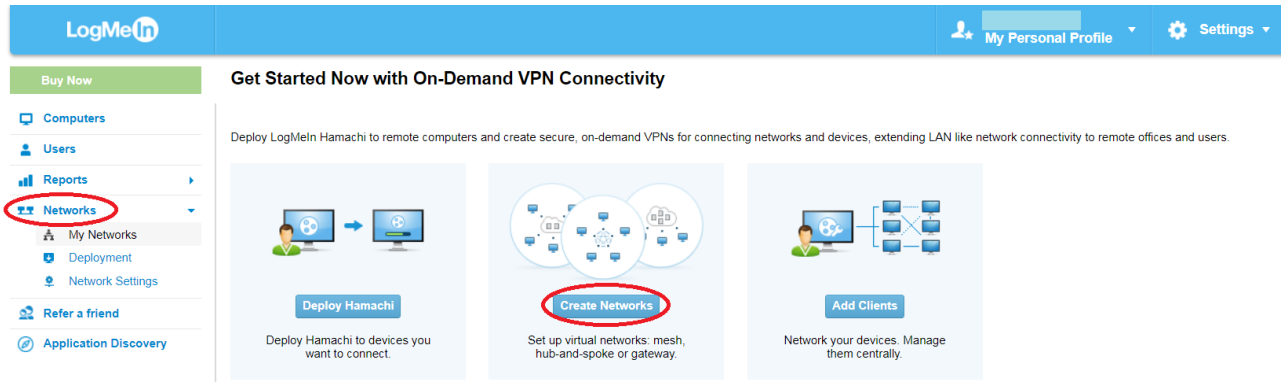


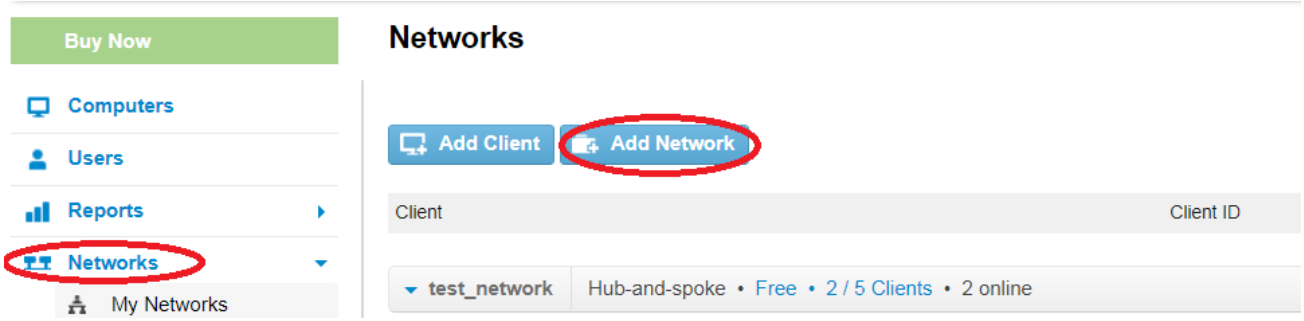
To create a Hamachi VPN network, browse to https://secure.logmein.com/central/Central.aspx and create an account or log in with your account credentials.



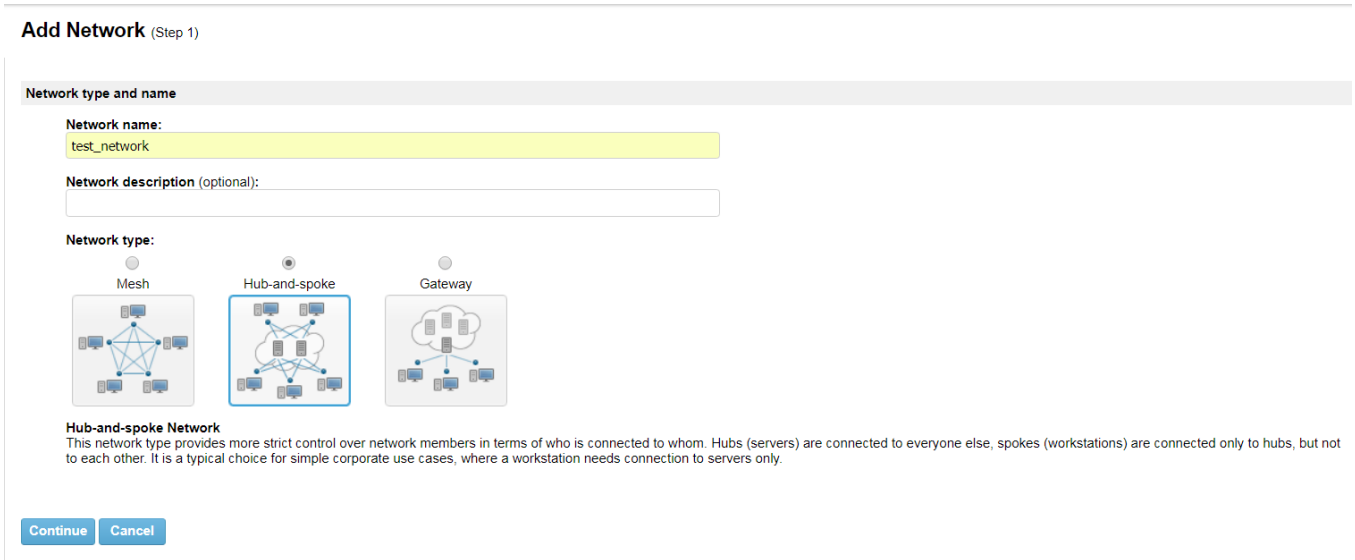
USER MANUAL

Go to the Networks section and click on “Create Networks” if this is the first network you create or “Add Network” for the following networks.



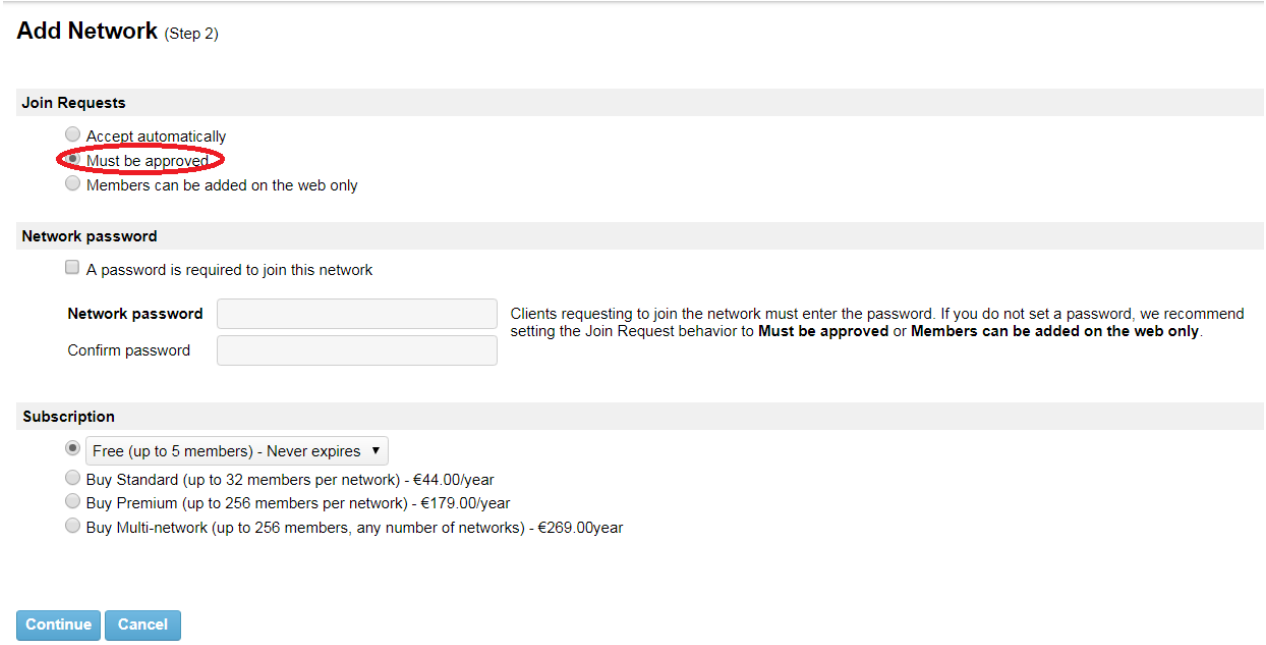


Fill out the network name. Select “Hub-and-spoke” as the network type and click Continue.

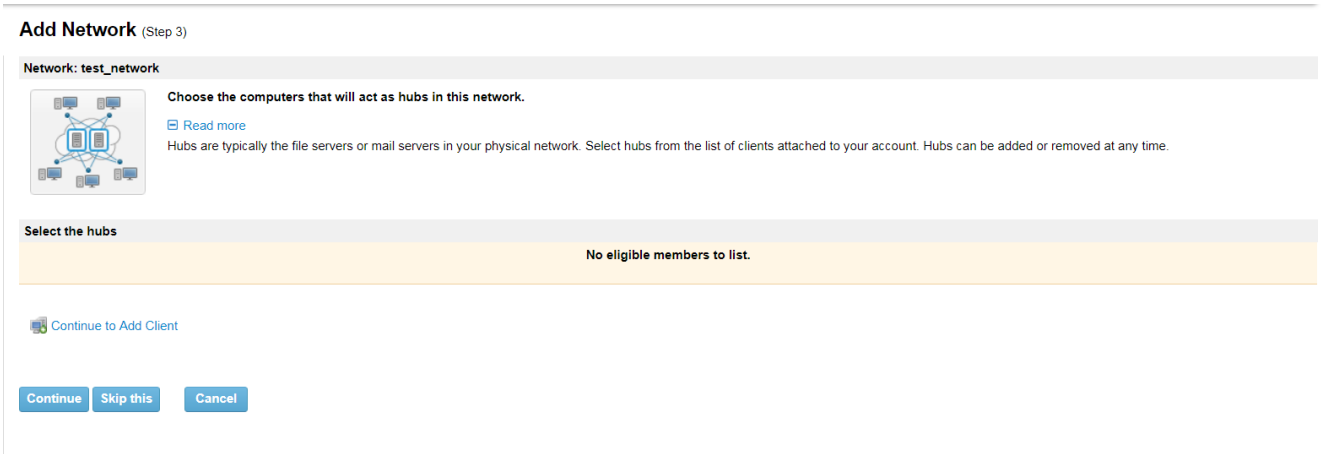


USER MANUAL

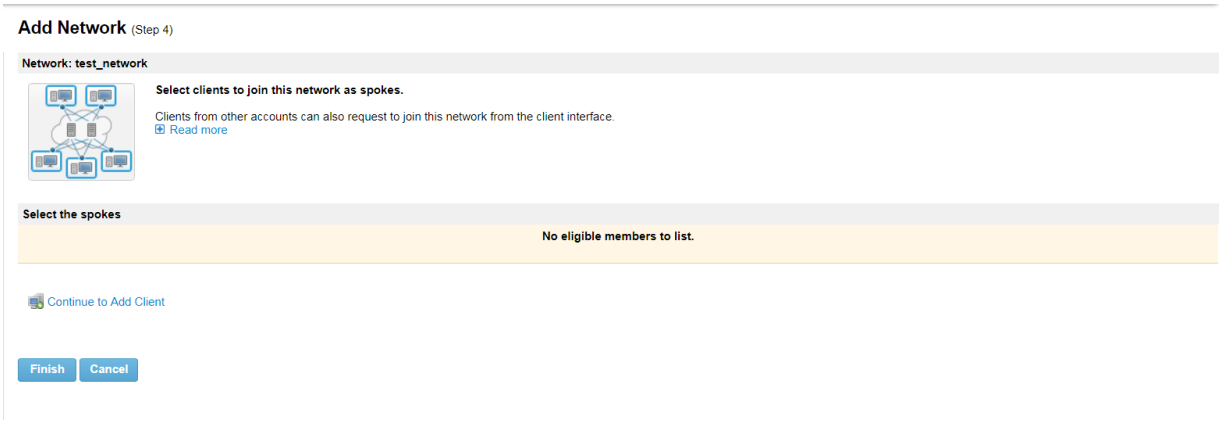
Check the “Must be approved” option in the “Join Requests” section and click Continue.



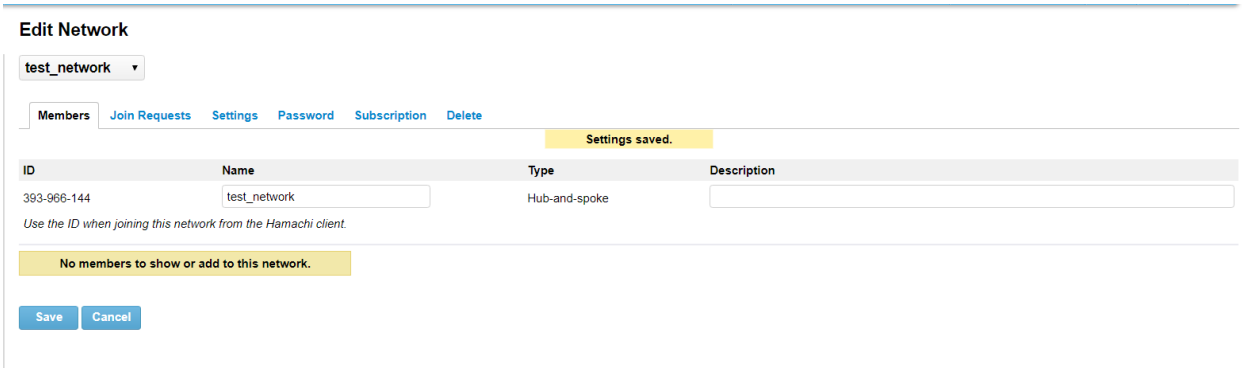
Click Continue.



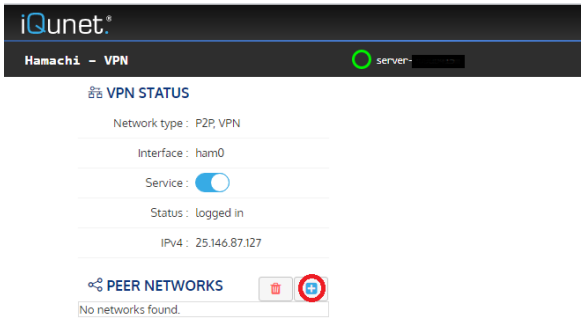
Click Finish.



Your VPN network is now created. You can find the ID by editing the network.

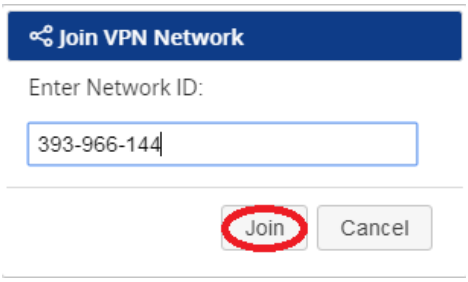


Add the VPN network in the iQunet Sensor Dashboard by clicking the plus sign in the “Hamachi – VPN” panel.

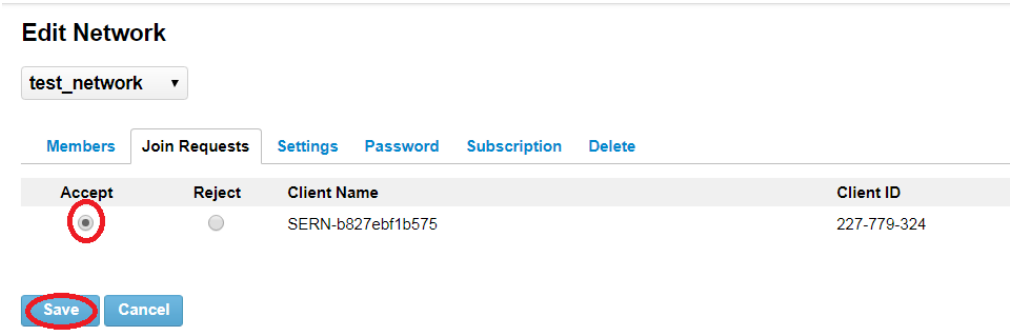


USER MANUAL

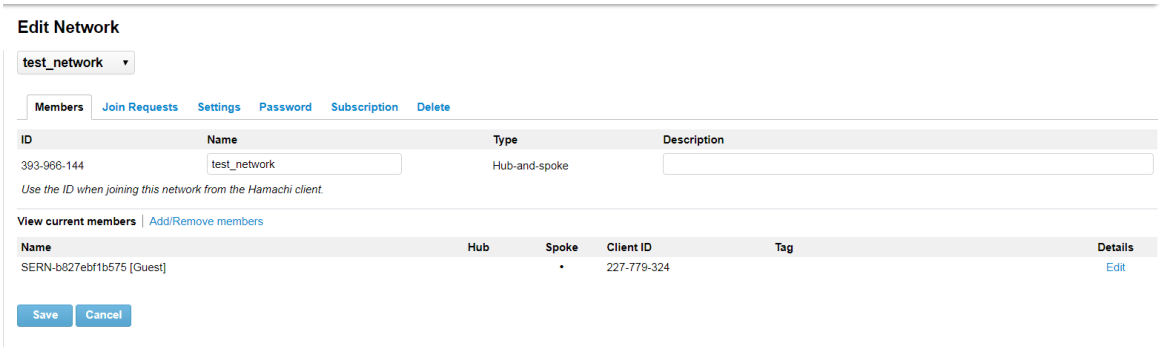
Enter the network ID and click the Join button.



Go back to the Hamachi Logmein website and accept the iQunet Server as a client in the “Join Requests” section of the created network.



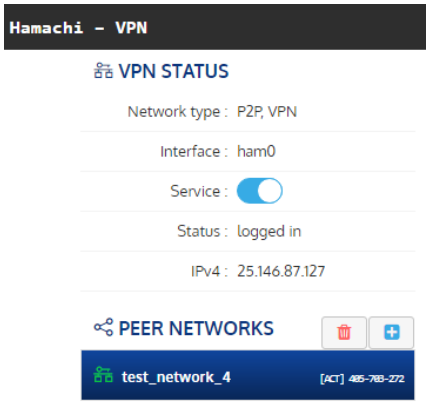
The iQunet Server will now appear in the Members section of the VPN network.



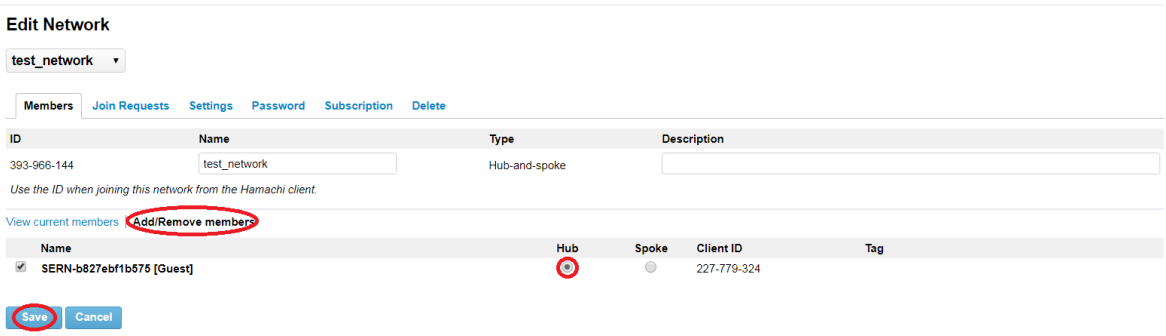
USER MANUAL

Reselect the “VPN” symbol on the left side in the iQunet Sensor Dashboard and the VPN network will appear in the list of peer networks.

Remark: the list of peer networks is not updated automatically since Hamachi doesn’t provide any sign or warning when changes have been applied. For this reason, you need to reopen the “Hamachi -VPN” panel to update the list of peer networks.



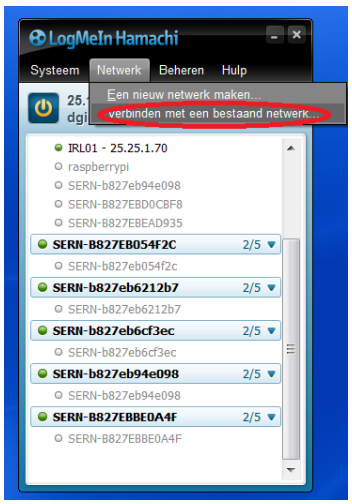
Set the SERN-xxxxxxxxxxxx to act as a hub on the Logmein web page by clicking on “Add/Remove members”. Check the Hub box and press Save.



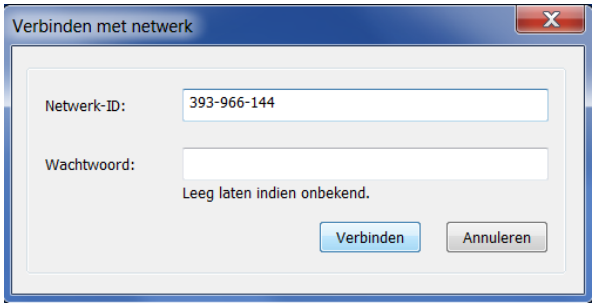
You now need to add your personal computer to this network. Download the Logmein Hamachi software from www.vpn.net.

USER MANUAL

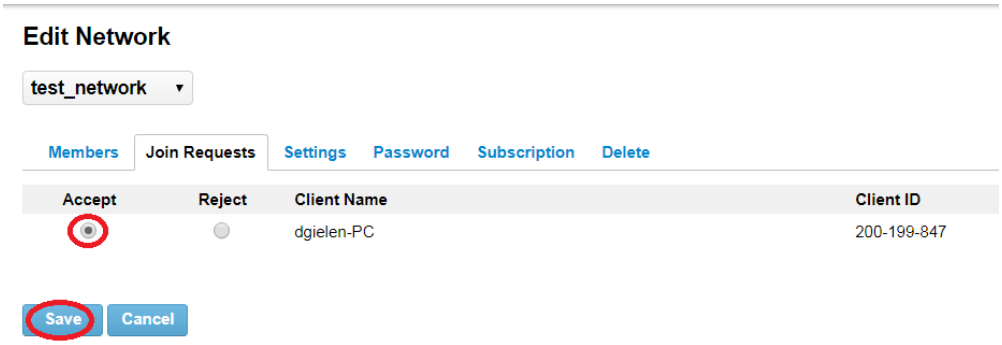
Open the software and click on the Network tab. Select “Join an existing network”.



Fill out the network ID and click Connect. Confirm that you want to ask for membership.

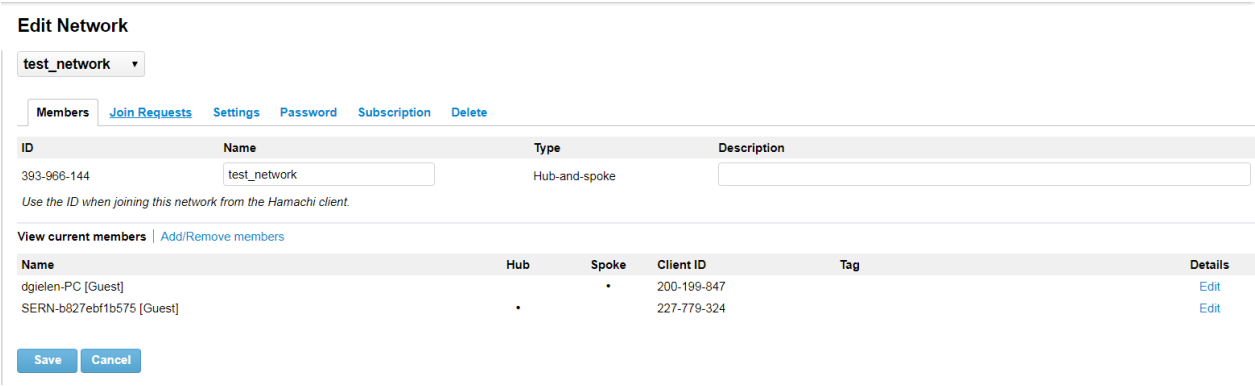


Accept your PC as a client in the Join Requests section on the Logmein page and click Save.



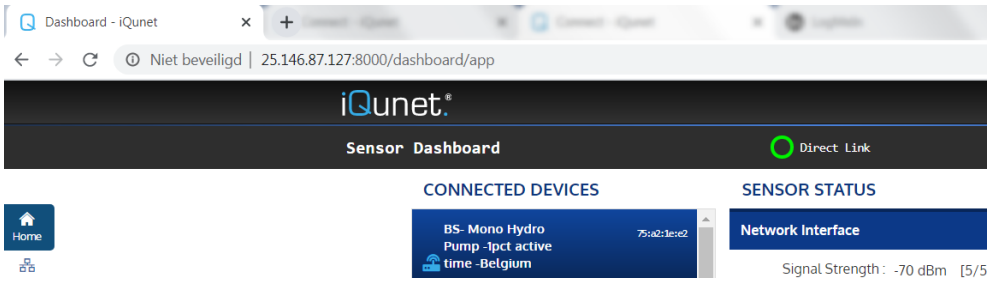
USER MANUAL

Now both your PC and the iQunet Server should be in the list of network members. Make sure that the iQunet Server is listed as a hub.



You can find the IP address of this VPN network in the “Hamachi – VPN” control panel. You can now use this IP address instead of the IP address listed at “Ethernet – 802.3” to for example make a direct access connection or connect with UA Expert.

Copy the IP address into http://xxx.xxx.xxx.xxx:8000/dashboard/app and open it in your browser. You will now get a direct link to the iQunet Server.

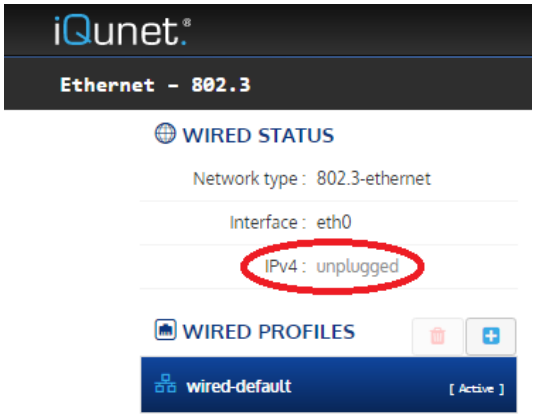


5.5. Preferred connections of the iQunet Server

The flowchart below shows which connection to the iQunet Server will take precedence if several connection types are used simultaneously.

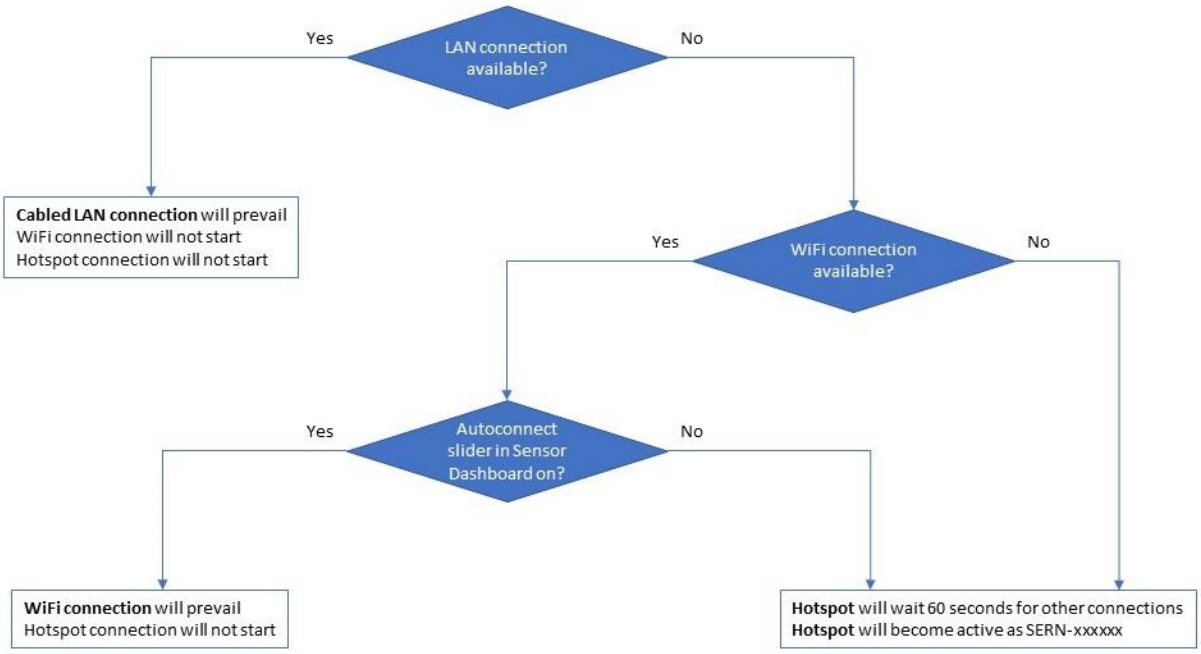
a) If there is a cabled LAN connection available, the cabled LAN connection will take precedence. The Wi-Fi connection and the Wi-Fi hotspot connection will not become active.
Remark: the Wi-Fi connection can however co-exist next to the cabled LAN connection. The Wi-Fi connection will not become active, but you can scan for wireless networks in the Sensor Dashboard, fill out the Wi-Fi connection details and turn on the "Auto connect" slider while connected via LAN (see section 5.3 for more information on how to activate a Wi-Fi connection). In the "Wireless – 802.11" pane you can see that the Wi-Fi connection has an IPv4 address, but this IP address cannot be used since the Server is working via the preferred LAN connection.

b) If there is no LAN connection available (cable is unplugged), the Wi-Fi connection is the preferred connection. For the Wi-Fi connection to become active, an active Wi-Fi connection must be available and the "Auto connect" slider in the "Wireless – 802.11" pane needs to be set up to connect to one of the scanned Wi-Fi networks (see section 5.3 for more information on how to activate a Wi-Fi connection). The hotspot connection will not become active.
Remark: the LAN connection will show "unplugged" in the Sensor Dashboard in the "Ethernet - 802.3" pane instead of the IPv4 address.



c) If there is no LAN or Wi-Fi connection available and/or the Wi-Fi auto connect slider is turned off, the hotspot will wait for **60 seconds** for still another connection to pop up. If no other connection becomes active, the hotspot (SERN-xxxxxxxxx) will become active and will appear in your list of available Wi-Fi connections on your PC/phone. You can connect to the hotspot as described in section 5.1.
Remark: we strongly advice to turn the hotspot's "Auto Off" slider on (blue). When there is a LAN or Wi-Fi connection available, the hotspot will turn off and the Server will switch back to a LAN or Wi-Fi connection.

USER MANUAL


LAN connection available?
Yes
No
Cabled LAN connection will prevail
WiFi connection will not start
Hotspot connection will not start
WiFi connection available?
Yes
No
Autoconnect slider in Sensor Dashboard on?
Yes
No
WiFi connection will prevail
Hotspot connection will not start
Hotspot will wait 60 seconds for other connections
Hotspot will become active as SERN-xxxxxx

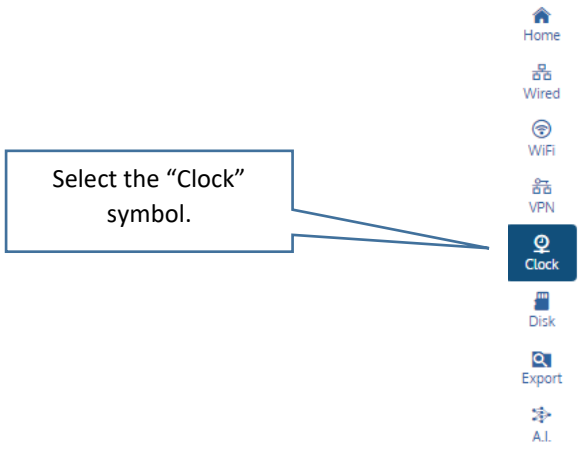
USER MANUAL

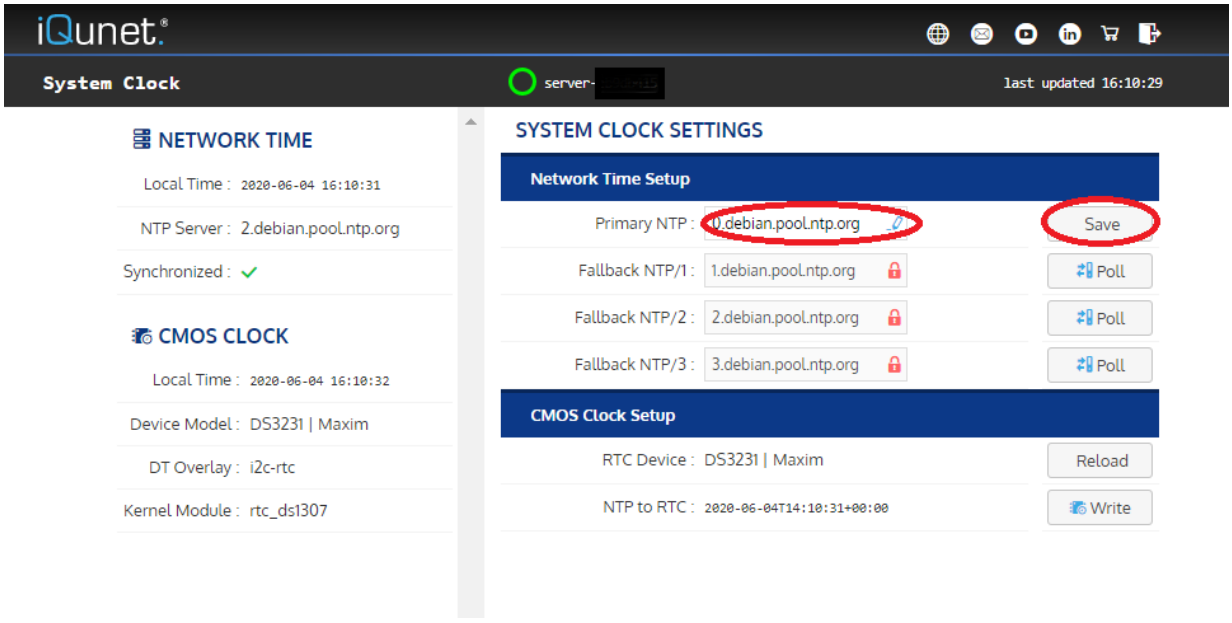
6. System clock

In the "System Clock" section you can set up your own Network Time Protocol (NTP) server to synchronize the hardware clock with. Normally the default NTP server is used (0.debian.pool.ntp.org). The iQunet system considers the drift and offset between the Real Time Clock (RTC) and the NTP clock so in most cases this default NTP server will work fine.

If you need to use your own NTP server for example when the default NTP server is blocked by the firewall, you can change the Primary NTP server.

Open the "System Clock" panel by clicking on the "Clock" symbol on the left-hand side in the iQunet Sensor Dashboard. Edit the Primary NTP (to for example time.google.com) and press "Save".

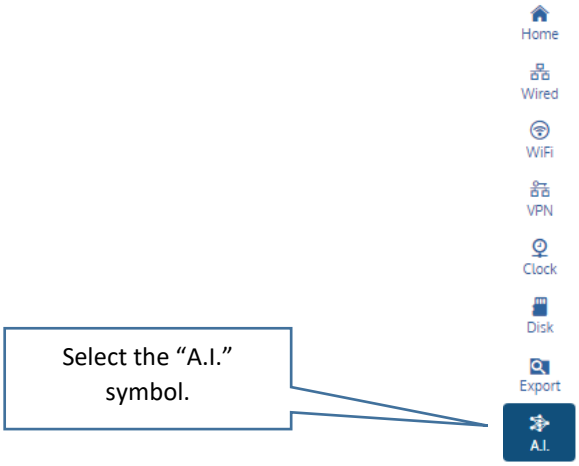




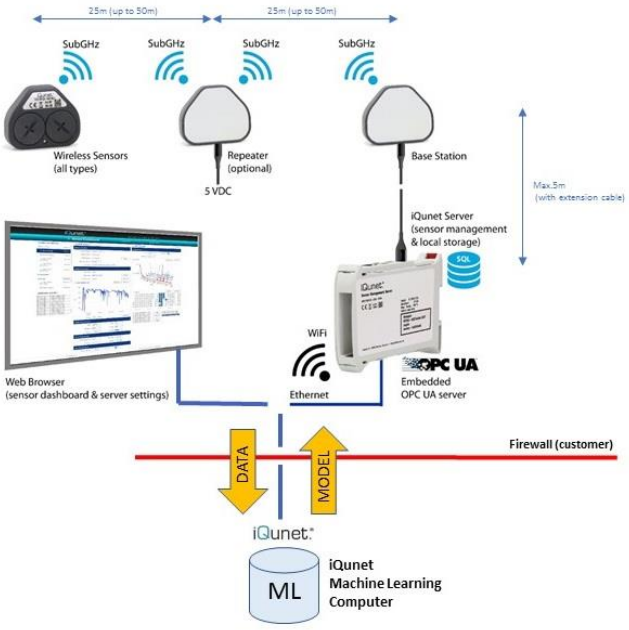
USER MANUAL

7. Anomaly Monitor

Open the “Anomaly Monitor” panel by clicking on the “A.I.” symbol on the left-hand side in the iQunet Sensor Dashboard.

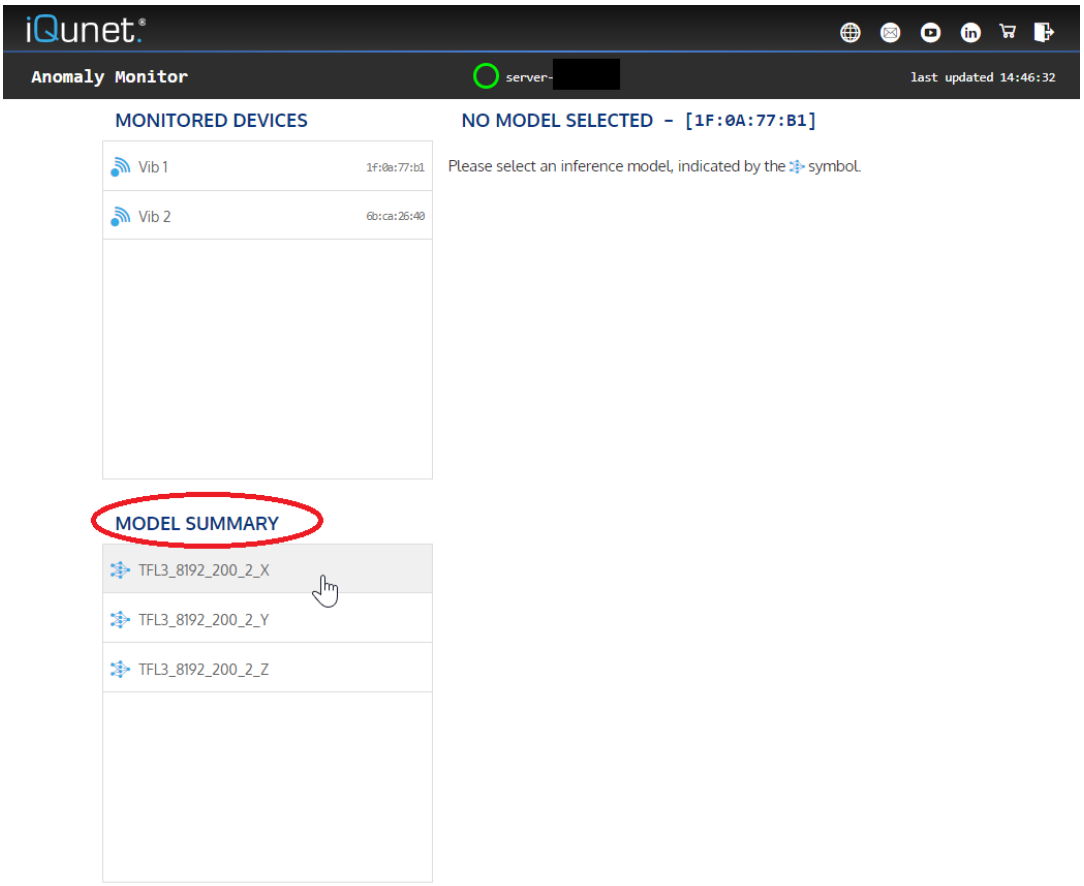


When you subscribe for the iQunet Anomaly Monitoring Service, a model will be created based on your acquired data set. All historical sensor data stored on your local iQunet Server will be automatically compressed and transferred once to the iQunet Machine Learning Servers (located in the iQunet premises) to calculate a machine learning data model. This model is then returned and saved on to your local iQunet Server for continuous local anomaly monitoring. New measurements that differ too much from the calculated data model are detected as anomalies and can be followed up and flagged (difference based on the Mean Squared Error).



USER MANUAL

To start monitoring anomalies, select an existing sensor model in the “Model Summary” section. The model name is composed of the sensor settings (for example TFL3_8192_200_2_X).

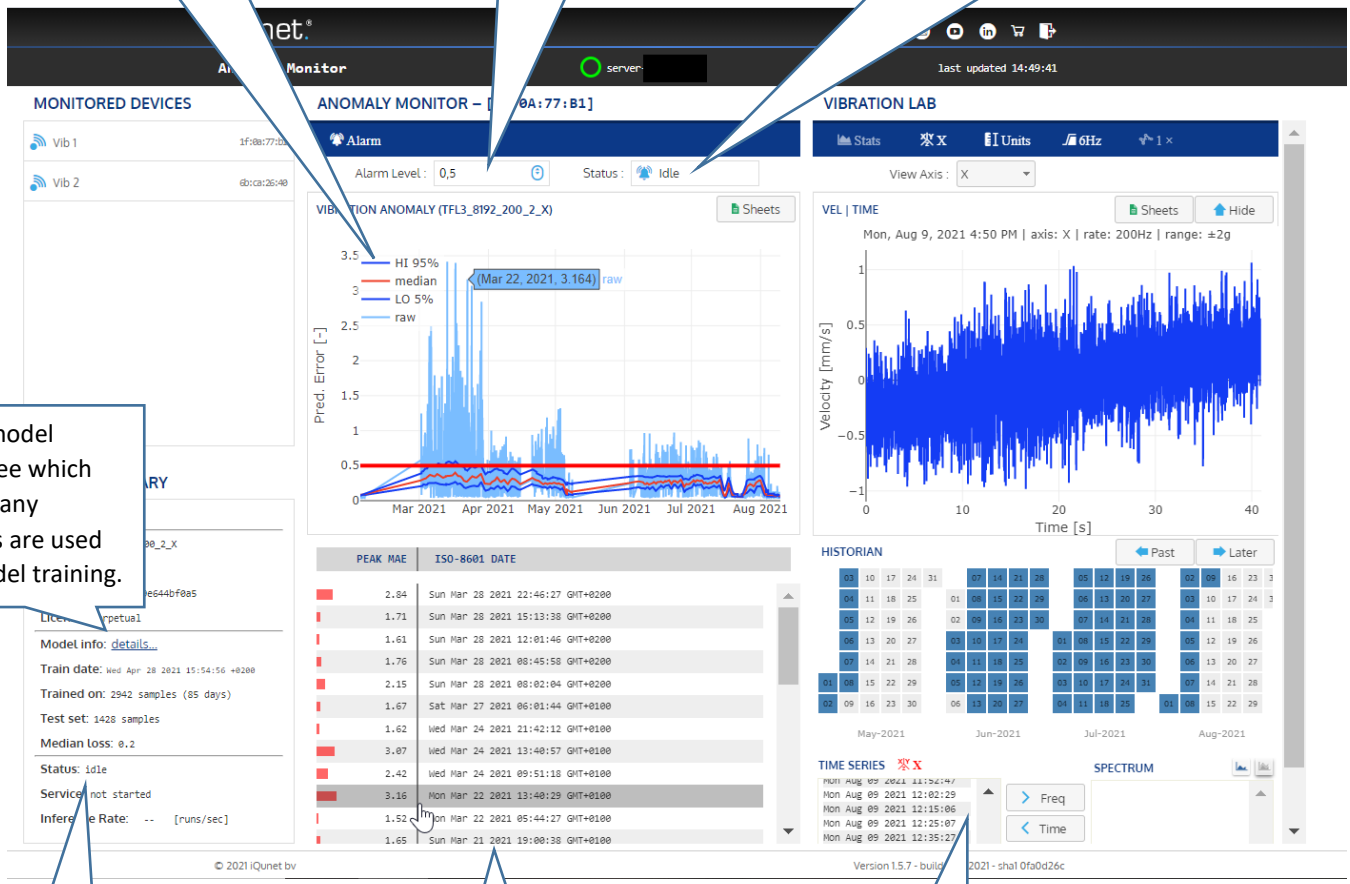


USER MANUAL

Select or unselect an expectile by clicking on the colored lines.

Set an alarm level for the median prediction error.

Status of the last new measurement: alarm (median error above alarm level) or idle (median error below alarm level).



Open the model details to see which and how many parameters are used for the model training.

Status of the anomaly monitor: a new measurement is being processed if the status is not idle.

List of the highest prediction errors (peaks): BLUE colored items are raw anomalies below alarm level, RED colored items are above alarm level.

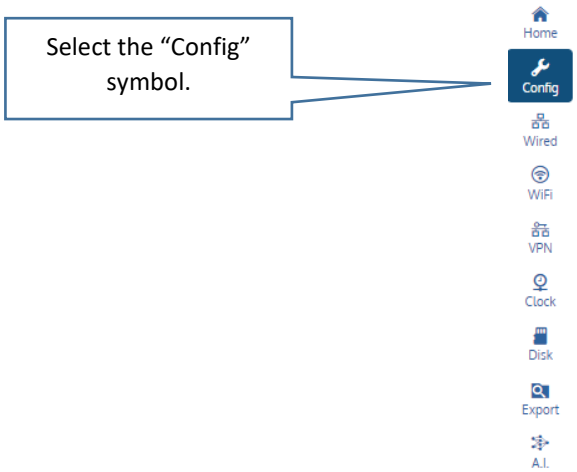
Clicking on 1 of these items shows where the anomaly is situated in the graph above and opens the time series in the vibration lab on the right-hand side.

You can compare the selected anomaly related measurement with measurements coming before and after that measurement. Check for 3D trends by adding them to the SPECTRUM box in the vibration lab (see figure below).

USER MANUAL

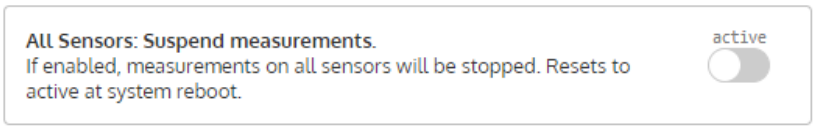
8. System settings

Open the “System Settings” panel by clicking on the “Config” symbol on the left-hand side in the iQunet Sensor Dashboard.



USER MANUAL

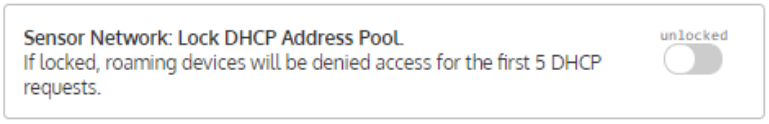
8.1. Suspend measurements



If the slider is set to active, all measurements on the complete connected devices list will be paused. Inactivating the slider will activate the measurements on all sensors.

Remark: the slider will be reset to active after a system reboot.

8.2. Lock DHCP Address Pool



If the slider is set to locked, roaming sensor devices will be denied access to this iQunet Server for the first 5 DHCP requests. The sensor will still be allowed access but with a delay of approximately 15 seconds. In this way an accidental sensor reboot within the wireless sensor network of this Server will not be picked up.

After the 15 seconds delay the sensor will be accepted by the Server and listed as pending (blue color) in the “Connected Devices” list. After 10 minutes the sensor will be rebooted so it can reconnect itself to its original Base Station/Repeater and corresponding Server where it received a name previously. If it was the intention to connect the sensor to this Server, you must (re)name the sensor (see section 2.1).

Remark: it is recommended to leave the switch in the **unlocked** status in normal operation.

Remark: a sensor will always look for a Base Station or Repeater within its wireless range. In this way sensors cannot get “lost”. If a sensor in blue “pending” status is not able to connect to a second Base Station or Repeater (with better connectivity and/or previously named there), it will remain connected to the Base Station or Repeater with the best connectivity (see section 1.2.1).

8.3. Reduce MTU size

Reducing the MTU (Maximum Transmission Unit) size can improve the latency on some networks with packet fragmentation. The MTU size defines the largest packet size that can be transmitted as a single entity over the network connection (without fragmentation). If an IP packet is larger than the MTU size of the connection, the packet will be fragmented into smaller packets so that it fits within the network constraints. The MTU is usually limited by the underlying network capabilities. If the MTU is larger than the network can support, data will get lost.

A larger MTU value allows more data to be transferred at once and therefore reduces the overhead. On the other hand, smaller packets (smaller MTU sizes) can be transferred faster and reduce the network delay. Therefore, the MTU size should be adjusted to optimize both requirements for the specific network connection.